



Industria y Comercio

SUPERINTENDENCIA

P. C. T.

Delegatura de Propiedad Industrial

División de Nuevas Creaciones

05031840

SOLICITUD

PATENTE DE INVENCION

21. EXPEDIENTE No.

05031840

54. TÍTULO *Dispositivo y sistema de Seguridad.*

51. CLASIFICACIÓN INTERNACIONAL

71. SOLICITANTE *Ingenia Holdings Limited. e.
Ingenia. Technology Limited.*

DOMICILIO *Fortela, Islas Virgenes Britanicas
Londres, Inglaterra, Reino Unido.*

74. APODERADO *Dra. Margarita Castellanos Abondano*

22. BOGOTÁ, D. C., *08 - Abril 2005*

PETITORIO



SUPERINDUSTRIA Y COMERCIO
Radicación: 05031040 00000000 Fólios: 234
Fecha (AMD): 2005-04-08 14:22:39
Trámite: 011 PCT-PATENT 379 FASE NACI 411 PRESENTAC
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

FORMULARIO UNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL

SOLICITUD DE:

①

☒ Patente de Invención.☐ Patente de Modelo de Utilidad.☐ Capítulo I☒ Capítulo II

②

SOLICITANTE (71)

Nombre: INGENIA HOLDINGS LIMITED e
INGENIA TECHNOLOGY LIMITED
Dirección: Mill Mall, Suite 8, Wickhams Cay 1,
PO Box 3085, Road Town, Tortola, ISLAS
VIRGENES BRITANICAS y
New Garden House, 78 Hatton Garden, Londres
EC1N 8JA, INGLATERRA, REINO UNIDO.
Nacionalidad o Domicilio: Tortola, ISLAS VIRGENES
BRITANICAS y Londres, INGLATERRA, REINO UNIDO
Lugar de Constitución: ISLAS VIRGENES
BRITANICAS e INGLATERRA.

Teléfono: Fax:
E-mail:

IDENTIFICACIÓN

C.C. ☐ NIT ☐C.E. ☐ Otro ☐

Número Cual

③

REPRESENTANTE
O APODERADO (74)

Nombre: MARGARITA CASTELLANOS A.
Dirección: Calle 94 A No. 7 A-09
Teléfono: 610 74 20 Fax: 610 07 06
E-mail: mail@alvarocastellanos.com

IDENTIFICACIÓN

C.C. ☒ NIT ☐C.E. ☐ Otro ☐
Cual

Número 39'779.654 TPA 70,819

④

INVENTOR (ES) (72)

Nombre: RUSSELL PAUL COWBURN
Dirección: University of Durham, Department of Physics, Rochester Building, Science
Laboratories, South Road, Durham, DH1 3LE, INGLATERRA, REINO UNIDO.
Nacionalidad o Domicilio: INGLATERRA, REINO UNIDO

⑤

PCT (86)

Solicitud Internacional No. PCT/GB2003/003938

Fecha 10/09/2003

Publicación Internacional No. WO 2004/025549

Fecha 25/03/2004

⑥

Título (54)

"DISPOSITIVO Y SISTEMA DE SEGURIDAD"

⑦

Clasificación Internacional (51) G06K 19/06, 19/12

⑧

Prioridad

(33) País de Origen

(32) Fecha

(31) Número de Solicitud

SI ☒ NO ☐

GB

10/09/2002

0220907.0

⑨

Comprobante de pago No.

05-21,913

Fecha

Marzo 29 de 2005

Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página.

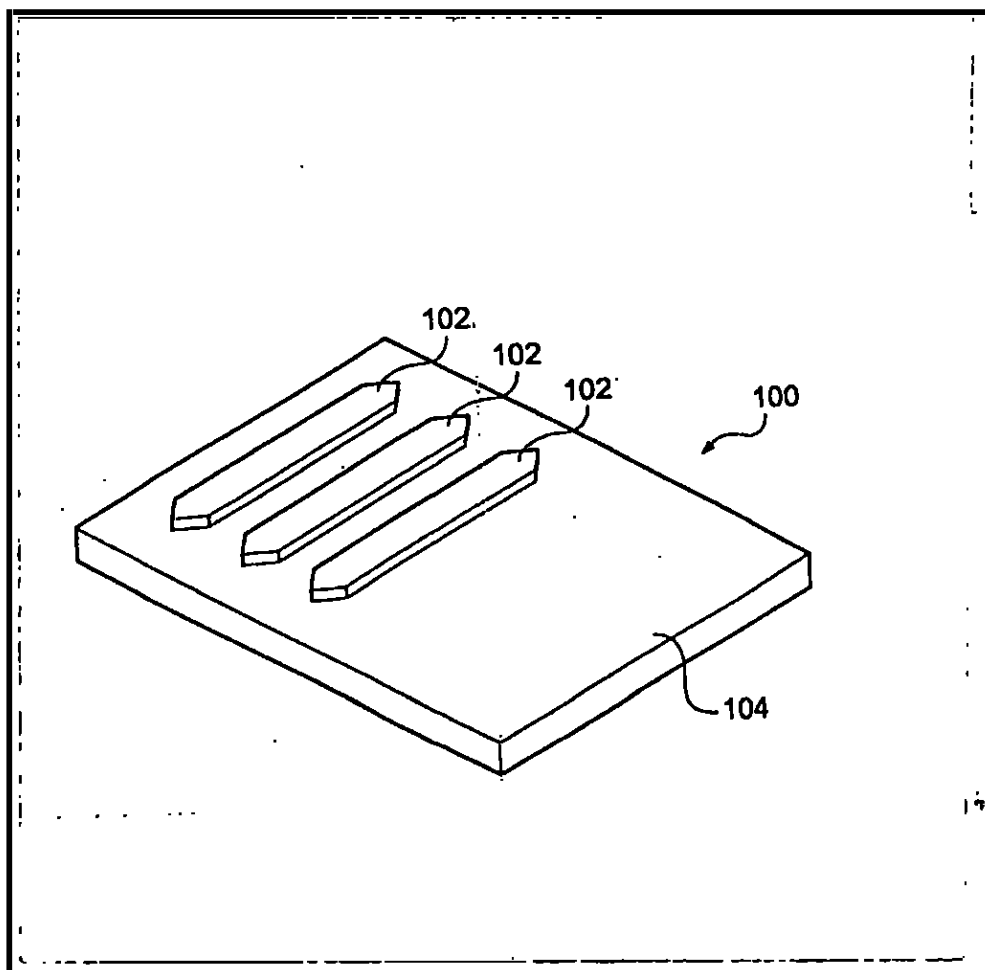
10

Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredite la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Poderes, si fuere el caso, junto con la sustitución del mismo a mi favor
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☐ Declaraciones.
- ☒ Copia de la solicitud internacional (Resumen, descripción, reivindicaciones, dibujos).
- ☒ Traducción de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos).
- ☒ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA).
- ☒ Traducción del examen preliminar internacional efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☒ Arte final 12x12
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros Segundo Examen Preliminar, junto con anexos y traducción.

11

FIGURA CARACTERISTICA:



12

Solicito la concesión de la patente,

08 ABR. 2005

NOMBRE: MARGARITA CASTELLANOS ABONDANO

FIRMA:

C.C. No. 39.779.654 Usaquén - TPA 70.819 C.S.J.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

SUPERINDUSTRIA Y COMERCIO

Radicacion : 05031040 00000000

Folios: 234

Fecha (AMD): 2005-04-08 14:22:39

Tramite : 011 PCT-PATENT 379 FASE NACI 411 PRESENTAL

Dependencia: 2603 DIVISION DE NUEVAS CREACIONES

RECIBO OFICIAL DE CAJA : 05 - 21,913
FECHA : MARZO 29 DE 2005

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
ALVARO CASTELLANOS	CONSIGNACION	BANCO POPULAR	050-00110-6	35849141	29/03/2005	12,451,000.00

***** CONCEPTO *****

CANT. RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1 50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	443,000.00
	TOTAL :	\$ 443,000.00

SON: CUATROCIENTOS CUARENTA Y TRES MIL PESOS

RESPONSABLE : 

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

(19) World Intellectual Property
Organization
International Bureau



INTERNATIONAL BUREAU OF PATENT COOPERATION
35, rue de la Harpe, CH-1015, Genève, Suisse
P.O. Box 6809, CH-1211, Genève, Suisse
P.O. Box 18, Armonia, RJ-22461-900, Brazil
P.O. Box 11,111, Montevideo, Uruguay
P.O. Box 11,111, Montevideo, Uruguay

(43) International Publication Date
25 March 2004 (25.03.2004)

PCT

(10) International Publication Number
WO 2004/025549 A1

(51) International Patent Classification: G06K 19/06,
19/12

(74) Agents: POTTER, Julian, Mark et al.; D. Young & Co,
21 New Fetter Lane, London EC4A 1DA (GB)

(21) International Application Number:
PCT/GB2003/003938

(81) Designated States (national): AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KH, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NI, NO, NZ, PG, PH, PL, PT, RO, RU, SC, SD,
SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date:
10 September 2003 (10.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SI, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(30) Priority Data:
0220907.0 10 September 2002 (10.09.2002) GB

(71) Applicants (for all designated States except US): INGE-
NIA HOLDINGS LIMITED [—/—]; Mill+Mall, Suite
6, Wickhams Cay 1, PO Box 3085, Road Town, Tortola
(VG). INGENIA TECHNOLOGY LIMITED [GB/GB];
New Garden House, 78 Hatton Garden, London EC1N 8JA
(GB).

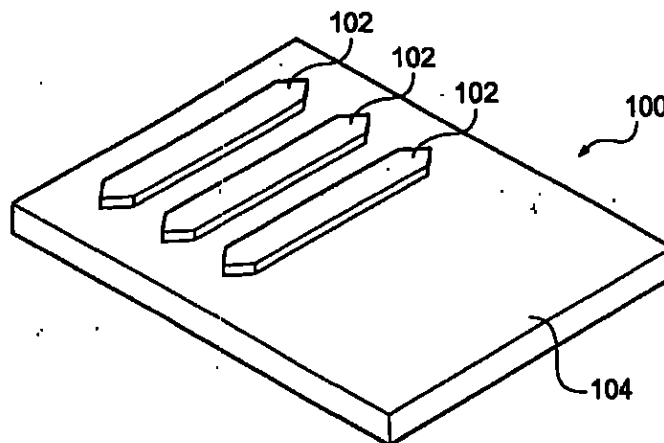
Declaration under Rule 4.17:
— of inventorship (Rule 4.17(iv)) for US only

(72) Inventor; and
(75) Inventor/Applicant (for US only): COWBURN, Russell,
Paul [GB/GB]; University of Durham, Department of
Physics, Rochester Building, Science Laboratories, South
Road, Durham DH1 3LR (GB).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: SECURITY DEVICE AND SYSTEM



(57) Abstract: A security device (100) comprises at least one magnetic element (102). The magnetic element (102) is responsive to an applied magnetic field to provide a characteristic response. The characteristic response can be used to identify a particular security device (100) when interrogated by a security system, thereby aiding in prevention of copying of the security device (100).

WO 2004/025549 A1

Security device and system

The present invention relates to security devices and methods. In particular, the present invention relates to security devices and methods for identifying unauthorised copying of goods etc. to which such security devices are applied.

5

As is known, and discussed herein, copying of various products such as, for example, documents, passports and goods etc., is a common problem. Counterfeiters and/or pirates often copy items having various levels of copy protection and have become increasingly adept at evading existing higher level copy protection schemes. For example, they are increasingly copying items such as credit cards by reproduction of magnetic strips, passports with holograms etc.

Various aspects and embodiments of the invention seek to provide a way for improving detection of copied items to reduce the effects of counterfeiting.

15

According to a first aspect of the invention, there is provided a security device comprising at least one magnetic element. The at least one magnetic element is responsive to an applied magnetic field to provide a characteristic response. This characteristic response is inherently difficult to reproduce as it depends upon uncontrollable nano-scale variations in the structure of the magnetic elements. Thus, a skilled scientist, even one who understands the technology, cannot copy such security devices using current technology, even if he wanted to. The inherent variability of such nano-scale variations may also provide that many such characteristic responses are obtained for individual security devices, thereby ensuring that a brute-force approach to reproducing them requires an extremely large number of such devices to be made before an acceptable copy can be made. (e.g. it may be necessary to produce millions or billions of such devices before a suitable copy is made)

Security devices may be provided with an identifier to identify an individual security device. Identifiers may be unique. Where unique identifiers are provided, any attempt at brute force copying requires a copier to make an extremely large

30

number of devices for each identifier before one acceptable copy can be made. Hence a copier cannot readily simply stock a large number of devices and select ones with matching characteristic responses unless he stocks a large number *per* identifier: e.g. where there is a 1 in 2×10^6 chance of randomly copying a security device and 2^{32} identifiers are provided, a forger has to produce $2 \times 10^6 \times 2^{32}$ identifiers to have an even chance of copying a single security device: this number is enormous: i.e. 8,589,934,592,000,000. Hence, the difficulty in copying a given device becomes apparent.

10 Identifiers may be formed by the magnetic elements themselves. In various embodiments a pattern of one or more of the identifiers may be used to define a unique identifier. Such magnetic elements provide both the characteristic response and the unique identifier, making them even more difficult to copy as the characteristic response and the unique identifier are both provided, inseparably, by the same physical
15 structure(s).

According to another aspect of the invention, there is provided a method of manufacturing a security device, comprising providing at least one magnetic element, wherein the at least one magnetic element provides a characteristic response in
20 response to an applied magnetic field. The characteristic response provided may be used to provide a premeasured characteristic response that may subsequently be used in identification of the security device that generated it.

According to another aspect of the invention, there is provided a system for
25 reading a security device, comprising: a magnetic field generation system for applying a magnetic field to a security device; and a detection system for measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field, wherein said system is operable to compare said one or more parameters representative of a measured characteristic response to
30 one or more respective parameters of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

According to another aspect of the invention, there is provided a method for reading a security device, comprising applying a magnetic field to a security device; measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field; and comparing said one or more parameters representative of a measured characteristic response to one or more respective parameter(s) of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

Security devices can be incorporated into products etc. during manufacture and/or thereafter. They may be used to detect counterfeit goods, products etc. by comparing the premeasured characteristic response with a measured characteristic response. Various premeasured characteristic responses may be used to compare a premeasured characteristic response with a measured characteristic response for a security device according to an identifier associated with that security device.

Security devices can be incorporated into products such as, for example, one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging; an item of clothing; an item of footwear; a smart-card; a credit or bank card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise. In order that counterfeit or forged variants thereof may be identified.

The term magnetic element is intended to include any element formed of any material that provides a measurable signal in response to an applied magnetic field, whether or not that material itself possesses an inherent magnetisation.

One aspect of the invention relates to a security device, for example to comprise an identification and/or authentication device for use in isolation or for use in association with, incorporated into or onto or attached to another article. The security device provides a characteristic response or signature for identification and/or authentication in a manner that limits or makes difficult the copying of the device, and

consequently the copying or counterfeiting of any item used in association therewith. Another aspect of the invention relates to a data reader particularly suited to reading such a characteristic response/signature, to a method of producing/measuring such a characteristic response/signature in a security system including device and reader, and/or to an identification or authentication method using such a device and/or system.

A major loss of revenue to many businesses and a substantial source of criminal activity arises from illegal counterfeiting or copying of items. Examples include, but are not limited to:

- Copying cards and like devices used for paperless financial transactions such as credit card and bank cards to allow unauthorised transactions and withdrawals from ATMs;
- Forging and copying items used for identification, such as passports, visa documents, driving licenses, personal identity cards and the like;
- Copying material carried on a data storage medium, such as CD and DVD disks;
- Forging and copying official documents such as certificates;
- Duplicating smart cards used for identity/ access purposes, for example to control access to areas as part of a security system, to control access to services such as pay-TV, to control or log use of hardware such as computers or other office equipment in a multiple user environment;
- Copying security or authenticity labels as part of counterfeit goods manufacture, to make unauthorised and/or inferior copies of high-value branded goods, high specification safety-critical goods and the like.

This is a particularly identified problem in relation to cards and like devices used for paperless financial transactions and for identification purposes, and this area has led development of security systems, which are nevertheless likely to be generally applicable to most or all areas where copying is a problem.

As paperless commercial and general security systems have become more sophisticated, increased automation coupled with an increased information storage

capacity on the item have created great opportunities for financial and identity fraud by copying of such documents. The concentration of wealth and/or information accessible through credit and bank cards and identity documents has increased. There has developed a growing need for accurate verification and identification such items and/or effective copy prevention.

Card and documentary systems in particular have adopted measures that improve security by making counterfeiting difficult or inconvenient. This approach has concentrated in particular on incorporation of embedded devices on or in the card or other document which are difficult to copy effectively. Examples include holographic images, diffraction gratings, specialist substances (inks, materials etc), embossed structures, structures within the material of the card, etc.

Ultimately though, these markings can be copied by the sophisticated counterfeiter, and will be if the rewards are sufficient. There exists a general desire for a security marking that cannot practically be counterfeited.

An effective strategy against unauthorised copying of items exists if a *random signature* or characteristic response can be associated with the item or with a device that is attached to the item. The random signature/characteristic response could come from some uncontrollable manufacturing process that can never be duplicated precisely. Thus, there always exists some small difference between the original item and its copy; if this difference can be detected and compared with a previously measured response (e.g. a baseline response in which the response of individual magnetic elements are recorded separately, or the average response of a collection of such magnetic elements are recorded) taken from the original item, forgery can be identified.

There are 4 primary preferred requirements of a practical random signature:

- That it be possible to measure the signature easily and without excessive cost;

- That it be possible to represent the baseline signature easily, preferably by a small list of digital numbers.
- That there be a large degree of randomness inherent in the manufacture of the signature, such that every signature is slightly different;
- 5 • That it not be possible to control the manufacture of the signature so that its randomness could be stripped out or suppressed and an identical copy of an existing signature made.

Difficulties in achieving all of these requirements have to date limited the
10 practical applicability of the concept on a wide scale in everyday systems.

Viewed from a first perspective the invention provides a security device for an item which is inherently difficult to copy and thus limits counterfeiting.

15 Viewed from another perspective the invention provides a security device for an item based upon a random signature which is readily manufactured and measurable on a scale and at a cost appropriate for everyday use in authentication/ counterfeit prevention of high value items.

20 Viewed from a further perspective the invention provides a data reader particularly suited to reading the signature of such a device.

Thus, according to the invention in a first aspect there is provided a security device comprising at least one and preferably a plurality and more preferably a large
25 plurality of magnetic elements arrayed on a suitable substrate and having a machine readable magnetic signature response, provided in combination with a predetermined baseline magnetic signature response reading.

In various embodiments, the magnetic elements may comprise thin layer
30 magnetic material, such as thin magnetic wires. The magnetic material may comprise macroscopic wires and/or dots, microscopic wires and/or dots and/or nanowires and/or nanodots, laid down in suitable form on a suitable substrate to give a machine readable

magnetic marking, with a measurable baseline signature signal highly dependent upon the precise inherent structure. The predetermined recorded baseline signature response gives a comparative figure, an "expected" response which can be used in connection with a measured response to authenticate the device.

5

As used herein, "device" at its broadest comprises the magnetic element(s) as hereinbefore described to be laid down on a suitable substrate, such as, for example, the surface of an item to which a security device is to be applied. Examples of the application of such a device include without limitation such a device constituting or
10 comprising a part of an object adapted for use in its own right as an identification, authentication, key or any other application; a device constituting or comprising part of such an object provided for use with a second object, in particular for example as an attachment thereto, for authentication, identification or other labelling, related security or other purposes; a device portion incorporated into or onto a second item for such
15 identification, authentication or related security or other purposes. In particular, the device is provided to authenticate and impede/prevent unauthorised counterfeiting by copying or cloning of an article of which it forms a part, or with which it is associated.

Examples of suitable collections of magnetic elements are described in R.P.Cowburn,
20 Journal of Physics D, 33, R1 (2000). The present invention may rely upon their singular effectiveness in creating a random signature for anti-forgery.

The magnetic elements are such that when a time-varying magnetic field is applied to the elements, their magnetic response is a non-linear and hysteretic function
25 of that applied field. This non-linearity may be characterised by discrete jumps in the magnetisation at certain applied field values. The elements are such that the small differences in fabrication which must naturally exist from one element to another will cause the magnetic response to vary slightly from element to element. Furthermore, for various embodiments, the elements are such that a given element responds in as
30 similar a way as possible to each cycle of the time-varying applied magnetic field.

12

In order to determine the baseline signature response of a collection of magnetic elements, a time-varying magnetic field is applied to the elements, and the magnetic response of the elements is recorded. The response can be measured using the device described herein, or by some other means.

5

The baseline response may be condensed by identifying specific features, such as sudden jumps, or the mean and standard deviation of the switching fields. Alternatively, the baseline response may be converted from a time-domain sequence of magnetisation measurements to a frequency-domain list of measurements.

10 Alternatively, the baseline response may be unprocessed.

Measuring the predetermined baseline response is analogous to a calibration procedure. It is anticipated that the predetermined baseline response will only be measured once, at the time of manufacture and that the device will then be supplied to the user with the predetermined baseline response stored in a manner accessible to the user, for example remotely from the device, or in association with the device in a form inaccessible without authorisation. In particular, it is desirable that the predetermined baseline response is securely encrypted, especially if held on or with the device. Preferably the predetermined baseline signature response is encrypted using an asymmetric encryption algorithm with the private key used for enciphering being kept secret and the public key used for deciphering being made available to any reader of the device such that the expected predetermined baseline signature response can be decrypted and comparison can be made with a measured response.

25 In order to test the authenticity of an item protected by a random signature, it is necessary in various embodiments to apply a time-varying magnetic field to the magnetic elements and to record the measured magnetic signature response of the elements to that applied field. The same procedure is used first to determine the predetermined, expected baseline response which is then stored as above, and then by use of a suitable reader to obtain subsequently measured baseline responses which can be compared to the predetermined, expected baseline response to authenticate the device.

13

Authentication relies on the inherently random nature of the device. Artificially fabricated magnetic elements make a very good practical random signature because the magnetic switching field of each element depends critically upon the physical structure of the ends of the elements. Structural variations of only a few nanometres in size can cause significant changes to the switching field (K. J. Kirk, J. N. Chapman, and C. D. W. Wilkinson, J. Appl. Phys. 85, 5237 (1999)). Therefore, in order to replicate the random signature, it is necessary to replicate the precise shape of the elements to near-atomic precision. This is unfeasible using current technology and is likely to remain so for many decades. While near-atomic level manipulation is required to copy the device described in this invention, a macroscopic measurement is sufficient to check authenticity, because when the structure undergoes magnetic switching, the entire structure switches together, making the magnetic response very easy to measure. Thus, the random signature according to this invention requires low-cost, simple processes to interrogate it, but unfeasibly difficult engineering to copy it. This is ideal for a practical random signature.

If the magnetic response of a collection of elements is recorded together as an ensemble measurement, it must be appreciated that the statistical fluctuations upon which this invention is based will be attenuated. The attenuation factor will be $1/\sqrt{N}$, where N is the number of nominally identical elements in the ensemble. Thus, if a collection of individual elements has a switching field with a standard deviation of 10 Oe, then a collection of ensembles of 100 elements will only have a standard deviation of 1 Oe. The measurement of the magnetic response must therefore be made more carefully. On the other hand, the total volume of magnetic material has increased by a factor N , which makes the measurement easier to make.

In various embodiments, authentication relies upon a match between the measured baseline response of the device, and a predetermined baseline response stored securely, in particular in encrypted form. A forger attempting to forge a device incorporating a prerecorded baseline response in an encrypted form will be extremely unlikely to produce a perfect forgery having a measurable magnetic signature response

matching an encrypted prerecorded original. In the genuine device, the predetermined baseline response is recorded in an encryption known only to the manufacturing company or those authorised thereby. If the prospective forger merely attempts to copy both the signature device and the encrypt derived therefrom the forgery will fail, because even if the encrypt is copied exactly the magnetic signature response of the copied device will differ from the original. Thus, on the forgery, the measured and predetermined and recorded signature responses will not match. If the forger creates a copy of the signature device, he could instead measure the baseline response of the forged device readily. However, he could not create a suitable valid encrypt corresponding to the forged baseline response because he does not know the encryption. Thus, both possible copying strategies fail.

Thus, in accordance with various aspects of the invention, a practical method of generating and reading a random signature using artificially structured magnetic materials is described which is for practical purposes nearly impossible to copy, and which thus offers a security device which can authenticate originals and prevent counterfeiting by copying of such originals.

The magnetic elements of various embodiments comprise thin layers of magnetic material, preferably less than 1 μm thick, and more preferably less than 100 nm thick. They may be 10 nm thick or less, but by preference will be generally around 40 nm thick.

The elements may all be nominally identical in shape and of regularly distributed arrangement, or differences between them and/or irregular patterns of arrangement may have been intentionally introduced. It should be emphasised that the random nature of the magnetic response is an inherent consequence of material fabrication, not dependent upon the shape, configuration and distribution pattern of the elements.

The elements may be generally rectangular in shape, in particular elongate rectangular for example comprising an array of generally parallel magnetic elongate

rectangular elements, or may comprise areas of magnetic material, for example being square or circular, or some other regular geometric shape, which may for example be formed into a two dimensional array.

5 As used herein reference made to magnetic wires, microwires or nanowires should be construed as being to such elements of elongated form, and in particular elongate rectangular elements and/or elongate elements in a generally parallel array, but not restricted to the parallel rectangular examples given herein for illustration purposes. As used herein reference made to magnetic dots, microdots or nanodots
10 should be construed as being to such elements comprising areas of magnetic material of less elongate, more squat form, and in particular of regular geometric shape, and/or formed into a two dimensional array, but not restricted to the circular geometry of the examples given herein for illustration purposes.

15 The elements may be discrete, with no magnetic material connecting them, or they may be partially connected by magnetic material into a number of networks, or they may be entirely connected by magnetic material into a single network.

 The elements may be made from a magnetic material, which will by preference
20 be magnetically soft, for example based on nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.

 The elements may be coated with a protective overlayer to prevent oxidation or
25 mechanical damage, said protective over layer comprising a thin layer of non-magnetic material having suitable mechanical and/or environmentally-resistant properties and/or surface treatments and/or coatings, for example comprising a layer of ceramic, glass or plastics material. Such overlayers are conveniently transparent. Particular examples of protective overlayers include titanium dioxide, transparent epoxy resin, plastic or
30 glass, transparent modified silicone resin conformal coating and transparent acrylic conformal coating.

13

The elements are laid down upon a suitable substrate. An underlayer may exist between the elements and the substrate. The device may be incorporated directly into or upon the item which is to be protected, in which case the substrate may be the item which is to be protected against forgery itself or some suitable substrate material laid down thereupon or incorporated therein for the purpose. Alternatively, the device may be incorporated into a separate unit such as a tag, label, certification etc, attachable to or otherwise useable in conjunction with an item to be protected, the attachable unit comprising or incorporating some suitable substrate material. Suitable substrate materials include silicon, glass, plastic or some other material with a smooth surface.

10

In the case of the magnetic elements being formed on an attachable unit, the attachable unit may be attached directly to the item to be protected, or may form part of a certificate or other documentation associated with the item to be protected. Means may be provided in association with an attachable unit to effect attachment between the unit comprising an identification device in accordance with the invention and the item to be protected. Such means may provide for releasable, removable engagement of the attachable unit to the protected item, or for permanent engagement thereupon. In the former case, attachment means may further comprise locking means to ensure that only authorised persons can remove the unit. In either case, the attachment means may further comprise anti-tamper protection and/or mechanisms to indicate tampering by unauthorised persons.

Suitable uses for such attachable unit include, without limitation, labels for items of value, of security importance, or of otherwise critical importance, for example to enable identification of the article, authentication of the article as genuine, verification of the provenance of the article and the like and/or to label the article in a secure and controlled manner, for example with information about the article, pricing information, stock control information etc.

30 In the case of magnetic elements being formed directly upon an item to be protected, similar usages might also be envisaged. Such direct incorporation of the device onto the item to be protected however will be singularly effective in preventing

unauthorised reproduction, given the random and hence inherently non-controllably reproducible nature of the signature device, and will therefore be particularly useful in association with items which might be susceptible to the production of counterfeit copies, since the device will provide for ready authentication of an item as original.

5

The elements may be formed by optical lithography, for example, using the method described herein, although embossing or some other form of contact printing may be used.

10

The plurality of elements making up the device may be of generally the same size and shape, or may have a size and/or shape differing continuously or discontinuously across the device. Preferably, a number of different element sizes will be present in one ensemble.

15

In one embodiment, several discrete groups of differently sized and/or shaped elements, the elements being generally similarly sized or shaped within each group, are provided so that several different switching fields can be identified. For example, an ensemble of rectangular elements in parallel array may comprise several discrete groups of different widths.

20

A suitable example comprises 100 rectangular elements, each 1 mm long; 10 will be 5.0 μm in width, 20 will be 2.5 μm in width, 30 will be 1.7 μm in width, 40 will be 1.2 μm in width. The magnetic response of such an ensemble will then show four distinct groups of switching fields, each of which will exhibit a statistical variation from one tag to the next, which can be used to form a random signature.

25

A second example comprises 450 rectangular elements, each 1 mm long; 150 will be 1.0 μm in width, 120 will be 1.25 μm in width, 90 will be 1.67 μm in width, 60 will be 2.5 μm in width and 30 will be 5 μm in width. The magnetic response of such an ensemble will then show five distinct groups of switching fields.

30

18

In the examples, the number of elements in each group is such that each group should cover generally the same area. The strength of the detected signal from the reader usually depends upon the total area of coverage, so each of the four or five groups of switching fields will register the same strength at the reader. This is a preferred feature for many applications, but it can be envisaged that for other applications several discrete groups of differently sized and/or shaped elements may be provided wherein different groups occupy different areas of the device.

In an alternative embodiment, differently sized and/or shaped elements are provided in a continuously varying array, so that variations in size and/or shape between an element and its neighbours are minimised to avoid large discontinuities. For example the area of an element should vary from its neighbours by no more than 5% and in particular by about 1%. As a result, a smoothly varying collection of switching fields is produced. The variation could be tuned in accordance with a suitable functional form which may be linear or non-linear.

For example, in an analogous device to that described above with rectangular elements in parallel array the width of the elements varies as a smooth function across the array. An ensemble might start with a 2.5 μm wide wire; the next would be 2.53 μm , the next 2.56 μm etc, until 56 wires later the width has risen to 5 μm . The total wire width is 200 μm in this example. An alternative ensemble might start with a 1 μm wide wire; the next would be 1.01 μm , the next 1.02 μm etc, until 450 wires later the width has risen to 5 μm . Different functional forms, e.g. linear, quadratic etc could be used to determine the progression of widths across the ensemble. Unlike the previous example, this would not give distinct groups of switching fields, but rather a smooth collection of switching fields.

In one embodiment, the device, in addition to the signature array comprising a large plurality of signature elements, comprises a single relatively large area magnetic element for use as a reference element, for example a relatively wide magnetic nanowire or wide microwire. In the foregoing examples such a single wide wire could be 1 mm long and 150 μm wide. For a wire at such a large width, the magnetic

property is almost identical to the bulk material, which is usually quite well defined. Thus, in addition to five blocks which have erratic switching fields there is provided one well defined switching field, which can be used to calibrate the reader. This calibration could include making environmentally-based adjustments, such as
5 subtracting the influence of the Earth's magnetic field, for example, or compensating for changes in temperature.

It is necessary that a predetermined base line magnetic signature response is provided in combination with a security device in accordance with various of the
10 embodiments of the invention. It will however be understood that it is not necessary that such a predetermined base line magnetic signature response is provided in physical association with the security device, but merely that it is available to the authorised user of the device for comparison purposes to give an "expected" response to be compared with an actual response when the device is read by suitable means,
15 such as the magnetic signature reading means described herein.

Various embodiments may be provided. In a first, the pre-recorded baseline may be provided in physical association with the device or protected item. In a second, the pre-recorded baseline may be stored by a device reader. In a third, the pre-
20 recorded baseline may be remotely stored from both device and device reader in a manner accessible to an authorised person such that the necessary comparison between expected (i.e. pre-recorded) and actual (measured) baseline readings can be made for authentication purposes.

25 In the first embodiment mentioned above, the pre-recorded baseline response is provided in close physical association with the device or protected item. In one alternative, the pre-recorded baseline is stored in physical proximity to the device in machine-readable form. For example, the pre-recorded baseline is stored as a part of the device; or is stored adjacent to or under the device on a common substrate; or is
30 stored in the vicinity of the device as part of a unit incorporating the security device of the invention, optionally with other security or information features, such as a smart card, identification document, key card, key fob or the like, or a label for an article to

be protected; or is stored on or with an article to be protected which article to be protected has also been provided with a device in accordance with the invention; or is stored as part of a certificate or other documentation associated with an item to be protected which certificate or other documentation may also incorporate such a device
5 in accordance with various embodiments of the invention.

In this embodiment, the prerecorded baseline should be stored in readable but encrypted form. For example, the condensed or unprocessed baseline response is digitally signed using an asymmetric encryption algorithm such as RSA. The private
10 key, which is used for enciphering, is known only to the manufacturing company; the public key, which is used for deciphering, is held on every reader terminal which might be used to read the device.

The digitally signed and encrypted baseline response is stored on the item,
15 preferably with the magnetic elements for example in that it is printed underneath or alongside the elements, or alternatively by recording it onto a magnetic data strip, or by recording it onto an optical bar code or by recording it onto a smart card chip, or by some other means. Other information, such as, but not limited to, the owner's name or a unique identity code or a checksum may also be encrypted into the same data stream
20 and digital signature to prevent the magnetic elements from being transferred to another item or important information on a document or certificate from being modified.

In the second embodiment referred to above, the prerecorded/premeasured base
25 line response is stored on, by, or in close association with a device reader. Such an embodiment lends itself in particular to "lock and key" type systems where the device acts as a key and is used in association with a reader acting as a lock to limit access to particular areas, operation of particular items, or use of particular services to the specified key holder(s).

30

In this embodiment, it is not necessary for prerecorded baseline signature data to be stored upon or in close association with the device itself or a protected item.

Optionally however, the data may still be stored in an encrypted form for security, for example in the manner above described, or may be otherwise security protected.

In the third embodiment referred to above, the prerecorded/premeasured
5 baseline signature data is stored remotely from both the device and protected item and the device reader. Such a mode of operation lends itself in particular to, but is not limited to, systems where a network comprising a large number of readers each expecting to interrogate a large number of devices is envisaged, for example as might be the case with credit cards and the like with multiple points of sale, security and
10 identification systems with multiple points of access etc.

In accordance with this embodiment prerecorded signature data about the device, and in particular about a plurality of different devices, is preferably stored at a central data store, for example connected to a plurality of readers on a distributed
15 network. In such a network two alternative modes of operation can be envisaged. In the first, a reader is adapted to read a device, interrogate a central data store for the prerecorded signature data, and make the comparison. In a second, the device reader is adapted to read the device and pass the actual signature data to such a central data store for verification purposes. The essential principles remain the same.

20

In a further aspect of the invention there is provided a security system including at least one device as hereinbefore described and at least one device reader, said device reader comprising means to read the magnetic response of the device. In particular, the device reader comprises or is provided in association with a magnetic
25 field generator to apply a time-varying magnetic field to the elements, and has a magnetic response recorder to record the response of the magnetic element to that applied magnetic field. An embodiment of a device reader is described herein.

For different applications, suitable systems may comprise a plurality of such
30 readers and/or a plurality of such devices. A system comprising a plurality of such readers may be arranged such that each reader functions independently in isolation, or such that some or all of the readers are linked on a distributed network.

22

Readers provided for a system operated in accordance with the first mode of operation outlined above preferably further comprise means to read the pre-recorded predetermined baseline signature response, in particular the pre-recorded and encrypted signature response, stored on, with or in association with a device or protected article; and preferably further comprise comparator means to compare the prerecorded and measured baseline signature responses. Readers adapted for a system for use in accordance with the second mode of operation described above preferably further comprise storage means for storing the predetermined baseline signature response(s) of the device(s) intended for use therewith, and preferably further comprise comparator means to make a comparison between stored and measured baseline responses. Readers intended for use in accordance with the third mode of operation described above preferably comprise means to receive data concerning a remotely stored predetermined baseline signature response, for example via direct entry of data by a user, or via interrogation of a remote database on a distributed network, together with comparator means to compare the predetermined response to the measured response; or in one alternative, means to transmit the measured response to a remote comparator, which comparator incorporates or is in data communication with a store of predetermined responses.

20

In all cases, the device reader preferably makes a comparison between the measured and predetermined baseline magnetic signature responses, for example against a predetermined tolerance limit, and actuates a response mechanism depending upon whether signatures are identical, for example within those tolerance limits.

25

The response mechanism may comprise a simple display means, of any suitable form, including visual, audio, alphanumeric indicators and the like, of whether the device is authenticated. Additionally or alternatively, other responses may be provided for. For example, authentication might serve to release a real or virtual lock, permitting access to a restricted area, operation of an item of restricted equipment, access to a particular service or the like.

30

According to a further aspect of the invention, a simple device is described which can measure the magnetic response of a small area of thin-film magnetic material. The device is well suited, but not limited, to measuring the magnetic random signature of a device such as described above. The small area will by preference be of size 0.2 mm x 0.2 mm or greater; the magnetic material will be in the thickness range 1 nm to 500 nm, and by preference will be in the range 1 nm to 50 nm. The magnetic material may be a continuous film or may be a collection of magnetic elements. The magnetic material may have a transparent protective overlayer. In various embodiments the magnetic material remains optically reflective.

10

In various embodiments according to this aspect of the invention a device for measurement of the magnetic response of such an area of magnetic material as a time-varying magnetic field is applied to the magnetic material comprises an illumination source, and in particular an infra-red illumination source; a collimator to focus the illumination onto the surface of the magnetic material; and a collector to collect reflected illumination, and to monitor the varying response of this reflection over time as the time-varying magnetic field is applied. Optionally, the device incorporates or is provided with a magnetic field generator to generate such a field.

20 In various embodiments, the transverse magneto-optical Kerr effect is used to measure the magnetic response of the area of magnetic material as a time-varying magnetic field is applied to the magnetic material. This effect is well known in the literature. The response measuring device may incorporate additional means to apply such a time varying magnetic field to the area of magnetic material under investigation, or a separate device may be used to apply the same.

30 In various embodiments the device operates without polarised light. Conventionally, the transverse Kerr effect requires the incoming light to be plane polarised. This is usually achieved by inserting a sheet of Polaroid or some other polarising optical element in the in-coming beam path. It has been surprisingly found that in application to this invention, the polariser can be removed to reduce manufacturing cost and to reduce the size of the device. In the preferred embodiment

of the present device a polariser is absent. This is suitable for many applications. Nevertheless it will be understood that a polariser may be included, for example in the in-coming beam path in conventional manner, where this is desirable or necessary.

5 Preferably, the collimator comprises a pinhole. At the scale of device operation this is found to effectively focus the light without the need to use a lens. This again reduces manufacturing cost and reduces the size of the device. Conveniently, the pinhole has diameter in the size range 0.2 mm – 5 mm.

10 The light is then reflected off the surface of the magnetic thin film. Preferably, a second pin-hole, with diameter in the size range 0.2 mm – 5 mm, is provided to focus the reflected light. It is preferred that the second pin-hole should have the same diameter as the first pin-hole. Light is passed to a collector comprising a light sensitive device, which is by preference a phototransistor or photodiode sensitive to
15 the radiation produced by the light source.

In various embodiments, the light source comprises a light emitting diode. This is in contrast to prior art large scale devices for measuring the magneto-optical Kerr effect where a laser or a discharge lamp or an incandescent lamp is used. The present
20 device is smaller, cheaper and removes the hazards associated with a product containing a laser.

An infra-red light emitting diode (LED) is preferred over a visible spectrum LED for two reasons: high optical intensities are achievable in the infra-red due to the
25 higher currents that infra-red LEDs can sustain; the optical receiver can be rendered insensitive to visible light, thus reducing interference from ambient light.

In various embodiments, the light source comprises a laser diode. Laser diodes are relatively inexpensive and can provide high intensity light.

30

In a further aspect of the invention, a method of manufacture of a security device comprises forming at least one, and preferably a large plurality of, magnetic

elements as above described; obtaining a baseline signature magnetic response for the elements; storing the baseline response as a predetermined baseline response in a form accessible to a user of the device, optionally by encrypting and storing in physical association with the device in any readable form.

5

In various embodiments the elements will be formed by optical lithography.

In various implementations according to this aspect of the invention, a cost saving can be made in the lithography process in the case of the magnetic elements comprising an array of generally rectangular structures. The photoresist is applied to the substrate in the usual fashion and patterned by an optical exposure followed by development. The magnetic material is then deposited onto the patterned photoresist. Usually, the photoresist would then be dissolved in a solvent (lift-off process). However, the photoresist can be left in place, because the magnetic material deposited on top of it forms a second set of rectangular magnetic elements. For example, suppose that the resist had been patterned into rectangular structures of width 0.5 μm with a centre-to-centre spacing of 1.5 μm . If the photoresist is left in place, then the structures comprise a set of 0.5 μm wires attached to the substrate, and an equal number (minus 1) of 1 μm wires attached to the top of the substrate.

20

The invention in a further aspect comprises a method of marking an item for security, identification or authentication purposes by use of the foregoing device and/or system and/or method and in particular by associating a device as hereinbefore described therewith.

25

The invention in a further aspect comprises a method of identifying or authenticating an item by use of the foregoing device and/or system and/or method and in particular by associating a device as hereinbefore described therewith, applying a time-varying magnetic field to the elements thereof to obtain a measured baseline magnetic signature response, for example using the reader hereinbefore described, and comparing the measured response to a predetermined recorded baseline magnetic signature response.

30

Embodiments of the invention will now be described, by way of example only, with reference to the appended figures in which:

5 Figures 1 to 4 show embodiments of security devices according to the present invention in perspective view;

 Figure 5 shows a further embodiment of a security device according to the present invention in plan view;

 Figure 5a shows a another embodiment of a security device according to the
10 present invention in plan view;

 Figure 6 shows another embodiment of a security device according to the present invention shown in cross-sectional view;

 Figures 7a to 7d illustrate magnetic switching modes of magnetic elements that may be used in various embodiments of the present invention;

15 Figures 8a and 8b show idealised, schematic real and averaged hysteresis curves for the magnetic switching of a permalloy material that may be used in various embodiments of the present invention;

 Figures 9a to 9h illustrate a manufacturing technique for producing various embodiments of security devices according to the present invention;

20 Figure 10 shows a reading arrangement forming a part of a security reading device system according to various embodiments of the invention;

 Figure 11 shows a mirror actuator for use in a security device reading system according to various embodiments of the invention;

 Figure 12 shows a further part forming a part of a security device reading
25 system according to various embodiments of the invention;

 Figure 13 shows a signal that drives a magnetic field generator according to various embodiments of the invention;

 Figure 14 shows a signal that drives the mirror actuator according to various embodiments of the invention;

30 Figure 15 shows one cycle of the signal of Figure 13;

 Figure 16 shows a unipolar detector signal representing a characteristic response according to various embodiments of the invention;

Figure 17 shows a synchronisation signal for synchronising various security device reading systems according to various embodiments of the invention;

Figure 18 is an illustration of a first collection of magnetic elements used for a random magnetic signature/characteristic response in accordance with the invention;

5 Figure 19 is an illustration of a second collection of magnetic elements;

Figure 20 is an illustration of a third collection of magnetic elements;

Figure 21 is an illustration of a device for measuring the magnetic response of a small area of thin magnetic film;

Figure 22 is an illustration of an embodiment of the invention in a smart card;

10 Figure 23 is an illustration of an embodiment of the invention in an electronic key;

Figure 24 is an illustration of an embodiment of the invention in an identity tag for attachment to an item to be protected;

15 Figure 25 is an illustration of an embodiment of the invention incorporated into a CD/DVD for authentication purposes; and

Figure 26 is an illustration of an embodiment of the invention incorporated onto a certificate for authentication purposes.

In various embodiments, magnetic materials are used to form magnetic elements responsive to an applied magnetic field. The characteristic response of these magnetic elements to the applied magnetic field gives rise to a measurable characteristic response or signature for identifying a security device including a set of
5 such magnetic elements.

Many types of magnetic material are available that could be used to form magnetic elements in various two-dimensional and three-dimensional shapes: for example, magnetic wires, flattened wires, bars, dots, random spots, random blobs etc.
10 While many such materials can be used in embodiments of the invention, certain materials give a better magnetic response than others when subject to an applied magnetic field; particularly if the magnetic switching properties of the material are to be used as the, or as part of the, measurable characteristic response.

15 Where embodiments of the invention use the magnetic switching properties of the material to produce a characteristic response, magnetically soft materials are useful. Magnetically soft materials are ferromagnetic materials in which the magnetisation can be easily reversed. These materials generally have narrow square-shaped hysteresis loops. Thus, the magnetisation of a magnetic element made from
20 such a material switches its direction in response to an applied field relatively sharply. The coercivity of such materials (i.e. the reverse field needed to drive the magnetisation of a magnetic element made of such a material to zero after being saturated) tends to be relatively low, thereby ensuring that relatively low-field-strength magnets can be used to cause a switch in the magnetisation direction of the magnetic
25 element. Such, relatively low field-strength magnets may be fairly inexpensive, generally compact and easily driven to produce a controlled magnetic field of good uniformity.

Figure 1 shows a security device 100. The security device 100 comprises a
30 plurality of magnetic elements 102 formed upon a silicon substrate 104. The magnetic elements 102 are made of permalloy material.

Figure 2 shows a security device 200. The security device 200 comprises a plurality of magnetic elements 202 formed upon a silicon substrate 204. The magnetic elements 202 are made of permalloy material. Data area 206 is provided in the substrate 204 for storing encrypted premeasured characteristic response information and/or a unique identifier for identifying the security device 200.

The data area 206 of this embodiment comprises a set of etched pits (not shown) encoding binary data corresponding to encrypted premeasured characteristic response information and/or a unique identifier that can be read, for example, by an optical reader (not shown) in a manner analogous to a compact disc.

In further variants of this embodiment, the data area 206 may alternatively, or additionally, comprise electronic circuitry (not shown) that retains characteristic response and/or a unique identifier information.

15

Figure 3 shows a security device 300. The security device 300 comprises a plurality of magnetic elements 302 formed upon a silicon substrate 304. The magnetic elements 302 are made of permalloy material. Data area 306 is provided in the substrate 304 for storing encrypted premeasured characteristic response information and/or a unique identifier for identifying the security device 300.

In the data area 306 of this embodiment indicia 308 are provided. The indicia 308 encode data corresponding to encrypted premeasured characteristic response information and/or a unique identifier that can be read by a reader (not shown). In one variant of this embodiment, visible indicia 308 are provided by a machine readable bar code (not shown) that encodes both encrypted premeasured characteristic response and unique identifier information. In another variant of this embodiment, visible indicia 308 are provided by a machine readable bar code (not shown) that encodes only unique identifier information.

25
30

Figure 4 shows a security device 400. The security device 400 comprises a plurality of magnetic elements 402 formed upon a silicon substrate 404. The magnetic

elements 402 are made of permalloy material. Each magnetic element 402 is backed by a reflective layer 410 made from gold, aluminium, chromium and/or tantalum, for example. The reflective layers 410 provide enhanced reflectivity contrast between the magnetic elements 402 and the substrate 404. This embodiment thus provides for an improved signal to noise ratio (SNR) when the security device 400 is being interrogated by a reading apparatus, such as, for example, a reading apparatus of the type described herein. An advantage of increased SNR is that it enables such a security device 400 to be rapidly interrogated to determine whether or not it is a forgery, and/or needs lower levels of incident light (e.g. ultraviolet to infrared, such as, for example, from 200nm to 1500nm) in order to be interrogated.

Figure 5 shows a further embodiment of a security device 500 in plan view. The security device 500 comprises a plurality of magnetic elements 502a-502e formed upon a silicon substrate 504. The magnetic elements 502a-502e are made of permalloy material formed in the shape of wires, or flattened wires. The magnetic elements ends 505, 507 are formed as angled shapes.

In this embodiment, the width of the magnetic elements 502a-502e in the direction A-A can be made of various widths. In this case, the width of the magnetic elements 502c and 502e are approximately double those of magnetic elements 502a, 502b and 502d. Since the magnitude of the characteristic response signal produced by any particular element is proportional to the volume of material that makes up that element, larger elements give rise to a larger signal that is accordingly more easily measured.

25

In addition, the magnetic elements 502a-502e can themselves be used to encode an identifier. In the illustrated embodiment, the five magnetic elements 502a-502e occupy an area of approximately 1x1 mm with space enough for some seven to twelve magnetic elements of the 40 μ m width and 900 μ m length of magnetic elements 502a, 502b and 502d. The pattern of the five magnetic elements 502a-502e is used to provide an identifier for the security device 500. This pattern is analogous to

30

a bar code that identifies a particular security device 500, and may be unique to each individual security device 500 that is manufactured.

5 The number of unique identifiers that can be provided by variants of this embodiment depend upon the number and density of the magnetic elements 502. For example, embodiments having a possible 32 magnetic elements provide for a possible 2^{32} (i.e. 4,294,967,296) unique identifiers. Moreover, where the magnetic elements are identifiable using a two-dimensional scanning pattern, e.g. where magnetic elements 502 are provided in an array of 32x32 dots, this figure can be squared.

10

Figure 5a illustrates another embodiment. Various magnetic elements 81, 82 of different lengths are provided. In this embodiment a characteristic response can still be measured even from what appear as part of an identifier pattern as 'spaces', since the effective bits of an identifier provided by the magnetic elements 81 each still provide a response. Reading is achieved using a laser beam that may only be focused in one dimension, e.g. to 1mm long and 20 microns wide. The reflected intensity, as measured e.g. using the magneto-optic Kerr effect as herein described, therefore changes according to the length of the bar. Typically 30 μm width bars with longer bars 82 about 700 μm long and shorter bars 81, for example, some 300 μm long, may be provided.

20

Figure 6 shows an embodiment of a security device 600 in cross-sectional view. Although this embodiment incorporates both reflectivity and contrast enhancing materials, these can be provided separately in various other embodiments.

25

The security device 600 is formed from a silicon substrate 604. The substrate 604 incorporates reflective layers 603 formed beneath magnetic elements 602 made from, for example, gold, aluminium, chromium and/or tantalum. The reflective layers 603 increase the optical signal (including the Kerr effect signal, as described below) reflected from the magnetic elements 602 as compared to magnetic elements formed directly onto a substrate material.

30

Adjacent to the magnetic elements 602 absorbing layers 605, made of, for example, carbon, are formed. The absorbing layers 605 have a low reflectivity, and thus enhance the contrast between light reflected therefrom and the adjacent magnetic elements 602.

5

Another variant of the embodiment shown in Figure 6 uses, for example, a roughened surface formed by deposition or etching, as a scattering material in place of the absorbing layers 605. The effect of the scattering material is to attenuate any optical signal reflected from the areas adjacent the magnetic elements 602, with the additional advantage that the security device 600 need not absorb as much optical energy.

In order to characterise various materials that may have desirable responses to an applied magnetic field, it is useful at this point to describe some of the physics involved in the switching of the magnetisation direction of various types of ferromagnetic materials. Such ferromagnetic materials may be used in various embodiments.

Referring to Figure 7a, a magnetic element 102 is shown. In this example, the magnetic element 102 is formed of a ferromagnetic material shaped in the form of a flattened wire. The magnetic element 102 has a magnetisation M having an initial magnitude and direction as indicated by the arrow 150. An applied magnetic field H is shown being applied to the magnetic element 102 in a direction substantially parallel to a longitudinal axis of the magnetic element 102, and with an opposite polarity to the initial magnetisation.

The applied magnetic field H acts to reverse the polarity of the magnetisation of the magnetic element 102. There are various physical mechanisms by which the magnetisation of the magnetic element 102 can reverse. Each of these leads to a different magnetic switching characteristic of the magnetisation M .

In a first switching mode (sometimes referred to as a coherent rotation mode, shown schematically in Figure 7b) the individual magnetisations of a plurality of magnetic domains 152 rotate coherently, as shown schematically by the broken arrows 154. Thus in this mode, the overall magnetisation of the magnetic element 102 undergoes smooth directional rotation and magnetisation magnitude changes to align with the applied magnetic field H.

In a second switching mode (sometimes referred to as a multiple nucleation mode, shown schematically in Figure 7c) many magnetic domains 156 dominates the switching of the magnetisation of the magnetic element 102 when an applied magnetic field H is present. The magnetisations of the individual domains 156 initially rotate into alignment with the applied magnetic field H, as illustrated in Figure 7c. Subsequently the domains grow in size. However, in this mode the temporal evolution of the magnetisation of the whole of the magnetic element 102 cannot be readily discerned, and may change randomly in response to environmental conditions, such as temperature.

Thus, although materials that operate according to the second switching mode can be used for magnetic elements of various embodiments, they are not optimal since, because there is less variation in the magnetic switching properties to provide a measured characteristic response, it is relatively easy to copy.

In a third switching mode (sometimes referred to as Brown's paradox, a sharp switching or a brittle mode, shown schematically in Figure 7d) the growth of a single magnetic domain 158 dominates the change in magnetisation of the magnetic element 102. Such a domain 158 may be associated with a structural defect in the magnetic element 102 that is randomly introduced during a manufacturing process, e.g. by uncontrollable fabrication noise arising from random nano-scale material defects (e.g. defects that occur on a size scale from about 0.5 nm to about 500 nm) that are virtually impossible to reproduce controllably or predictably. In this mode, the growth of domain 158 dominates the switching of the magnetisation of the magnetic element 102 over a wide variety of physical and environmental conditions. Accordingly, materials

that operate according to the third mode are ideally suited to the provision of stable, but non-predetermined, magnetic switching properties that provide a reproducibly measurable characteristic response.

5 Various possible defects can form a nucleation centre, these can, for example, include one or more of the following: local failures in lithographic definition, e.g. small (micron or sub-micron) notches out of the edges of tips of elements; local crystallographic defects, such as dislocations, inclusions, nanometre-scale voids; local variations in chemical composition or stoichiometry, leading to a local change in
10 magnetic anisotropy; and local short-scale variations in thickness, leading to a surface indentation which can generate Orange Peel fields, as envisaged by Brown.

The reference 'Introduction to the Theory of Ferromagnetism' by Amikam
15 Aharoni (ISBN 0 19 851791 2), pp. 204 - 214, gives a useful overview of many of the aforementioned concepts.

Figure 8a shows an idealised single hysteresis loop 160 indicating how the magnetisation M of a magnetic element 102 made from the permalloy material varies as a function of an applied magnetic field H. Dotted lines 169 indicate how the
20 idealised single hysteresis loop 160 may vary from the ideal for a real magnetic element 102. The magnetic element 102 starts with an initial magnetisation 172. The applied field H is increased until it reaches a value 170. Thereafter, the applied field H is increased to a switching value 168 where, due to hysteresis, the magnetic element 102 rapidly switches its magnetisation M from the initial magnetisation 172 to a
25 magnetisation 164. Thereafter, the applied field H is decreased to a switching value 174 where, due to hysteresis, the magnetic element 102 rapidly switches its magnetisation M from the magnetisation 164 back to the initial magnetisation 162.

As is observed from Figure 8a, the magnetic switching characteristics of the
30 magnetic element 102 made from permalloy material is seen to operate in the sharp switching mode, even when the real hysteresis loops deviate from the ideal, as the transitions of the magnetisation from one polarity to the other are still sharply defined.

Figure 8b illustrates an averaged hysteresis loop 180 for many (e.g. ~100) cycles of the magnetic element 102 made from the permalloy material around hysteresis loops of Figure 8a. It is observed that the averaged hysteresis loop 180 does not show sharp transitions in the state of magnetisation of the magnetic element 102, even though sharp transitions do occur for each individual magnetic cycle 160. The reason for this is because the switching values 168 and 174 of each individual magnetic cycle 160 vary between cycles which gives rise to jitter.

The magnitude Δ of the jitter 196, determined as the standard deviation of the differences in switching values 168 for the various magnetic cycles 160, is shown in relation to the averaged hysteresis loop 180. In turn, the jitter magnitude Δ provides a characteristic response for the magnetic element 102 that generates it. The magnitude of the jitter is dependent on the precise volume and energy of the nucleation centre that is responsible for magnetisation reversal. It therefore varies from one magnetic element to another, since no two nucleating defects are likely to be the same.

Coercivity is also a characteristic measurement that indicates uniqueness. In various embodiments coercivity provides for a better characteristic response than jitter. In such embodiments jitter can be measured as an additional characteristic response parameter. Viewed from one perspective, a distribution function representing the reversal/switching field (of a single magnetic element) as observed across many reversals/switchings has a central value of the distribution corresponding to the coercivity and a width distribution representative of the jitter.

Various embodiments of a security device incorporating magnetic elements can be provided. One process of manufacturing various of such security devices on a silicon substrate using optical lithography will now be described, by way of example.

The manufacturing process is illustrated in Figures 9a to 9h. The process starts in Figure 9a with a cleaned and polished silicon wafer 704. In various embodiments, the silicon substrate is approximately 0.5 mm thick in order to facilitate handling and

provide a rugged security device. A photoresist layer 714 is spun onto the wafer to provide a smooth coating as shown in Figure 9b. The wafer and photoresist layer 714 are then baked to set the photoresist layer 714.

5 Figure 9c illustrates the device of Figure 9b post-exposure to UV radiation or near-UV radiation (e.g. at 405 nm). The regions 708 represent exposed regions. The exposed regions 708 are directly written onto the upper surface 701 of the photoresist layer 714 using a commercially available direct write scanning optical lithography system such as, for example, a NanoMOKE2 system with a LaserWriter add-on
10 supplied by Durham Magneto Optics Ltd. In this way, an individual one-dimensional or two-dimensional pattern can be written into the photoresist layer 714 for each security device that is manufactured. This pattern may define a plurality of wire shapes, such as, for example, those illustrated in Figure 1.

15 Figure 9d shows the device of Figure 9c after it has been developed to remove exposed photoresist 708. Removal of the exposed photoresist 708 exposes portions 710 of the underlying silicon substrate 704.

 Subsequently, as shown in Figure 9e, magnetic elements 702 formed of a
20 permalloy material such as, for example, $\text{Ni}_{80}\text{Fe}_{20}$ (see, for example, Bozorth, Ferromagnetism, ISBN 0-7803-1032-2, for further information) are deposited in exposed portions 710 by a sputter deposition or evaporation process, typically to a thickness in the range from about 10 to about 100 nm, e.g. to about 40 nm. Further layers 712 of permalloy material also form on the remaining unexposed photoresist
25 706 during the sputter deposition process.

 Next, metal capping layers 716, 718 of gold or aluminium are formed over the permalloy layers 712 and magnetic elements 702, as illustrated in Figure 9f. The capping layer 718 is designed to protect the permalloy layer from oxidation and also
30 provides an enhanced optical reflectivity.

The unexposed photoresist 706 along with overlying permalloy layers 712 and capping layers 716 are removed using a suitable solvent, e.g. acetone, to leave the structure illustrated in Figure 9g. The resulting structure comprises the magnetic elements 702 formed on the silicon substrate 704 separated by exposed silicon substrate regions 720. The upper surfaces of the magnetic elements 702 are capped by capping layers 718.

The aforementioned resulting structure is placed into a plasma enhanced chemical vapour deposition (PECVD) chamber where a silicon dioxide (SiO_2) layer 722 is deposited upon the upper exposed silicon substrate regions 720 and capping layers 718. The silicon dioxide layer 722 forms an optically transparent layer (including, *inter-alia*, a layer that is substantially transparent to infra-red electromagnetic radiation). The resulting security device 700 is shown in Figure 9h.

Where several security devices 700 are manufactured upon a single silicon substrate 704, the silicon substrate 704 can subsequently be diced into a plurality of individual security devices 700.

The applicants have produced several prototype security devices using the process hereinbefore described. During production of these prototype security devices the sputter deposition process parameters used were as follows: 250W power setting; base pressure 5×10^{-7} mbar; Argon gas; gas pressure 1 to 2 mTorr; flow of 5 cc/minute; substrate rotation rate 10 rpm; deposition rate 1 to 1.5 Angstroms per second; and a substrate temperature of 22 to 27 °C. It is also possible to apply a magnetic field along the plane of the device during the manufacturing process.

The applicants note from an analysis of their prototype security devices, that fine tuning of the growth rate and/or sputter pressure for the magnetic elements can provide improvements to sharp switching mode magnetic switching characteristics. The applicants have also noted from an analysis of their prototype security devices, that magnetically soft materials tend to give rise to desirable magnetic switching properties.

Once a security device had been manufactured it is tested, either alone or as part of a batch of such security devices, to determine its characteristic response. The characteristic response is measured to ensure it provides for adequate identification of the particular security device.

Magnetic elements are first tested to determine whether or not they operate in the sharp switching mode. A Kerr magnetometer, as described in Applied Physics Letters, Vol. 73, p. 3947, 1998, is used to measure the coercivity at a number of points on each individual magnetic element. For example, five points on each element may be used and the coercivity measured at each point. Magnetically sharp switching is deemed to exist if the variation between measured coercivity values from one magnetic element is small compared with the variation between coercivities measured across a number of elements. In practice, magnetically sharp structures switch with less than 0.2 Oe variation across the element, while one element may differ in coercivity from another by approximately 1 - 2 Oe.

A jitter measurement may also be made for each magnetic element, or for a group of such elements, by repeating measurements on that element/group and determining how much the coercivity varies between sets of measurements. These sets of measurements are repeated many times for each magnetic element/group of the security device. In one example, coercivity may be measured at one point on a security device, one hundred times per each magnetic element/group of magnetic elements at room temperature. The measured coercivity values are then fitted to a Gaussian bell-curve, and the mean coercivity and jitter (as indicated by the mean and standard deviation Δ of the fitted Gaussian curve, respectively) calculated.

The applicants have found that for various embodiments, over a typical likely operating temperature (for example, from -20°C to 50°C where anti-misting measures are provided in a reader), jitter exhibited only a weak temperature dependency.

In various embodiments, there is a measurable dependence of mean coercivity on temperature. However, provided that the mean coercivity of a plurality of magnetic elements varies in the same way with temperature, the coercivity differences between magnetic elements remains almost constant. Thus, when comparing the measured mean coercivity against the premeasured characteristic response, an allowance may be made for a constant offset between the two sets to compensate for different temperatures.

However, if desired or required for various other embodiments, coercivity and jitter measurements may be made at several temperatures, including temperatures outside a normal operating temperature range. For example, sets of measurements could be made on each magnetic element at -50°C, 0°C and 65°C for a security device rated for operation from about -20°C to about 50°C.

In practice, an upper limit on the permitted variation allowed between the measured coercivity values measured for a single magnetic element should be set. This can be an absolute value (e.g. 0.2 Oe) or be determined relative to the jitter magnitude (e.g. 10% of the measured jitter value). Security devices having one or more magnetic elements that gave rise to coercivity variation values greater than the permitted variation should be rejected.

A desirable characteristic is that any variation due to jitter be small in order that the mean coercivity be easier to measure. Mean coercivity can then be used as a parameter for a premeasured characteristic response. Jitter may also be used as parameter for the premeasured characteristic response, e.g. in addition to mean coercivity for respective magnetic elements or groups of such elements.

In various embodiments, security devices may have their premeasured characteristic response defined by a mean coercivity value and/or a jitter value Δ , for various magnetic elements or groups of magnetic elements. Various other embodiments use, for example, either a mean coercivity value or a jitter value to represent a premeasured characteristic response. In use, the premeasured characteristic

response of a security device is compared to its measured characteristic response to determine if that security device is a forgery.

5 The premeasured characteristic response can be encoded, for example, by digitising the values of the mean coercivity and/or the jitter value Δ . In various embodiments, these values are stored in encrypted form upon the corresponding security device, either with or without an identifier that may be unique. In various other embodiments, these values are stored separately from the corresponding security device. In various embodiments, during a reading operation (as described below) the
10 digitised values of mean coercivity and/or jitter value Δ representing a premeasured characteristic response can be retrieved/recovered for a particular security device and compared to measured values of mean coercivity and/or jitter value Δ for a security device purporting to be the same device, so as to determine whether or not the security device whose characteristic response has been measured is a forgery.

15

Security devices may be attached to articles in order to aid in identifying such articles as genuine or non-counterfeit. In use it is necessary to read the characteristic response of a particular security device in order that it may be compared to a premeasured characteristic response, such as for example, a baseline response. Any
20 differences between the measured and premeasured response, outside of any allowable limits, indicate that the security device that has been read is a forgery. Since the production of magnetic nucleation centres is beyond the control of the manufacturer, any copying of the device will almost invariably result in a different characteristic response, such as, for example, mean coercivity and jitter values.

25

Various embodiments of systems, both hand-held or otherwise are envisaged. Various such embodiments are described below in connection with Figures 10 to 17 of the drawings.

30

Figure 10 shows a reading arrangement 930 forming a component of a security device reading system for obtaining a measured characteristic response of a security device 900 while the security device 900 is subject to an applied magnetic field 932.

The reading arrangement 930 can detect changes in the polarisation of light reflected from the magnetic elements using the magneto-optic Kerr effect (MOKE).

5 The reading arrangement 930 comprises an aluminium block 934 whose internal and external surfaces are blackened using a black matt anti-reflection paint. The size of the an aluminium block 934 is typically 2 cm x 2 cm x 1 cm. The aluminium block 934 comprises beam path channels 938, 940, 942. A near infra-red or visible laser diode 936, which is provided with collimating optics (not shown), is operable to produce a collimated laser beam 944 at a wavelength of, for example, 600
10 to 1550 nm. One embodiment uses a laser diode operating at 670 nm. The laser beam 944 passes though a first beam path channel 938, before it leaves the aluminium block 934 and is incident upon a mirror 950.

15 The laser beam 944 is reflected from the mirror 950 into a second beam path channel 940 formed in the aluminium block 934. A polariser 952 placed into the second beam path channel 940 converts the laser beam 944 into a plane polarised laser beam 947. The plane polarised laser beam 947 then leaves the second beam path channel 940.

20 The aluminium block 934 also comprises a third beam path channel 942. The third beam path channel 942 is oriented so as to collect reflected light 949 that is reflected from a security device 900 when being read. Typically, if a security device 900 has wire-shaped or flattened wire-shaped magnetic elements 902, the applied field 932 is applied in a direction substantially parallel to the axis of the magnetic elements
25 902.

30 An analyser 954, used in various embodiments, incorporating an optional quarter wave plate and polariser is placed into the third beam path channel 942. The analyser 954 passes light of a first polarity and blocks light of a second an orthogonal polarity. Light of the first polarity is reflected from a magnetic element 902 when it is in a first saturated magnetisation state, and light of the second polarity is reflected from the magnetic element 902 when it is in a second saturated magnetisation state

having a largely reversed polarity or modified intensity with respect to the first magnetisation state.

The polariser 952 and the analyser 954 are arranged to measure the longitudinal magneto-optic Kerr effect signal produced when the plane polarised laser beam 947 is incident upon the magnetic elements 902. Other magneto-optic Kerr effect arrangements, for example, including arrangements without a polariser and/or analyser and/or using a transverse or polar arrangement may also be used. However, a benefit of using a longitudinal magneto-optic Kerr arrangement is that it generally provides an improved signal as compared to transverse or polar arrangements.

Aligned with the third beam path channel 942 is a detector unit 956, which in this embodiment incorporates a focussing lens and a photodiode circuit or phototransistor circuit sensitive to illuminating radiation. The photodiode circuit is responsive to light transmitted through the analyser 954 to provide a signal proportional to the magnetisation of any magnetic elements 902 illuminated by the plane polarised laser beam 947.

Figure 11 shows a mirror actuator 969 for moving a mirror 950. Such a mirror actuator 969 may be used in conjunction with the reading arrangement 930 described herein. The mirror actuator 969 comprises an electromagnet 971 operable to deflect a mild steel deflecting element 982 attached thereto. The electromagnet 971 comprises a first actuator coil 986 wound onto a first region of a magnetic core 980, and a second actuator coil 988 wound onto a second region of a magnetic core 980. The magnetic core 980 includes a gap 992 at which, when the electromagnet is energised, a magnetic deflecting field is produced.

The deflecting element 982 is connected to the magnetic core 980 by way of a threaded bolt 984. Tightening of the threaded bolt 984 secures the deflecting element 982 to the magnetic core 980 proximal one end of the deflecting element 982. An unsecured end of the deflecting element 982 distal the threaded bolt 984 is thereby able to move with respect to the magnetic core 980 under the influence of the magnetic

deflecting field due to the attractive force generated between the magnetic deflecting field and the mild steel material of the deflecting element 982. The mirror 950 is mounted upon one part of the deflecting element 982 and moves in response to movement of the deflecting element 982.

5

In operation, an energising current is passed through the first and second actuator coils 986, 988. The first and second actuator coils 986, 988 can be connected in series such that the same energising current passes through both coils. Passing an initial energising current through the first and second actuator coils 986, 988, causes the deflecting element 982 to deflect in the direction shown by arrow 990, thereby also deflecting the mirror 950.

10

Figure 12 shows a field generation system 935, a detection system 937, a control and processing system 939 and a beam scanning system 941 forming, in conjunction with the reading arrangement 930 described above, a further part of one embodiment of a security device reading system.

15

The field generation system 935 comprises components for producing a time varying applied magnetic field 932 for applying to a security device 900. The field generation system 935 comprises a driver circuit 966 operable to drive field generation coils 933a, 933b in response to a coil driving signal 970. The coil driving signal 970 is a periodic sinusoidal signal composed of a plurality of individual sinusoidal waveforms 972 oscillating at a frequency of 100 Hz (see Figures 13 and 15), that drives the drive field generation coils 933a, 933b to produce a sinusoidally oscillating magnetic field oscillating at 100 Hz. In this embodiment, the 100 Hz sinusoidal waveform is produced by a conventional electronic oscillator circuit (not shown).

20

25

The field generation system 935 additionally comprises a cross-over detector 968 for detecting polarity changes in the coil driving signal 970. The cross-over detector 968 produces a synchronisation signal 981 in response to being driven by the driver circuit 966, as shown in Figure 17. The synchronisation signal 981 is composed

30

of a sequence of spikes 983 each produced at a time when the polarity of the coil driving signal 970 changes. In various other embodiments, the same microcontroller that logs the Kerr signal is used to generate the applied field sequence (via a Digital to Analogue Converter), so the microcontroller can control synchronisation therebetween.

The detection system 937 comprises detector unit 956 for producing a signal in response to incident light 948. The detector unit 956 is coupled to an amplifier 958. Signals produced by the detector unit 956 are amplified by the amplifier 958 to provide a unipolar detector signal 973 (see Figure 16). The unipolar detector signal 973 is then fed into an analogue to digital converter (ADC) 960 for digitisation. The ADC 960 is a 10 bit device operating at a 10 kHz sampling frequency; thereby giving 1024 possible discrete data levels for each of the 100 samples taken over the time taken for one cycle of a 100 Hz cycle to complete.

In one embodiment, the ADC 960 operates at 10kHz and acquires around 100 data points per applied magnetic field cycle. The applied field is applied at a frequency of around $10\text{kHz} / 100 = 100\text{ Hz}$. Data is averaged for around 0.5 sec, i.e. there are 50 data sets averaged for a single magnetic element. From this mean coercivity and jitter are measured. The process is then repeated for another magnetic element. In total around 8 magnetic elements are analysed in this way.

The control and processing system 939 is used to acquire measured data representative of the characteristic response of the security device 900 from the detection system 937, analyse that measured data and compare it with a premeasured characteristic response to determine if the security device 900 is genuine. In various embodiments, the control and processing system 939 also controls a beam scanning system 941 to cause the plane polarised laser beam 947 to move across the surface of the security device 900.

The control and processing system 939 comprises a processing unit 962 having an associated data store 974. In various embodiments, the processing unit 962

comprises a microprocessor or microcontroller and associated memory (not shown), including a ring buffer to which data samples from the ADC 960 are constantly fed when the ring buffer is enabled by the microprocessor.

5 When the security device reading system is started, the ring buffer is disabled by the microprocessor. In order to begin accumulating data into the ring buffer, a first spike 983 is received by the microprocessor. This triggers the microprocessor to begin a count of the number of synchronisation spikes 983 that are received and simultaneously to enable the ring buffer. Thus, data begins accumulating into the ring
10 buffer in synchronisation with a polarity transition occurring in the applied magnetic field 932. When the microprocessor detects the Nth spike 983 (e.g. the 100th), a signal is sent to inhibit further accumulation of data into the ring buffer. The ring buffer at this time will contain N sets of data each accumulated during one half cycle of the applied magnetic field 972, with each set of data representing a digitised
15 respective portion 975, 977 of the unipolar detector signal 973 at a respective time during the time duration t ($t = N \times \text{applied magnetic field frequency} / 2$) of the data accumulation. (e.g. $t = 0.5$ second duration for 100 cycles at 100 Hz with $N=100$, and 5,000 individual measurements are made with an ADC rate set to 10 kHz).

20 For an embodiment that includes a beam scanning system 941 coupled to a mirror actuator 969, a processing unit 962 can also be used to provide control signals for moving the position of a mirror 950. The beam scanning system comprises a driver circuit 964 which includes a digital to analogue converter which sets the current provided through the first actuator coil 986 and the second actuator coil 988. The
25 switching circuitry is configured to connect the first and second actuator coils 986, 988 in series, and to apply a driving current in proportion to a control voltage 994 (see Figure 14) provided by the processing unit 962.

30 In one embodiment, the ring buffer accumulates several sets comprising N sets of data. Once a set of N sets of data has been accumulated, the ring buffer is disabled by the microprocessor until the N sets of data have been stored in the store 974. The processing unit 962 then increases the control voltage 994 to cause the mirror 950 to

deflect a plane polarised beam 947 onto a further area of the security device 900. After a short delay period to allow the mirror actuator 969 to settle, the microprocessor awaits a first spike 983 and subsequently begins to acquire the next N sets of data. This process continues until N sets of data have been accumulated and stored for each position of the mirror 950.

As indicated above, data sets can be accumulated in a variety of manners. Once acquired, the data can be processed to extract a variety of information regarding the measured characteristic signal response. Standard algorithms can be applied to the data sets to calculate the mean measured coercivity and/or jitter as given by a measure of the standard deviation of coercivity measurements. Examples of such algorithms may be found, for example, in "Numerical Recipes in C: The Art of Scientific Computing," W. H. Press, S. A. Teukolsky, W. T. Vetterling and B. P. Flannery, (Cambridge University Press, Cambridge, 1993).

Data fitting can either be done by the same microprocessor/microcontroller that determines the measured characteristic signal response, or by a connected computer system. For example, where a remote data base stores the premeasured characteristic response, raw measured characteristic signal response data can be transmitted to a remote processor to perform a Gaussian fitting. Similarly, where used as part of a fraud detection system, a reader may be connected to a Palm-top computer which stores premeasured characteristic response data by downloading it from the internet, and compares it to the measured characteristic signal response. In various embodiments, Palm-top computers can be used as the interactive display of the reader and also as a means of accessing remote data bases, e.g. by using GSM telephones.

Various ways exist for determining the premeasured characteristic response of a security device. These ways vary according to the type of security device and depend, for example, on whether or not the premeasured characteristic response is stored/encoded on the security device; whether or not the premeasured characteristic response is encrypted; and whether or not a unique identifier is provided in association with the security device. All these possibilities provide feasible embodiments.

In various embodiments, a unique identifier and an encrypted premeasured characteristic response, comprising encoded data representing a mean coercivity and a standard deviation in measured jitter, are encoded onto a security device as a sequence of pits. The pits are formed in a direction co-linear with a beam scanning direction, as provided by a beam actuator 969. Prior to determining the measured characteristic response, the beam actuator 969 is driven to provide a beam at points on the security device where the pits are anticipated to be. At each such point, a signal from detector unit 956 is measured. High reflectivity indicates a logical zero for the data bit corresponding to the respective point, and low reflectivity indicates a logical zero.

Of course, the plane polarised laser beam 947 of various embodiments may be focussed using a lens system to provide a small focal spot size at a security device 900. Similarly, collecting optics may be provided in the beam path channel 942 to aid in collecting light reflected from the security device 900.

In various other embodiments, a smart card carries a security device and unique identifier and an encrypted premeasured characteristic response information are stored in the smart card. The smart card is read in a conventional manner and a measured characteristic response is measured as herein described.

In certain embodiments the magnetic elements of a security device themselves may be used to encode further information. They can, for example, encode a unique identifier by forming a pattern of shapes. Such security devices may be scanned to see firstly if any magnetic elements are present at various possible locations. A linear scan pattern of reflected signal can then be used to obtain a binary value identifier for the security device. A way of visualising this is to consider the pattern of the magnetic elements to represent a form of bar code.

For embodiments of a security device comprising magnetic elements that encode a unique identifier, a characteristic response may be measured, as hereinbefore described, for each individual element. Various readers may however only measure

the characteristic response for a subset of the magnetic elements in order to speed up the reading process.

In an embodiment of a security device reading system, premeasured
5 characteristic response information is stored in a database to which one or more processing units have access. The premeasured characteristic response information is preferably encrypted. Such a system may be distributed and comprise a remote server coupled through a network to one or more security device readers. A system according to this embodiment is operable to determine a unique identifier for each
10 security device from the pattern of the magnetic elements, or by other means, and to retrieve premeasured characteristic response information corresponding to the unique identifier determined by the security device reading system. The premeasured characteristic response information can then be decrypted as necessary by a respective security device reader.

15

In embodiments of the security device reading system, once the information regarding the measured characteristic signal response has been extracted it is compared by the microprocessor to the premeasured characteristic response, possibly decrypted using a private asymmetric data key, to determine whether or not the security device
20 can be classed as non-counterfeit. Such a comparison is made within a margin of error allowed for variations that are introduced, for example, by temperature fluctuations. For example, for mean coercivity/jitter this may be when the measured coercivity/jitter does not differ from the premeasured coercivity/jitter by more than one standard deviation of the distribution of mean coercivity/jitter values.

25

Referring to Figures 18 to 20, illustrations of three example structures of magnetic elements are provided in plan view.

In the first, a collection of regular rectangular magnetic elements (1) is shown
30 schematically and not to scale. The material of the elements is $\text{Ni}_{80}\text{Fe}_{20}$. The material is laid down to a thickness of 40 nm. The overall area of the signature portion is 1 mm by 1 mm. The illustration is schematic only and not to scale. In particular it should be

appreciated that each 1 mm by 1 mm area will comprise a very large plurality of elements of micron-scale width.

Moreover, any representation that the elements are of equal widths is schematic only. An array of 1 μ m wide wires might be suitable for some applications. However, as has been noted above, any array of discrete groups of different wire width giving several discrete switching fields (for example as above described), or a continuously varying array with width varying in linear or other functional manner (for example as above described), will often be preferred.

10

Figure 19 shows a generally similar structure having generally similar dimensions. The caveats above about the schematic nature of the illustrated widths again applies. However, in this instance, the rectangular portions (2) do not have square ends, but are provided with pointed ends. Differently shaped ends can affect the switching field and thus be preferred for certain applications. Any suitable end shape can be made use of without departing from the principles of the invention.

On Figure 20 a yet further alternative is shown, the signature portion comprising a generally square 1 mm by 1 mm array of circular magnetic microdots (3). In this instance material thickness is around 100 nm. Each microdot is 100 μ m in diameter. Again this is illustrative only. Alternative shapes can be considered, and again elements of discretely or continuously varying size and/or shape, provided the basic requirement for a device in accordance with the invention that a reproducibly measurable baseline signature response is obtainable is met.

25

The film is laid down by any suitable method, in particular by optical lithography such as using the method herein described.

Figure 21 illustrates a mechanical drawing of an example of a small device suitable for measuring the magnetic response of a small area of thin magnetic film, such as a magnetic film comprising a magnetic signature in accordance with the invention, for example the signatures illustrated in Figures 18 to 20.

30

The device to measure the magnetic response comprises a high intensity light source, in this instance an infra-red light emitting diode within the housing (11). The light is collimated by a single pin-hole (12), of diameter in the size range 0.2 mm – 5 mm. The light is then reflected off the surface of the magnetic thin film placed in position (15) against it and passes through a second pin-hole (13), with diameter in the size range 0.2 mm – 5 mm, and preferably of the same diameter as the first pin-hole.

The reflected light then passes into a light sensitive device within the housing (14), which is by preference a phototransistor or photodiode sensitive to infra-red radiation. In this illustrated embodiment the light sensitive device is selected to have low sensitivity to visible light, allowing the device to be used without optical screening. The device may also be painted black to reduce stray light reflections.

Magnetic field coils (not shown) are attached to the device to apply magnetic fields in the range 0-500 Oe to the magnetic material under test. In the case of the magnetic material under test comprising an array of elongated elements, such as rectangles, by preference the magnetic field coils are oriented so as to apply a field in the plane of the film and either along the long-axis of the elongated structures or at an angle to the long-axis in the range 0° - 60°. Additional magnetic field coils can be present to apply an additional field transversely to the long-axis of the wire.

The phototransistor or other light receiving device is connected to suitable electronics (not shown) which record the reflected intensity from the magnetic material while an alternating current is passed through the coils generating the applied magnetic field. Signal processing electronics using a Digital Signal Processor chip or a Microcontroller chip record measured responses over a number of cycles of the applied magnetic field and add them together coherently to reduce noise. The number of cycles recorded will be such that the total acquisition time does not exceed 10 seconds, and for convenience will not exceed 5 seconds. The signal processing electronics then identifies the mean switching field for each of the major switching transitions in the recorded signal. These are then passed to other electronics (not

shown) which acquire and if necessary deciphers the prerecorded baseline response from a magnetic strip, smart card, optical bar code, or from a remote textual source or electronic data store or other means, or alternatively transmits the measured response to a remote data comparator having access to the prerecorded baseline response, and a
5 comparison is made.

Figure 22 illustrates the application of the present invention to a smart chipped card of otherwise generally conventional design. The card (21), typically sized and shaped as a credit card or the like, and which may indeed be used as a credit card or
10 the like, is illustrated in plan view both from above (A) and from below (B). The card carries some alphanumeric information, but its main information storage system is the smart chip (22). This is backed up by optional bar code (23), and magnetic stripe (24) which is typically provided for backward compatibility with magnetic stripe only systems.

15

A magnetic signature device (26) comprising a 1 mm by 1 mm array of magnetic elements of appropriate design in accordance with the invention is applied on the rear of the smart card. For convenience, in the example shown, it sits within the foot print of the smart chip itself as illustrated by the broken line (28). For many
20 applications it might be convenient to sit the magnetic element (26) within this footprint. An alternative approach to achieve the same effect might be to incorporate the relatively small 1 mm wide magnetic signature device into a specially enlarged space between contacts on the smart chip. However, such placement is purely for convenience, and the magnetic elements (26) could be placed elsewhere on the card.

25

At the time of manufacture of the card an initial baseline signature reading is taken. One way of doing this is to use a scanning magnetometer. In the illustrated embodiment of a smart card, the baseline response is stored on the card, having first been digitally signed using an asymmetric encryption algorithm such as RSA. The
30 public key can then be made available to a user and/or stored on a reader terminal or even on the card itself without compromising security. The signature can then be used to verify that the card is a genuine product of the manufacturer, and to eliminate the

threat of fraudulent misuse of cloned copies of the card, which constitutes an increasing source of both financial transaction fraud and identity fraud.

In use, the card is read by a suitable card reader, in particular by a card reader
5 incorporating a signature device reader such as that illustrated in Figure 21. The
device reader may be incorporated into an existing smart card reader. For example,
with the embodiment shown, the reading device for the magnetic element needs to
read opposite side of the card from that read by the smart card reader, and so can be
incorporated into a conventional smart card reader with relatively little engineering
10 difficulty. In this way, cards and readers remain backwards compatible to
conventional card/reader technology not having the identification and authentication
system herein described.

The reader measures an actual response from the card. An expected baseline
15 response is also stored upon the card. This can be stored in any readable form, but is
conveniently incorporated into the card in one of the existing data storage devices. For
example, the baseline signature may be recorded in its encrypted form on the smart
chip (22), the bar code (23) or the magnetic strip (24). The reader is thus able to read
both the actual magnetic signature and the predetermined and prerecorded expected
20 magnetic signature. The reader is adapted to compare these, within certain tolerance
limits, and to indicate whether the card is authenticated or not as a result of that
comparison.

The smart card in accordance with various embodiments of the invention will
25 be applicable to all circumstances where conventional smart card technology is being
used, including without limitation bank and credit cards, secure information storage
cards, identification and authentication cards and the like. It provides a means of
authenticating the card as genuine, and thus provides a significant obstacle to
fraudulent misuse of counterfeit copies of original cards.

30

The system represented by the embodiment in Figure 22 is a simple system, in
which a device in accordance with various embodiments of the invention serves

merely to authenticate the card as a genuine manufactured product and thus to detect counterfeit copies, and in consequence the predetermined baseline response is conveniently stored upon the card. It will be readily understood that such a system is only an example mode of operation. In one alternative, the original "expected" signature could be stored elsewhere. For example, in relation to the use of a card as illustrated in Figure 22 as part of a financial services system, for example as a credit card, a system can be envisaged where a plurality of cards are in issuance, where a plurality of readers are in use, and where the readers comprise a distributed network with a central data store such as will already hold customer details being further adapted to process signature information for verification purposes in accordance with the principles herein described. Other modes of operation will also readily suggest themselves.

In Figure 23 an illustration is provided of the use of an embodiment of the present invention in a lock and key arrangement. A key card (31) of suitable robust material, for example of a suitable plastic material, is provided with a device (36) comprising a 1 mm by 1 mm array of magnetic elements as previously described.

The key card is provided in association with a card reader/lock arrangement illustrated schematically by the remainder of Figure 23.

The lock (32) incorporates a slot (33) into which the end of the key card (31) can be received. When appropriately positioned therein, the device (36) sits adjacent a reader (34) of the general design illustrated in Figure 21.

The reader (34) obtains a reading of the magnetic response from the device (36) in the predescribed manner, and passes this response to a control unit (35). The control unit (35) stores or otherwise has access to the predetermined expected response, for example storing this within the lock, optionally in encrypted form. It effects the comparison, and in the event that a match is found within predetermined tolerances, passes an instruction to the control means (38) to actuate the lock levers (39) and open the lock.

Although the example illustrated in Figure 23 is an electromechanical lock, it will of course be understood that the principles of the present invention are equally applicable to all circumstances where a physical or a virtual locking means or other means of access control might be considered. For example, without limitation, a device along the lines of the embodiment illustrated in Figure 23 could be used in conjunction with an electronic lock for a door or other closure, in conjunction with an electronic ignition for a vehicle, in conjunction with an electronic immobiliser for a vehicle, as a means of controlling access to a piece of electronic equipment, for example by requiring insertion before the equipment operates, as a means of restricting access to a particular service etc.

In the illustrated embodiment, a single card is illustrated in association with the lock. In practice, even for simple single-user locks it is likely to be necessary to provide several keys. It is in the nature of the present invention that these will inherently have different signature devices. Accordingly, the lock would need to store and respond to baseline signatures for each of these devices. More complex modes of operation can also be envisaged where a lock provides for access for a plurality of users, or indeed where a plurality of locks are provided in association with a plurality of users.

In a first example of such operation, a plurality of locks and a plurality of keys are provided in association with a multiple use entry system into a secure area. In a second example of such a mode of operation, a plurality of operator cards are provided to control operation of multiple user office equipment. In these examples, all authorised base line signatures may be stored on each lock, or alternatively the locks may be linked together on a distributed network to a central database storing details of the cards of all authorised users. Such a system allows not only good security because of the difficult of producing counterfeit cards, but also allows control and monitoring of access in an active way.

A further embodiment of the invention is illustrated in Figure 24. In Figure 24, a signature device in accordance with the invention (46) is incorporated on a label attachable to an item to be identified/protected. The label comprises a plastic tab (41) which optionally incorporates alphanumeric information; a bar code (44) etc. to store, for example identification information, information of origin, pricing information or the like about item to be labelled. The tab (41) is attached to an item to be labelled by the attachment strap (42). In the embodiment illustrated, the attachment strap (42) is intended as a simple loop attachment. Attachment may be releasable or permanent. Where security and permanence of attachment of the label are of particular importance a more complex attachment would be readily envisaged which might for example include locking mechanisms, tamper prevention mechanisms, tamper indication mechanisms and the like.

The embodiment of Figure 24 allows labelling of items in either a temporary or permanent manner where it is not practical or desirable to incorporate a device in accordance with the invention directly onto the item itself. Example modes of use include without limitation improved security airline luggage labels, authenticity labels for high value branded items, in particular clothing and the like; origin and identity labels for the same, for stock control purposes, and for example for identifying original and hence controlling unauthorised importation of genuine branded articles intended for another market; marking of items for stock control purposes; price marking of items, labels being used in such a way as to make it difficult for a purchaser to transfer a (lower) price label from another item to obtain goods at a fraudulently low price.

The normal mode of operation of a label of the type illustrated in Figure 24 will be authentication. Accordingly, the prerecorded signature information will usually be stored on the tab (41). The prerecorded information will be stored in any suitable machine readable form. In the example given it could be incorporated in the bar code. A reader will be provided adapted to read both the magnetic signature of the device (46) and the encrypted expected signature, and to effect a comparison to authenticate the label. The security effectiveness of the label lies in that it is very difficult to copy,

since the random nature of the signature means that a copied label will be immediately identifiable as such.

Figure 25 illustrates a data storage disk such as a CD, DVD or the like to which
5 a device in accordance with the invention has been applied. The disc (51) incorporates a magnetic signature tab (56) comprising magnetic elements as above described preferably within the dead area (53) not otherwise carrying data. An encrypted predetermined reading of the signature (56) is provided elsewhere on the disc.

10 At its simplest, in a first mode of operation, the system allows the manufacturer to authenticate original CDs/DVDs, to identify counterfeit copies, and in association with a suitable stock control system to track origin and destination of genuine originals, and to identify unauthorised importation and the like.

15 In a more advanced mode of operation, disc readers can be manufactured which incorporate device readers to read the device (56) and to authenticate the disc, and which will be disabled from playing unauthorised copies. It is also possible to envisage a system whereby such modified players can be used in conjunction with the identification/ authentication system of the invention as part of an end user licence
20 arrangement.

Figure 26 is an example of the use of the invention on a formal identification document. Such a document might be an identification or authorisation document, such as a passport, driver's licence, authorisation or qualification certificate or the like,
25 an identity or authorisation certification intended to accompany, verify or otherwise identify an article, or any other document where counterfeit copies might be a problem.

The document (61) in the example includes visual information (62), for
30 example a photograph, written information (63), and a bar code (64). It might include other data storage or security devices.

A device comprising magnetic elements as above (66) is incorporated into the document. This device is readable in the manner above described. In one mode of operation, the device (66) serves a simple authentication purpose, and an encrypted prerecorded reading of its expected magnetic response is also incorporated into the document. Conveniently in the example given this could be incorporated into the bar code, or otherwise stored in a readable form. However, it will be appreciated that in more sophisticated systems it would be possible to store the expected magnetic signature remotely, optionally with further identification and/or other security details.

10 The device in accordance with the invention applied to documentation in this way serves primarily as a form of copy protection. It therefore serves as a cheap and convenient authentication device in all circumstances where there is a vulnerability to fraud arising from the counterfeiting of genuine originals, for example in relation to identification documents, formal certificates, financial paperwork such as cheques,
15 paper money and the like, important legal documents, and other such documentation.

Viewed from another aspect, there is provided a security device means comprising at least one magnetic element means, wherein said magnetic element means is responsive to an applied magnetic field to provide a characteristic response.

20 Viewed from a further aspect, there is provided a method of manufacturing a security device, comprising the step of providing at least one magnetic element, wherein said at least one magnetic element provides a characteristic response in response to an applied magnetic field.

25 Viewed from yet another aspect, there is provided a system for reading a security device means, comprising: a magnetic field generation means for applying an applied magnetic field to a security device; and a detection means for measuring one or more parameter representative of a measured characteristic response of said security device in response to said applied magnetic field, wherein said system is operable to
30 compare said parameter(s) representative of a measured characteristic response to one

or more respective parameter(s) of a premeasured characteristic response to determine whether respective of said parameters are substantially equivalent.

Viewed from another aspect, there is provided a method for reading a security device, comprising the step of applying an applied magnetic field to a security device; the step of measuring one or more parameter representative of a measured characteristic response of said security device in response to said applied magnetic field; and the step of comparing said parameter(s) representative of a measured characteristic response to one or more respective parameter(s) of a premeasured characteristic response to determine whether respective of said parameters are substantially equivalent.

Viewed from a further aspect, there is provided a product means comprising the security device means as herein described.

15

Those of ordinary skill in the art will realise that other techniques may be used to produce security devices. For example, instead of producing security devices using a lift off/wet etching process, ion beam etching may be used. Those of ordinary skill in the art will also be aware that various embodiments of security devices can be manufactured using various substrates, including, for example, silicon, glass, plastic, metals etc.

While certain of the example materials described herein are ferromagnetic, those skilled in the art will realise that other types of magnetic and/or non-magnetic elements may be used provided they give rise to a suitable measurable characteristic response. For example, non-magnetic elements may be used where such elements produce a measurable response in an applied magnetic field, where that response can be measured to provide a characteristic response.

Those of ordinary skill in the art will be aware of various techniques that can be used to manufacture and characterise magnetic elements suitable for security devices. An example of one such manufacturing technique and one such characterisation process can be found in "Optimised process for the fabrication of mesoscopic magnetic structures," Adeyeye *et al*, Journal of Applied Physics, Vol. 82, No. 1, pp. 469-473, 1 July 1997, which investigated the effect of magnetic element size upon the magnetic properties thereof.

Embodiments produced in accordance with the invention may incorporate reflectivity/contrast enhancement measures either alone, or in any combination. Materials such as gold, aluminium, chromium and/or tantalum can be laid beneath and/or above magnetic elements to enhance their reflectivity and/or the Kerr signal that the magnetic elements provide. Areas of a security device may be treated to reduce their reflectivity in order to improve the reflectivity/contrast between the magnetic elements and their surrounding areas.

In various embodiments, magnetic elements in the shape of wires or flattened wires are provided. The end shape of such wires can be controlled during manufacture of a security device. An angled end, for example, from about 60° to about 90° may be provided. In various other embodiments flattened ends and/or semi-circular ends may be provided to influence magnetic nucleation. The shape of the ends may be chosen to provide improved magnetic switching characteristics.

Although the invention has been described in relation to particular embodiments, it will be appreciated that the invention is not limited thereto, and that many variations are possible falling within the scope of the invention.

It will be appreciated that certain of various embodiments of the invention described above are implementable and/or configurable, at least in part, using a data processing apparatus, such as, for example, hardware, firmware and/or a computer configured with a computer program. The computer program can be stored on a carrier medium in data processing apparatus usable form. The carrier medium may be,

for example, solid-state memory, optical or magneto-optical memory such as a readable and/or writable disk for example a compact disk and a digital versatile disk, or magnetic memory such as disc or tape, and the data processing apparatus can utilise the program to configure it for operation. The computer program may be supplied
5 from a remote source embodied in a carrier medium such as an electronic signal, including radio frequency carrier wave or optical carrier wave.

Those of ordinary skill in the art will be aware that the description herein relates merely to illustrative examples of how the invention may be put into effect, and
10 that many embodiments incorporating one or more components, e.g. of other embodiments, can be envisaged, along with further embodiments not explicitly described herein. For example, data acquisition rates, sample rates, the number and size of sample quantisation levels, applied magnetic field cycling rates, the number of accumulated data sets, etc. may all be varied/selected as desired. Such parameters may
15 be varied programmably, for example, under the control of a microprocessor, possibly in dependence upon various measured conditions, such as, for example, temperature.

The scope of the present disclosure includes any novel feature or combination of features disclosed herein either explicitly or implicitly or any generalisation thereof
20 irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The applicant hereby gives notice that new claims may be formulated to such features during the prosecution of this application or of any such further application derived therefrom. In particular, with reference to the appended claims, clauses, aspects and paragraphs, features from
25 dependent claims, clauses, aspects and/or paragraphs may be combined with those of the independent claims, clauses, aspects and/or paragraphs and features from respective independent claims, clauses, aspects and/or paragraphs may be combined in any appropriate manner and not merely in the specific combinations enumerated.

CLAIMS

1. A security device comprising at least one magnetic element, wherein said at least one magnetic element is responsive to an applied magnetic field to provide a characteristic response.
- 5 2. The security device of Claim 1, wherein said at least one magnetic element is supported by a substrate.
3. The security device of Claim 2, wherein said at least one magnetic element is supported on said substrate.
4. The security device of any preceding Claim, wherein said at least one
10 magnetic element is responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of said at least one magnetic element.
5. The security device of any preceding Claim, wherein said at least one magnetic element is made from a material that operates in a sharp switching mode.
6. The security device of any preceding Claim, wherein said at least one magnetic
15 element is made from a magnetically soft material.
7. The security device of Claim 6, wherein said at least one magnetic element comprises a magnetically soft material selected from one or more of: nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.
- 20 8. The security device of Claim 6 or 7, wherein said magnetically soft material is a permalloy material.
9. The security device of any preceding Claim, wherein said at least one magnetic element is substantially wire-shaped or flattened wire shaped.
10. The security device of any preceding Claim, wherein said at least one magnetic
25 element is backed by a light reflective layer.

11. The security device of any preceding Claim, wherein said at least one magnetic element is provided proximal a reduced light reflectivity portion of said security device.
12. The security device of any preceding Claim, comprising a plurality of said at least one magnetic elements.
13. The security device of Claim 12, wherein said plurality of magnetic elements is arranged to provide a linear pattern.
14. The security device of Claim 12, wherein said plurality of magnetic elements is arranged to provide a two-dimensional pattern.
15. The security device of Claim 13 or Claim 14, wherein said pattern encodes an identifier.
16. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.
17. The security device of claim 16, wherein said unique identifier is provided by way of one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.
18. The security device of claim 17, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.
19. The security device of any preceding Claim, wherein premeasured characteristic response information representing one or more measurable parameters of said characteristic response is stored on said security device.
20. The security device of Claim 19, wherein said premeasured characteristic response information is in encrypted form.
21. A method of manufacturing a security device, comprising:
 - providing at least one magnetic element, wherein said at least one magnetic element provides a characteristic response in response to an applied magnetic field.

22. The method of Claim 20, comprising providing said at least one magnetic element on a substrate.
23. The method of Claim 21 or Claim 22, comprising forming said at least one magnetic element using a lift-off or wet etching process.
- 5 24. The method of Claim 21 or Claim 22, comprising forming said at least one magnetic element using an ion beam etching process.
25. The method of any one of Claims 21 to 24, comprising measuring the magnitude(s) of one or more magnetic parameters of said at least one magnetic element.
- 10 26. The method of Claim 25, comprising measuring one or more of coercivity and jitter values.
27. The method of Claim 25 or Claim 26, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.
- 15 28. The method of Claim 27, comprising encrypting said premeasured characteristic response information.
29. The method of Claim 27 or Claim 28, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.
- 20 30. The method of Claim 27 or Claim 28, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.
31. The method of Claim 30, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.
- 25 32. The method of any one of Claims 21 to 31, further comprising providing said security device with a unique identifier.

33. The method of Claim 32 when dependant upon any one of Claims 28 to 31, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.
34. A system for reading a security device, comprising:
- 5 a magnetic field generation system for applying a magnetic field to a security device; and
- a detection system for measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field,
- 10 wherein said system is operable to compare said one or more parameters representative of a measured characteristic response to one or more respective parameters of a premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.
35. The system of Claim 34, wherein the magnetic field generation system is
- 15 operable to apply a time varying magnetic field to a security device.
36. The system of Claim 34 or Claim 35, wherein a light beam is used to interrogate said security device.
37. The system of any one of Claims 34 to 36, wherein said light beam is a visible or near-infrared beam produced by a laser diode.
- 20 38. The system of any one of Claims 34 to 37, wherein said parameters represent one or more of coercivity and jitter values.
39. The system of any one of Claims 36 to 38, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for detecting changes induced in said light beam by magnetic elements of said security device.
- 25 40. The system of Claim 39, wherein said magneto-optic Kerr effect detection apparatus is configured to operate in transverse mode.
41. The system of any one of Claims 36 to 40, further operable to deflect said light beam across the surface of said security device.

42. The system of any one of Claims 34 to 41, further operable to read a unique identifier from said security device.

43. The system of Claim 42, wherein said unique identifier is identified by recognising a pattern of magnetic elements supported by said security device.

5 44. The system of Claim 42 or 43, wherein said unique identifier is identified by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

45. The system of any one of Claims 34 to 44, further operable to determine said one or more respective parameters of the premeasured characteristic response by
10 reading said one or more parameters from said security device.

46. The system of any one of Claims 34 to 45, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

47. The system of Claim 46, wherein said database is remotely located from said
15 detection system.

48. The system of any one of Claims 34 to 47, further operable to decrypt premeasured characteristic response information where it is read or provided in encrypted form.

49. A method for reading a security device, comprising:
20 applying a magnetic field to a security device;
measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field; and
comparing said one or more parameters representative of a measured
characteristic response to one or more respective parameter(s) of a premeasured
25 characteristic response to determine whether respective measured and premeasured
parameters are substantially equivalent.

50. The method of Claim 49, comprising applying a time varying magnetic field to a security device.

51. The method of Claim 49 or Claim 50, wherein measuring of one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field comprises measuring one or more of coercivity and jitter values.
52. The method of any one of Claims 49 to 51, comprising interrogating said security device using a light beam.
53. The method of any one of Claims 49 to 52, comprising operating a laser to produce a visible or near-infrared beam.
- 10 54. The method of Claim 52 or Claim 53, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.
55. The method of Claim 54, comprising using the magneto-optic Kerr effect transverse mode.
- 15 56. The method of any one of Claims 52 to 55, comprising deflecting said light beam across the surface of said security device.
57. The method of any one of Claims 49 to 56, comprising reading a unique identifier from said security device.
58. The method of Claim 57, comprising identifying said unique identifier by
20 recognising a pattern of magnetic elements supported by said security device.
59. The method of Claim 57 or 58, comprising identifying said unique identifier by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.
60. The method of any one of Claims 49 to 59, comprising determining said
25 respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

61. The method of any one of Claims 49 to 60, comprising determining said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.
62. The method of Claim 61, comprising accessing a database remotely located
5 from said detection system.
63. The method of any one of Claims 49 to 62, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.
64. A product comprising the security device of any one of Claims 1 to 20.
- 10 65. The product of Claim 64, comprising one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging; an item of clothing; an item of footwear; a smart-card; a credit or bank card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.

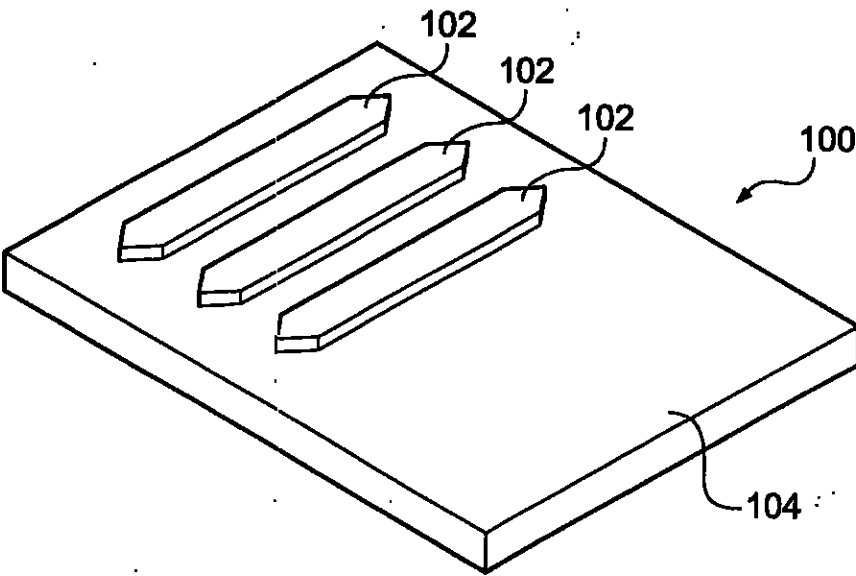


Fig. 1

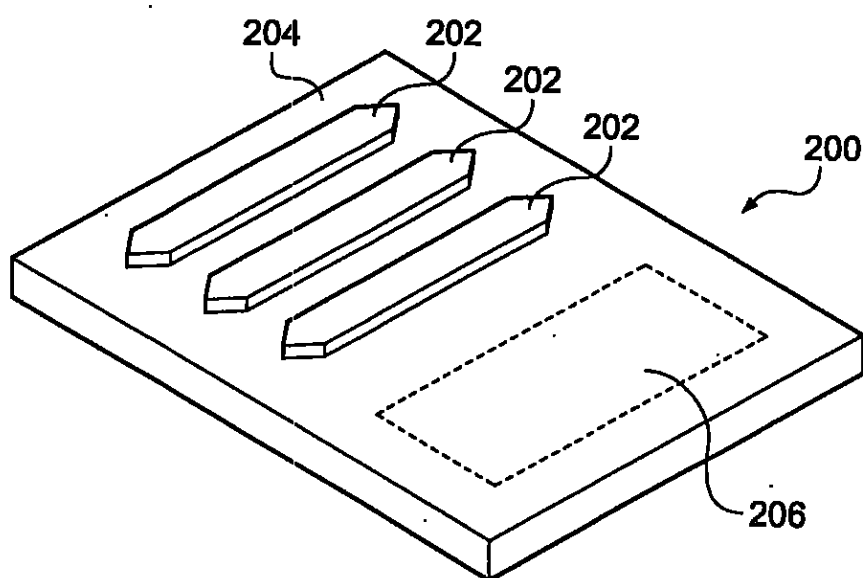


Fig. 2

SUBSTITUTE SHEET (RULE 26)

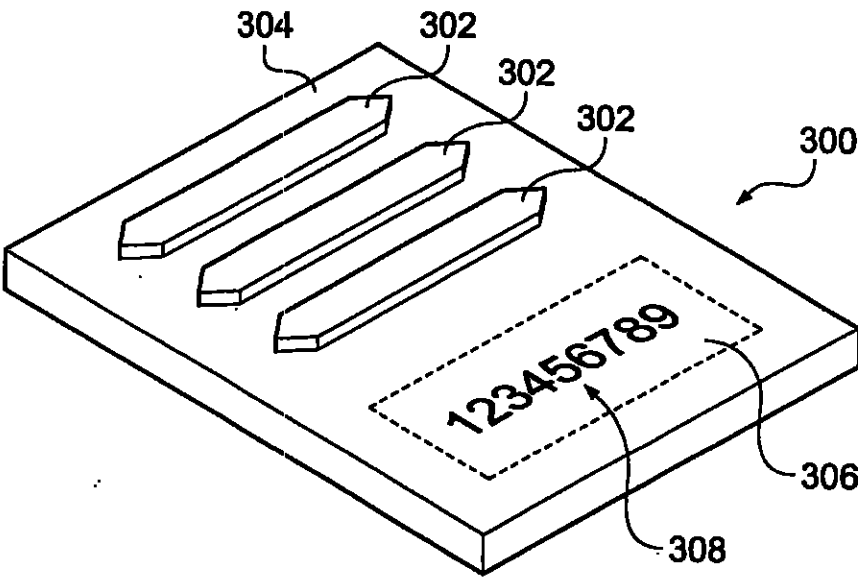


Fig. 3

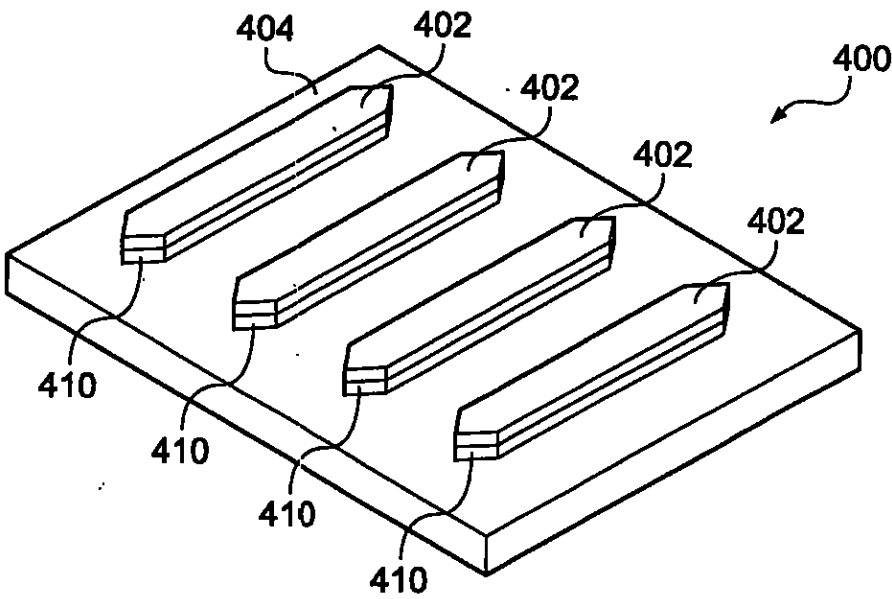


Fig. 4

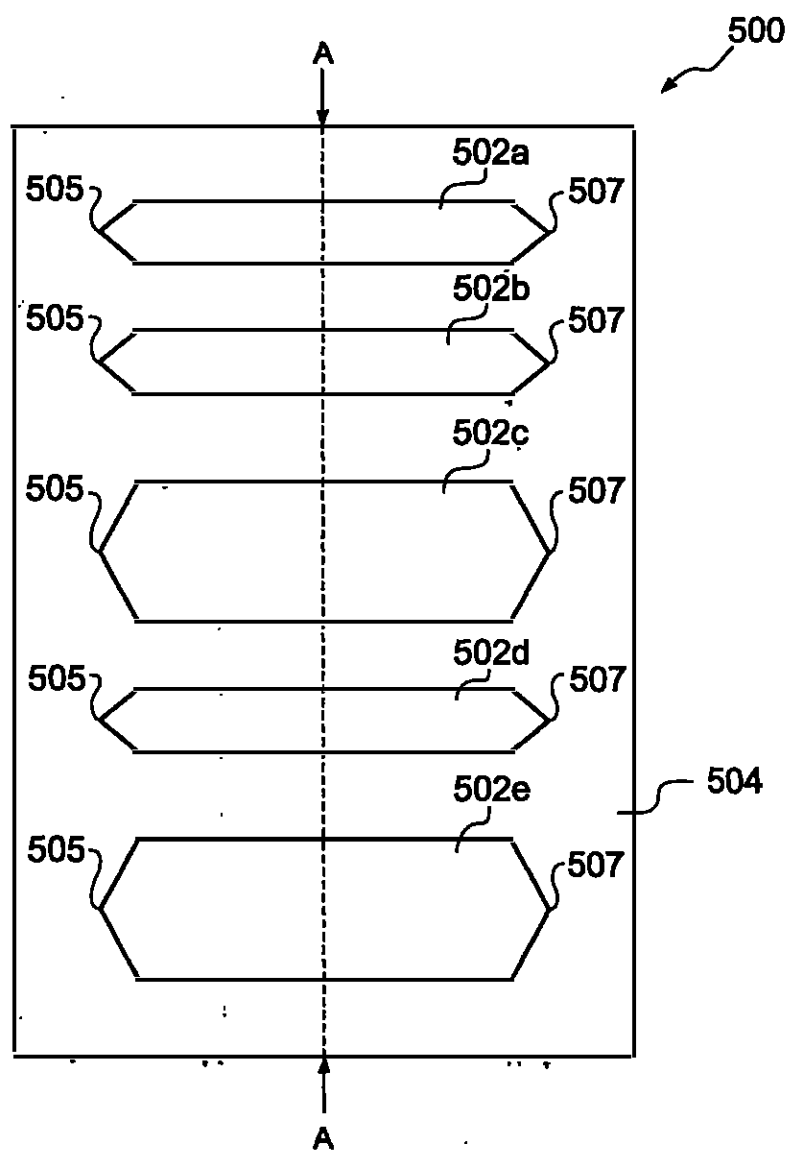


Fig. 5

SUBSTITUTE SHEET (RULE 26)

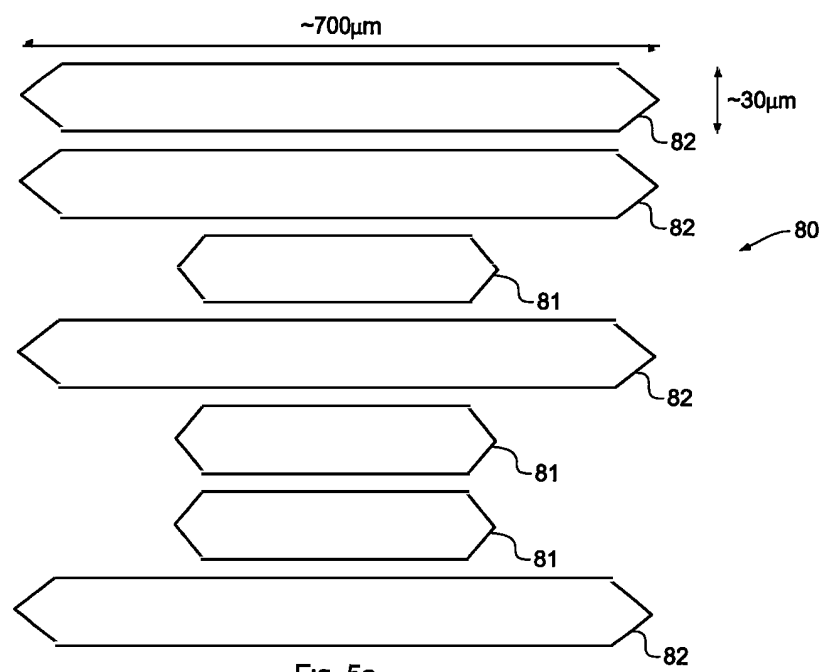


Fig 5a

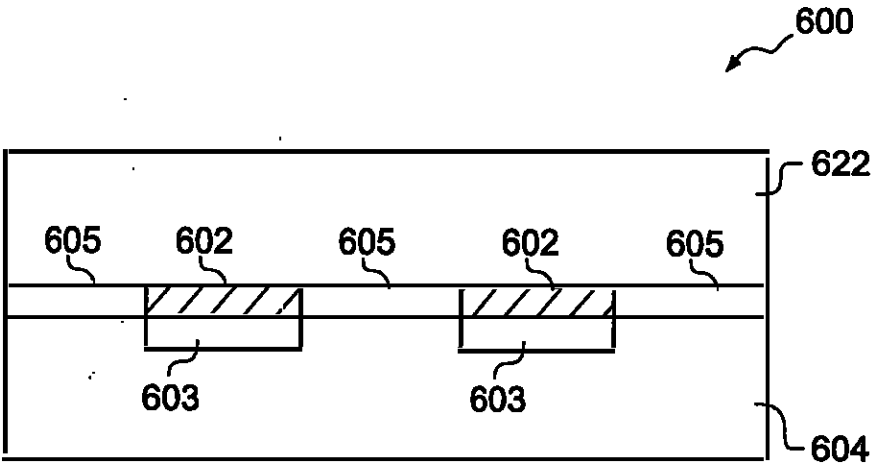


Fig. 6

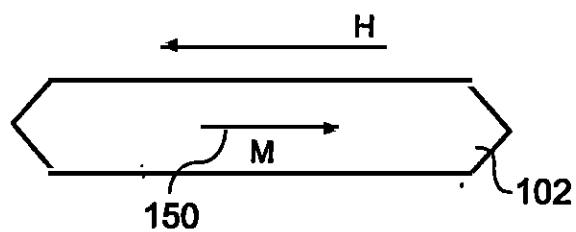


Fig. 7a

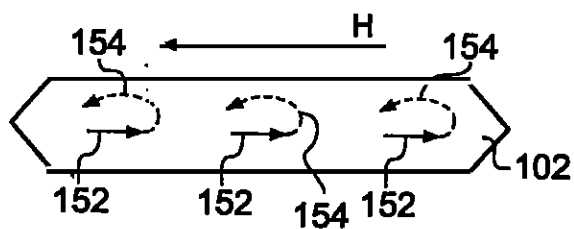


Fig. 7b

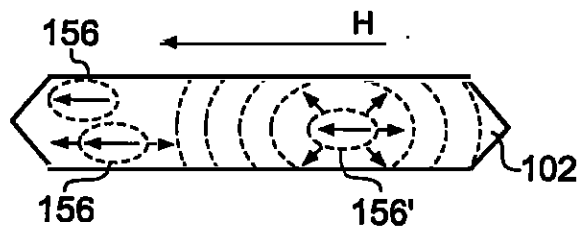


Fig. 7c

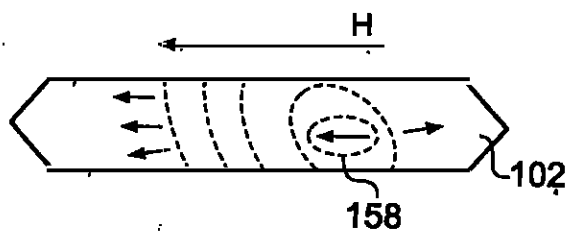


Fig. 7d

75
76

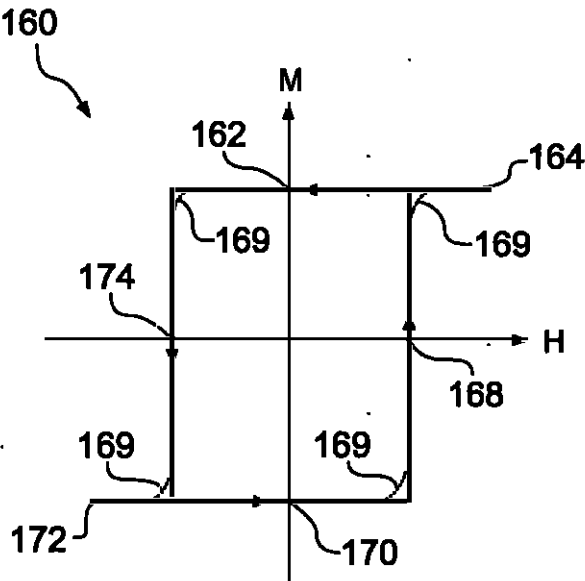


Fig. 8a

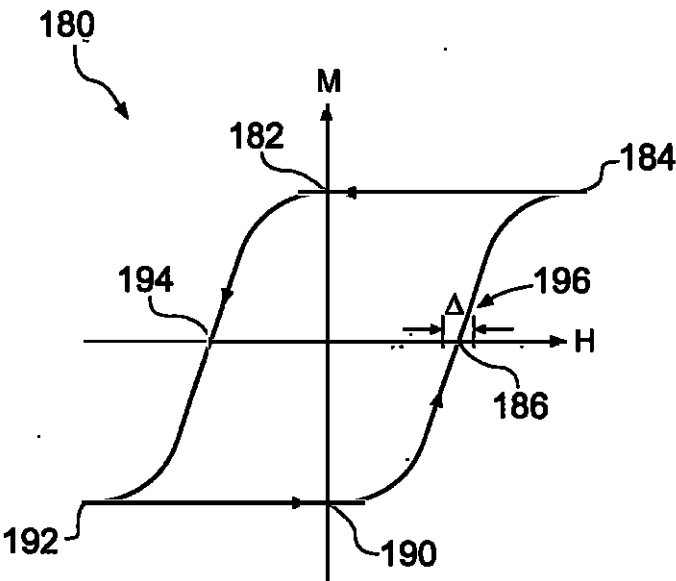


Fig. 8b

76
77



Fig. 9a

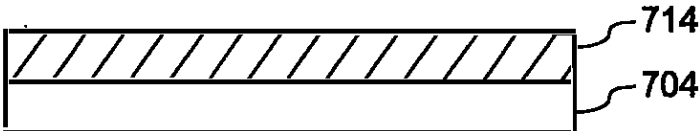


Fig. 9b

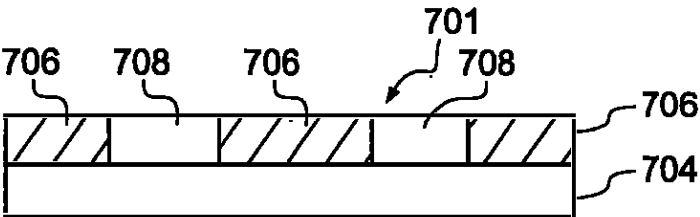


Fig. 9c

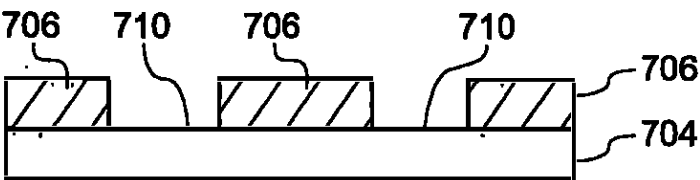


Fig. 9d

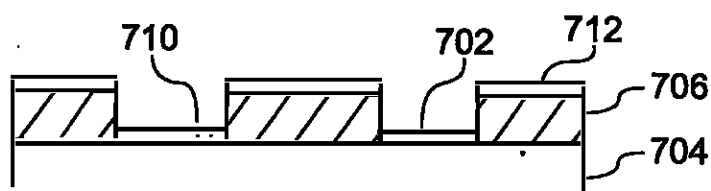


Fig. 9e

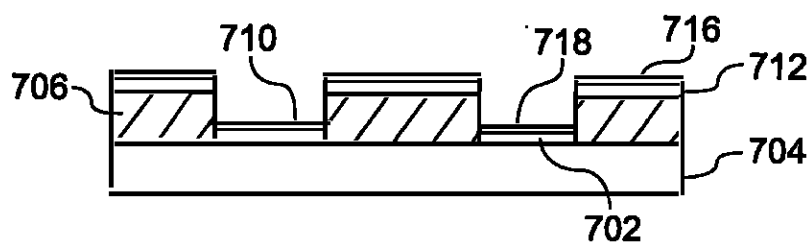


Fig. 9f

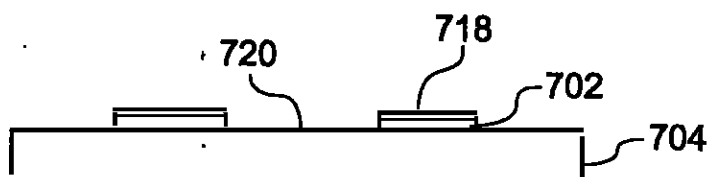


Fig. 9g

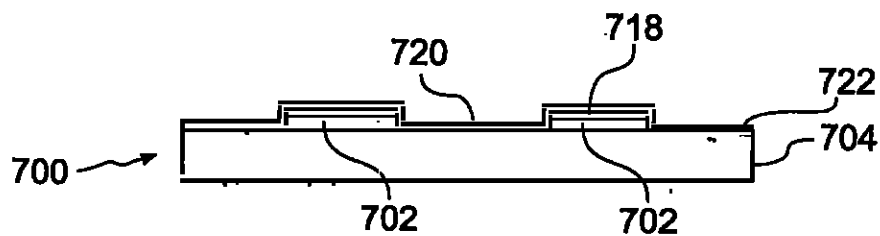


Fig. 9h

SUBSTITUTE SHEET (RULE 26)

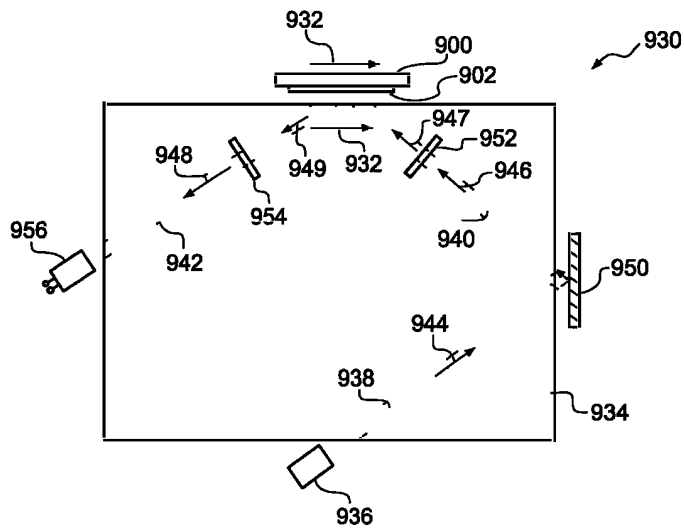


Fig 10

SUBSTITUTE SHEET (RULE 26)

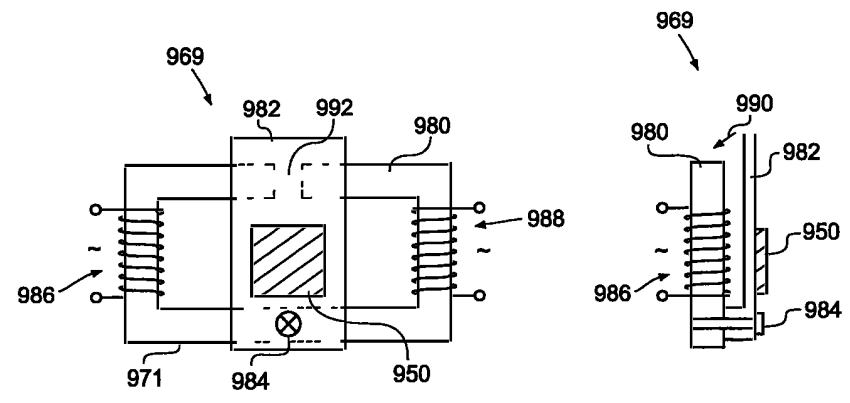


Fig 11

SUBSTITUTE SHEET (RULE 26)

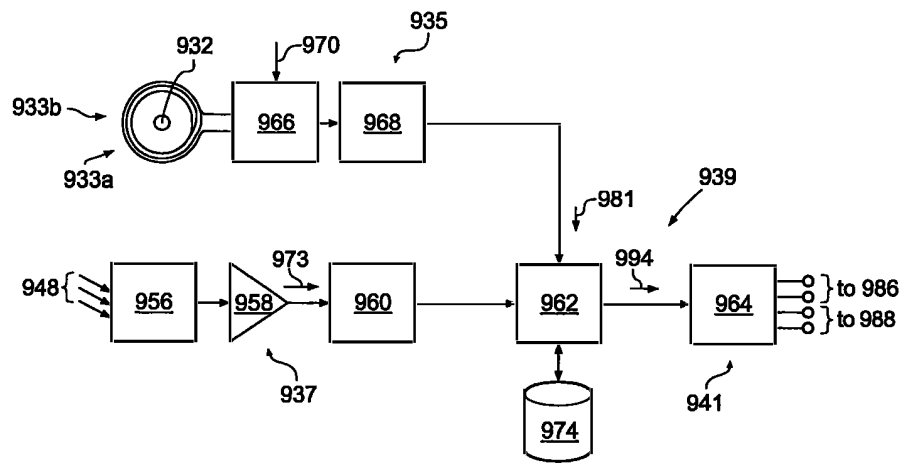


Fig 12

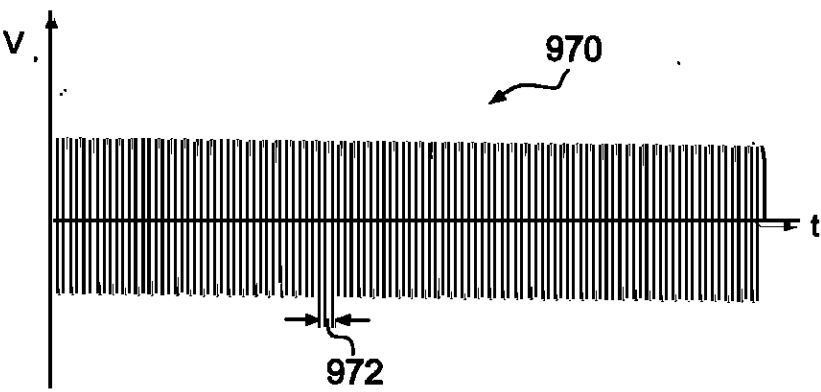


Fig. 13

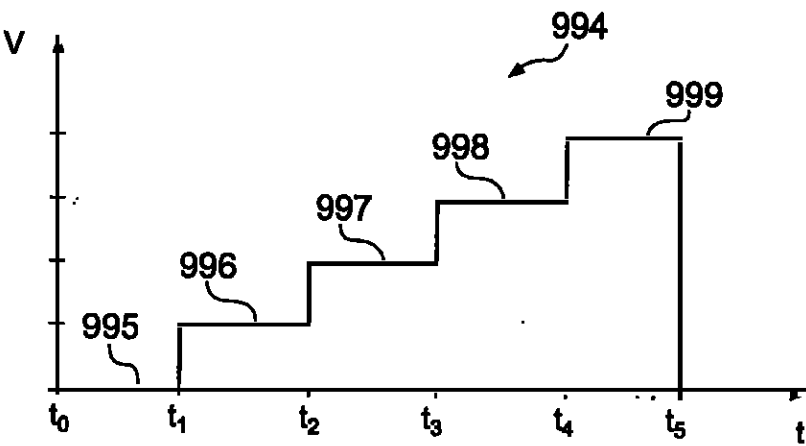


Fig. 14

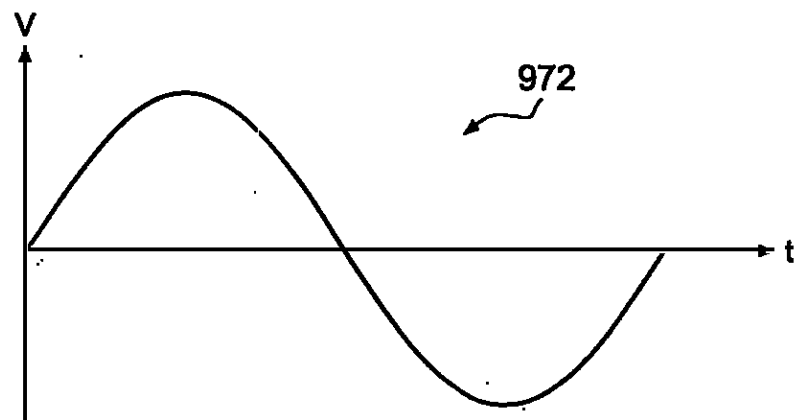


Fig. 15

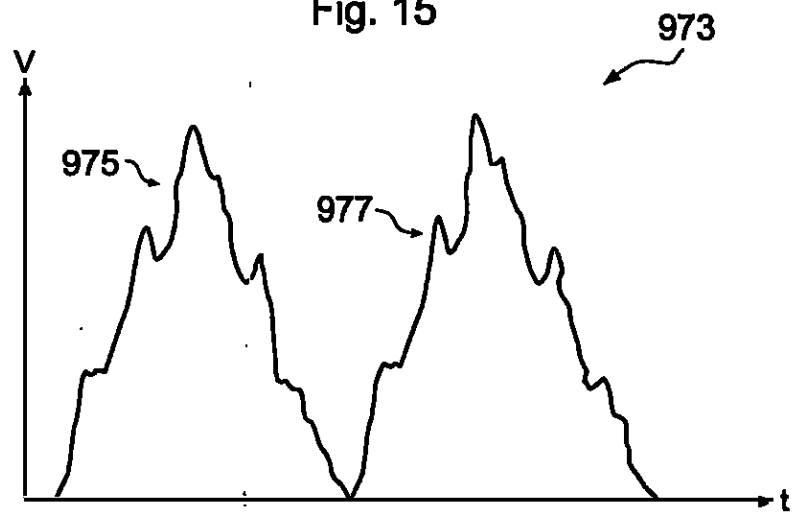


Fig. 16

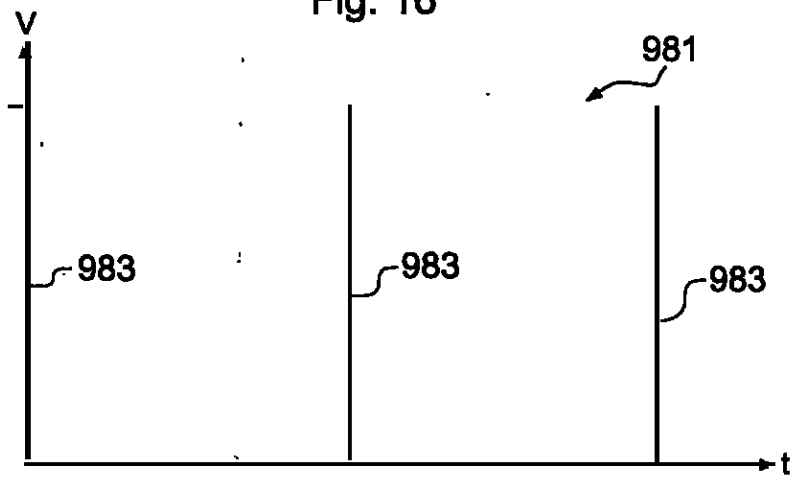


Fig. 17

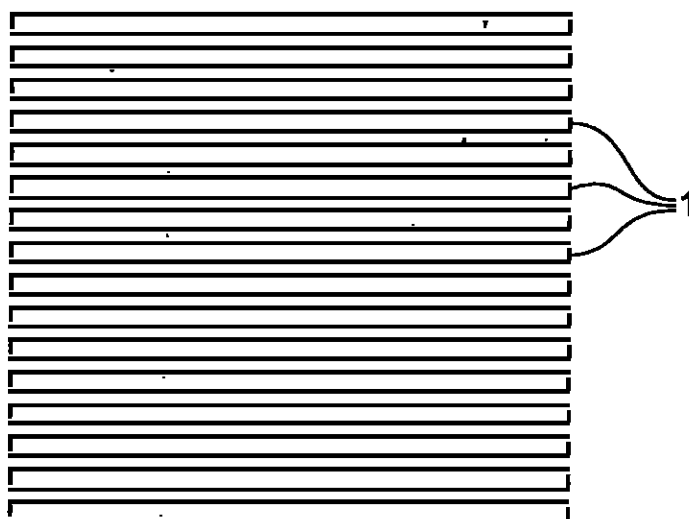


Fig. 18

SUBSTITUTE SHEET (RULE 26)

84
85

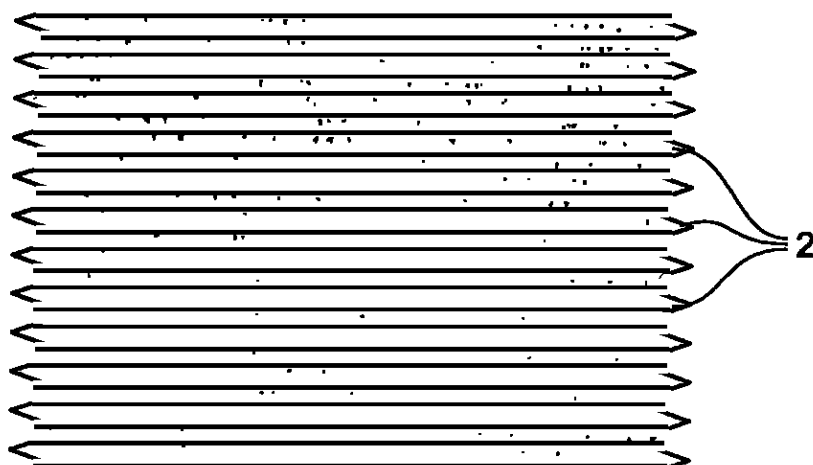


Fig. 19

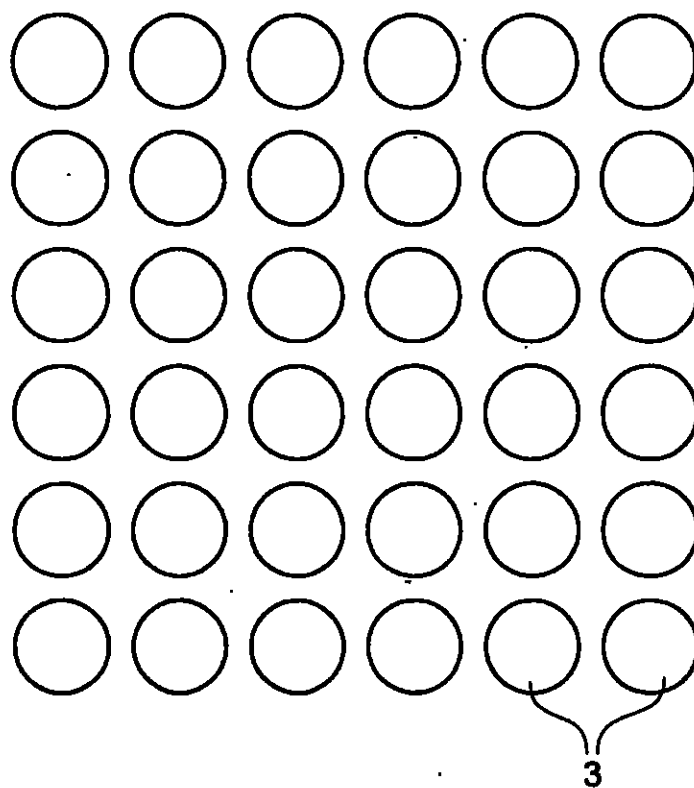


Fig. 20

SUBSTITUTE SHEET (RULE 26)

86
87

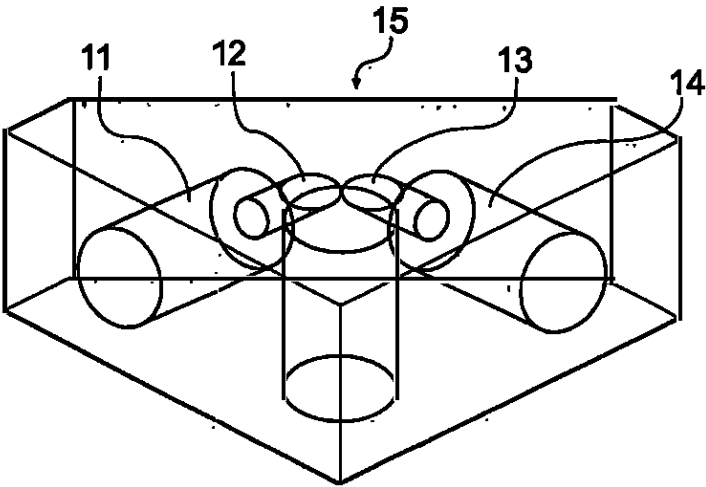


Fig. 21a

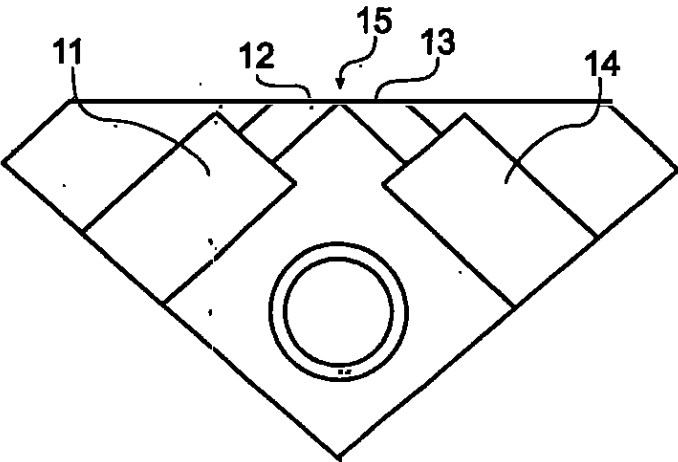


Fig. 21b

84
88

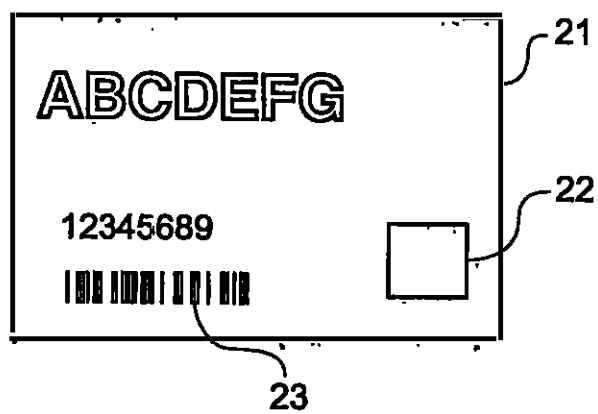


Fig. 22a

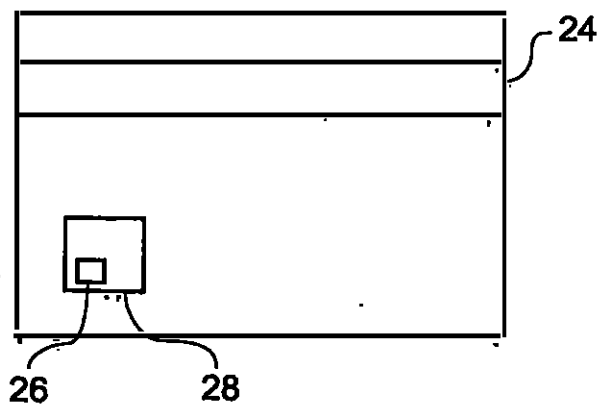


Fig. 22b

SUBSTITUTE SHEET (RULE 26)

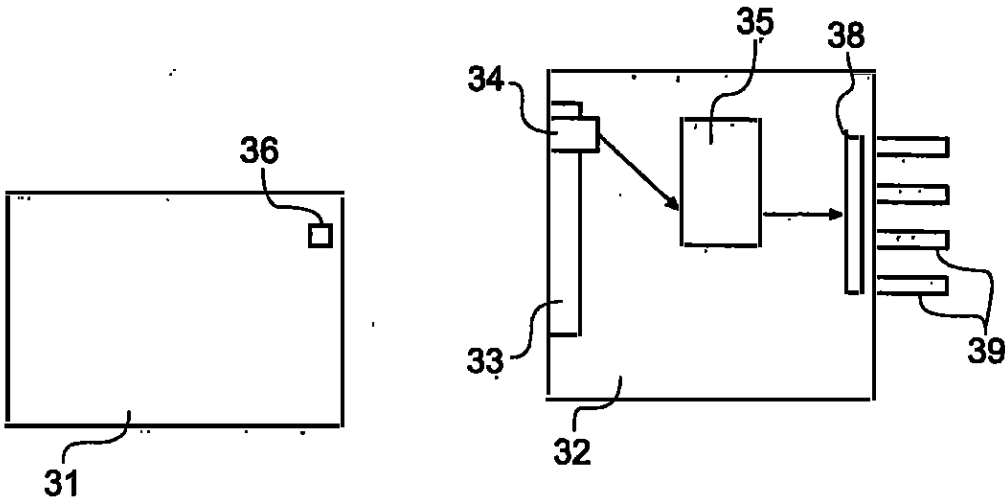


Fig. 23

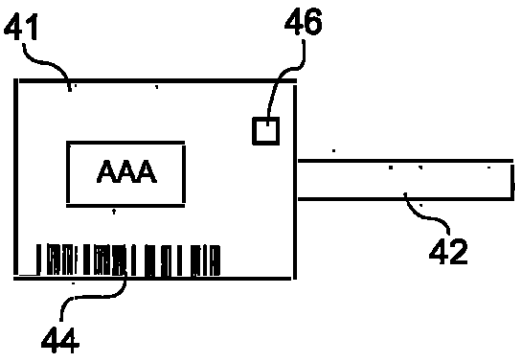


Fig. 24

81
90

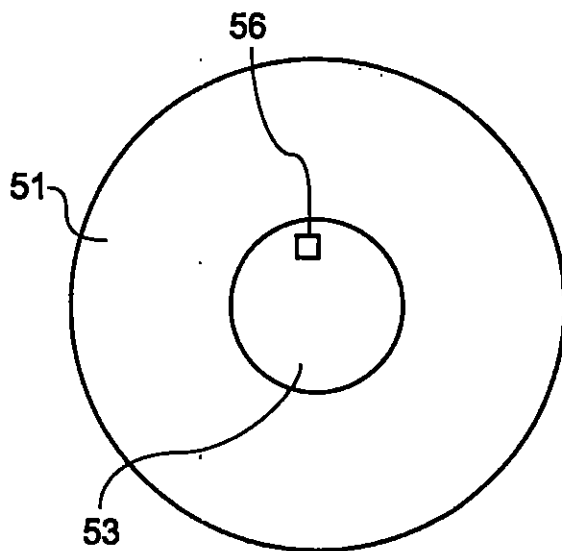


Fig. 25

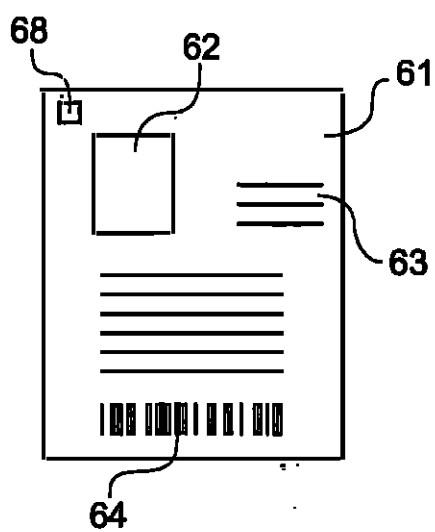


Fig. 26

SUBSTITUTE SHEET (RULE 26)

Dispositivo y sistema de seguridad

La presente invención se relaciona con dispositivos y métodos de seguridad.

En particular, la presente invención se relaciona con métodos y dispositivos de seguridad para identificar copias no autorizadas de bienes, etc. a los cuales se

5 aplican dichos dispositivos de seguridad.

Como se sabe y se analiza en el presente, la falsificación de diferentes productos como, por ejemplo, documentos, pasaportes y bienes, etc. es un problema común. Con frecuencia, los falsificadores y/o piratas copian artículos que

10 tienen diferentes niveles de protección contra el plagio y cada vez se han vuelto más expertos en evadir esquemas existentes de protección contra el plagio, de nivel más alto. Por ejemplo, cada vez más se falsifican artículos como las tarjetas de crédito, mediante la reproducción de las bandas magnéticas, pasaportes con hologramas, etc.

Varios aspectos y realizaciones de la invención buscan proporcionar una
15 manera de mejorar la detección de artículos falsificados, para reducir los efectos de la falsificación.

De acuerdo con un primer aspecto de la invención, se considera un dispositivo de seguridad que comprende, por lo menos, un elemento magnético. El, por lo menos, un elemento magnético, es sensible ante un campo magnético
20 aplicado para proporcionar una respuesta característica. Esta respuesta característica es intrínsecamente difícil de reproducir ya que depende de variaciones incontrolables a nanoescala, en la estructura de los elementos magnéticos. Por tanto, un científico capacitado, incluso uno que entienda la tecnología, no puede copiar dichos dispositivos de seguridad usando tecnología

corriente, incluso si quisiera hacerlo. La variabilidad inherente de dichas variaciones a nanoescala también puede considerar que muchas de esas respuestas características se obtienen para dispositivos de seguridad individuales, garantizando con ello que un enfoque de fuerza bruta para reproducirlos requiere una cantidad extremadamente grande de esos dispositivos, para que se pueda hacer una copia aceptable. (Por ejemplo, puede ser necesario producir millones o miles de millones de esos dispositivos antes de hacer una copia apropiada).

Los dispositivos de seguridad pueden estar provistos con un identificador para identificar un dispositivo de seguridad individual. Los identificadores pueden ser únicos. Cuando se proporcionan identificadores únicos, cualquier intento de fuerza bruta para hacer copias requiere que un plagio haga un número extremadamente grande de dispositivos para cada identificador, antes de que pueda hacer una copia aceptable. Por consiguiente, un plagio no puede simplemente almacenar un gran número de dispositivos y seleccionar algunos que correspondan con respuestas características, a menos que almacene una gran cantidad *por* identificador: por ejemplo, cuando hay una oportunidad de 1 en 2×10^6 de copiar en forma aleatoria un dispositivo de seguridad y se proporcionan 2^{32} identificadores, un falsificador tiene que producir $2 \times 10^6 \times 2^{32}$ identificadores, para tener una oportunidad adecuada de copiar un solo dispositivo de seguridad: este número es enorme; quiere decir 8,589,939,592,000,000. Por consiguiente, la dificultad para copiar un dispositivo dado se hace evidente.

Los identificadores pueden estar formados por los elementos magnéticos mismos. En varias realizaciones se puede usar un patrón de uno o más de los identificadores para definir un identificador único. Dichos elementos magnéticos proporcionan la respuesta característica y el identificador único, haciéndolos cada vez mas difíciles de copiar, en tanto la respuesta característica y el identificador

único se suministren juntos, inseparablemente, mediante la(s) misma(s) estructura(s) física.

De acuerdo con otro aspecto de la invención, se proporciona un método para fabricar un dispositivo de seguridad, que comprende proporcionar, por lo menos, un elemento magnético, en donde dicho elemento magnético proporciona una respuesta característica en respuesta a un campo magnético aplicado. La respuesta característica proporcionada puede usarse para proporcionar una respuesta característica premedida que posteriormente se puede usar en la identificación del dispositivo de seguridad que la generó.

De acuerdo con otro aspecto de la invención, se proporciona un sistema para leer un dispositivo de seguridad, que comprende: un sistema de generación del campo magnético para aplicar un campo magnético a un dispositivo de seguridad; y un sistema de detección para medir uno o más parámetros representativos de una respuesta característica medida de dicho dispositivo de seguridad, en respuesta a dicho campo magnético, en donde dicho sistema puede funcionar para comparar uno o más parámetros representativos de una respuesta característica medida con uno o más parámetros respectivos de una respuesta característica premedida, para determinar si los parámetros medidos y premedidos respectivos son sustancialmente equivalentes.

De acuerdo con otro aspecto de la invención, se proporciona un método para leer un dispositivo de seguridad, que comprende aplicar un campo magnético a un dispositivo de seguridad, medir uno o más parámetros representativos de una respuesta característica medida de dicho dispositivo de seguridad en respuesta a dicho campo magnético; y comparar dichos uno o más parámetros representativos de una respuesta característica medida con uno o más parámetros respectivos de

una respuesta característica premedida, para determinar si los parámetros medidos y premedidos respectivos son sustancialmente equivalentes.

Los dispositivos de seguridad pueden incorporarse dentro de los productos, etc. durante la fabricación y/o después de ella. Pueden usarse para detectar
5 bienes, productos falsificados, etc., mediante la comparación de la respuesta característica premedida con una respuesta característica medida. Varias respuestas características premedidas se pueden usar para comparar una respuesta característica premedida con una respuesta característica medida para un dispositivo de seguridad, de acuerdo con un identificador asociado con ese
10 dispositivo de seguridad.

Los dispositivos de seguridad pueden incorporarse en productos como, por ejemplo, uno o más de: un documento, un pasaporte, una tarjeta de identificación, un disco compacto, un disco versátil digital, un producto de software, empaque, una prenda de vestir, un artículo de calzado, una tarjeta inteligente, una tarjeta de
15 crédito o bancaria, un producto cosmético, una pieza de ingeniería, un accesorio, y cualesquier otros bienes y /o artículos de comercio, sean fabricados o de otro modo, para que las variantes adulteradas o falsificadas de ellos puedan ser identificadas.

El término elemento magnético está dirigido a incluir cualquier elemento
20 formado de cualquier material que proporcione una señal medible en respuesta a un campo magnético aplicado, sea o no que el material mismo posea una magnetización inherente.

Un aspecto de la invención se relaciona con un dispositivo de seguridad, por ejemplo, que comprende un dispositivo de identificación y/o autenticación para
25 usarlo aislado o en asociación con, incorporado en, dentro o acoplado a otro

artículo. El dispositivo de seguridad proporciona una firma o respuesta característica de identificación y/o autenticación, de una manera que limita o hace difícil copiar el dispositivo y, en consecuencia, el plagio o la adulteración de cualquier artículo usado en asociación con el mismo. Otro aspecto de la invención se relaciona con un lector de datos particularmente apropiado para leer la respuesta característica/firma, con un método para producir/medir dicha respuesta característica/firma en un sistema de seguridad que incluya dispositivo y lector, y/o con un método de autenticación o identificación usando dicho dispositivo y/o sistema.

10 Una pérdida importante de ingresos para muchos negocios y una fuente sustancial de actividad criminal surge de la falsificación ilegal o el plagio de artículos. Los ejemplos incluyen, pero no están limitados a:

- Falsificar tarjetas y dispositivos similares usados para transacciones financieras sin papel, como tarjetas de crédito y tarjetas bancarias, para permitir transacciones no autorizadas y retiros de los cajeros ATM;
- Falsificar y plagiar elementos usados para identificación, como pasaportes, visas, licencias de conducción, tarjetas de identificación personal y similares;
- Plagio de material transportado en un medio de almacenamiento de datos como discos CD y DVD;
- Falsificación y plagio de documentos oficiales, tales como certificados;
- Duplicados de tarjetas inteligentes usadas con fines de identificación/acceso, por ejemplo para controlar el acceso a áreas como parte de un sistema de seguridad, controlar el acceso a servicios como televisión

paga, o controlar o impedir el uso de hardware, como computadores u otro equipo de oficina, en un ambiente de múltiples usuarios;

- Plagio de rótulos de seguridad o autenticidad como parte de la fabricación de bienes falsificados, para hacer copias no autorizadas y/ o inferiores de productos de marca con gran valor, bienes con una alta especificación de seguridad crítica y similares.

Este es un problema identificado particularmente en relación con tarjetas y dispositivos similares usados para transacciones financieras sin papel y para propósitos de identificación, y esta área ha conducido al desarrollo de sistemas de seguridad, los cuales son, no obstante, probable y generalmente aplicables a la mayoría o a todas las áreas en donde la falsificación es un problema.

A medida que los sistemas de seguridad general y comercial sin papel se han vuelto más sofisticados, el aumento de la automatización unida a un crecimiento en la capacidad de almacenamiento de información en el producto han creado grandes oportunidades para el fraude financiero y de identificación mediante el plagio de esos documentos. La concentración de riqueza y/o información asequible a través de tarjetas de crédito, tarjetas bancarias y documentos de identificación han aumentado. Se ha desarrollado una creciente necesidad de verificación e identificación exactas de los artículos y/o la prevención del plagio efectivo.

Los sistemas de tarjetas y documentarios en particular han adoptado medidas que mejoran la seguridad, haciendo difícil o inconveniente la falsificación. Este enfoque se ha concentrado en particular en la realización de dispositivos incorporados sobre o dentro de la tarjeta u otro documento, los cuales son difíciles de copiar efectivamente. Los ejemplos incluyen imágenes holográficas, rejillas de

difracción, sustancias especializadas (tintas, materiales, etc.), estructuras en relieve, estructuras dentro del material de la tarjeta, etc.

Sin embargo, finalmente, estas marcas pueden ser copiadas por el falsificador sofisticado y lo hará si las retribuciones son suficientes. Existe un
5 deseo general por una marca de seguridad que prácticamente no pueda ser falsificada.

Una estrategia efectiva contra la copia no autorizada de artículos existe si una *firma aleatoria* o una respuesta característica se pueden asociar con el artículo o con un dispositivo acoplado al artículo. La firma/respuesta característica
10 aleatorias podrían provenir de algún proceso de fabricación incontrolable que nunca pueda ser duplicado con precisión. Por tanto, siempre existe alguna pequeña diferencia entre el artículo original y su copia; si esta diferencia puede ser detectada y comparada con una respuesta medida previamente (por ejemplo, una respuesta de la línea base en la cual la respuesta de los elementos magnéticos
15 individuales se registra por separado, o se registra la respuesta promedio de una colección de dichos elementos magnéticos) tomada del elemento original, la falsificación puede ser identificada.

Existen 4 requerimientos primarios preferidos de una firma aleatoria práctica:

- Que sea posible medir la firma fácilmente y sin un costo excesivo;
- 20 • Que sea posible representar la firma de la línea base fácilmente, preferiblemente mediante una lista pequeña de números digitales;
- Que exista un alto grado de aleatoriedad inherente en la fabricación de la firma, de modo que cada firma sea ligeramente diferente;

- Que no sea posible controlar la fabricación de la firma, de modo que su aleatoriedad pueda eliminarse o suprimirse y hacer una copia idéntica de una firma existente.

Hasta la fecha, las dificultades para cumplir todos estos requerimientos han limitado la aplicabilidad práctica del concepto en una escala amplia, en los sistemas de uso cotidiano.

Vista desde una primera perspectiva, la invención proporciona un dispositivo de seguridad para un artículo, el cual es intrínsecamente difícil de copiar y por tanto limita la falsificación.

Vista desde otra perspectiva, la invención proporciona un dispositivo de seguridad para un artículo basado en una firma aleatoria, la cual se fabrica fácilmente y es medible a una escala y un costo apropiados para el uso cotidiano en la autenticación/prevenición de falsificación de artículos de alto valor.

Vista desde una perspectiva adicional, la invención proporciona un lector de datos particularmente apropiado para leer la firma del dispositivo.

Por eso, de acuerdo con la invención, en un primer aspecto se proporciona un dispositivo de seguridad que comprende, por lo menos y preferiblemente, varios, y más preferiblemente, una gran variedad de elementos magnéticos organizados en un substrato apropiado y que tienen una respuesta de la firma magnética legible por máquina, proporcionada en combinación con una lectura de la respuesta de la firma magnética de la línea base predeterminada.

En varias realizaciones, los elementos magnéticos pueden comprender una capa delgada de material magnético, tal como alambres magnéticos delgados. El material magnético puede comprender alambres y/o puntos macroscópicos,

alambres y/o puntos microscópicos y/o nanoalambres y/o nanopuntos, distribuidos en una forma apropiada sobre un substrato apropiado, para dar una marca magnética legible por máquina, con una señal de firma de la línea base medible, altamente dependiente de la estructura precisa intrínseca. La respuesta de la firma de la línea base registrada predeterminada da una cifra comparativa, una respuesta "esperada", la cual se puede usar en conexión con una respuesta medida para autenticar el dispositivo.

Como se usa en el presente, "dispositivo" en su forma más amplia comprende el elemento magnético como se describió antes en el presente, dispuesto en un substrato apropiado como, por ejemplo, la superficie de un artículo al cual se va a aplicar un dispositivo de seguridad. Ejemplos de la aplicación del dispositivo incluyen, sin limitación, un dispositivo que constituye o comprende una parte de un objeto adaptado para uso por su propio derecho, como una aplicación de identificación, autenticación, clave o cualquiera otra; un dispositivo que constituye o comprende parte de un objeto proporcionado para uso con un segundo objeto, en particular, por ejemplo, como un acoplamiento al mismo para autenticación, identificación u otro rotulado, seguridad relacionada u otros propósitos; una parte del dispositivo incorporada en o sobre un segundo artículo para propósitos de identificación, autenticación o seguridad relacionada, u otros propósitos. En particular, el dispositivo se proporciona para autenticar e impedir/prevenir la falsificación no autorizada mediante plagio o clonación de un artículo del cual forma parte o con el cual está asociado.

Ejemplos de conjuntos apropiados de elementos magnéticos están descritos en R. P. Cowburn, *Journal of Physics D*, 33, R1 (2000). La presente invención puede basar su efectividad singular en la creación de una firma aleatoria antifalsificación.

Los elementos magnéticos son tales que cuando se aplica a los elementos un campo magnético variable en el tiempo, su respuesta magnética es una función histerética y no lineal de ese campo aplicado. Esta no linealidad puede caracterizarse por saltos discretos en la magnetización en ciertos valores del campo aplicado. Los elementos son tales que las pequeñas diferencias en fabricación, las cuales deben naturalmente existir de un elemento a otro, harán que la respuesta magnética varíe ligeramente de elemento en elemento. Además, para varias realizaciones, los elementos son tales que un elemento dado responde de una manera tan similar como sea posible ante cada ciclo del campo magnético aplicado variable en el tiempo.

Para determinar la respuesta de la firma de la línea base de un conjunto de elementos magnéticos, se aplica a los elementos un campo magnético variable en el tiempo y se registra la respuesta magnética de los elementos. La respuesta puede medirse usando el dispositivo descrito en el presente o por algún otro medio.

La respuesta de la línea base puede condensarse mediante la identificación de características específicas, como saltos repentinos o la desviación media y estándar de los campos de conmutación. Alternativamente, la respuesta de la línea base puede convertirse de una secuencia de medidas de magnetización de dominio temporal a una lista de mediciones de dominio frecuencial. Alternativamente, la respuesta de la línea base puede no ser procesada.

Medir la respuesta de la línea base predeterminada es análogo a un procedimiento de calibración. Se anticipa que la respuesta de la línea base predeterminada solamente se medirá una vez, en el momento de la fabricación y que el dispositivo se proporcionará al usuario con la respuesta de la línea base

predeterminada, almacenada de una manera accesible, por ejemplo, a distancia del dispositivo, o en asociación con el dispositivo de una forma inaccesible sin autorización. En particular, es deseable que la respuesta de la línea base predeterminada esté cifrada con seguridad, especialmente si tiene o está con el dispositivo. Preferiblemente, la respuesta de la firma de la línea base predeterminada está cifrada usando un algoritmo de cifrado asimétrico, manteniendo en secreto la clave privada usada para cifrar, y la clave pública para descifrar disponible para cualquier lector del dispositivo, de modo que la respuesta de la firma de la línea base predeterminada esperada pueda ser descifrada y se pueda comparar con una respuesta medida.

Para probar la autenticidad de un elemento protegido por una firma aleatoria, en varias realizaciones es necesario: aplicar un campo magnético variable en el tiempo a los elementos magnéticos y registrar la respuesta de la firma magnética medida de los elementos para ese campo aplicado. El mismo procedimiento se usa primero para determinar la respuesta de la línea base esperada predeterminada, la cual entonces se almacena como se indica arriba y luego, mediante el uso de un lector apropiado para obtener las respuestas de la línea base medidas posteriormente, las cuales pueden ser comparadas con la respuesta de la línea base esperada predeterminada, para autenticar el dispositivo.

La autenticación se basa en la naturaleza aleatoria inherente del dispositivo. Elementos magnéticos fabricados artificialmente hacen una muy buena firma aleatoria práctica porque el campo de conmutación magnética de cada elemento depende críticamente de la estructura física de los extremos de los elementos. Las variaciones estructurales de sólo unos pocos nanómetros de tamaño pueden ocasionar cambios significativos al campo de conmutación (K. J. Kira, J. N.

Chapman, y C. D. W. Wilkison, *J. Appl. Phys.* **85**, 5237 (1999)). Por tanto, para replicar la firma aleatoria, es necesario replicar la forma precisa de los elementos con una precisión casi atómica. Esto no es factible usando tecnología actual y es probable que siga así por muchas décadas. Aunque la manipulación a nivel casi atómico se requiere para copiar el dispositivo descrito en esta invención, una medida macroscópica es suficiente para verificar la autenticidad, porque cuando la estructura pasa por la conmutación magnética, toda la estructura cambia, haciendo que la respuesta magnética sea muy fácil de medir. Así, la firma aleatoria de acuerdo con esta invención requiere procesos de bajo costo y simples para interrogarla, pero ingeniería definitivamente difícil para copiarla. Esto es ideal para una firma aleatoria práctica.

Si la respuesta magnética de una colección de elementos se registra en grupo como una medida de ensamble, se debe apreciar que las fluctuaciones estadísticas sobre las cuales se basa esta invención se atenuarán. El factor de atenuación será $1/\sqrt{N}$, en donde N es el número de elementos normalmente idénticos en el ensamble. Así, si una colección de elementos individuales tiene un campo de conmutación con una desviación estándar de 10 Oe, entonces un conjunto de montajes de 100 elementos solamente tendrá una desviación estándar de 1 Oe. Por consiguiente, la medida de la respuesta magnética se debe hacer más cuidadosamente. De otro lado, el volumen total del material magnético ha aumentado en un factor N , el cual hace más fácil tomar la medida.

En varias realizaciones, la autenticación se basa en un equilibrio entre la respuesta de la línea base medida del dispositivo y una respuesta de la línea base predeterminada y almacenada con seguridad, en particular en forma cifrada. Un intento de falsificación para falsificar un dispositivo que incorpora una respuesta de la línea base prerregistrada en forma cifrada será extremadamente improbable de

que produzca una falsificación perfecta, teniendo una respuesta de firma magnética medible que corresponda con una original prerregistrada y cifrada. En el dispositivo genuino, la respuesta de la línea base predeterminada se registra en un cifrado conocido solamente por la compañía fabricante o los autorizados por ella. Si el falsificador potencial simplemente trata de plagiar el dispositivo de firma y el derivado cifrado de él, la falsificación fallará porque, incluso si el cifrado está copiado exactamente, la respuesta de la firma magnética del dispositivo copiado diferirá del original. Así, en la falsificación, las respuestas de la firma registrada, predeterminada y medida no corresponderán. Si el falsificador crea una copia del dispositivo de firma, en cambio podría medir la respuesta de la línea base del dispositivo falsificado rápidamente. Sin embargo no podría crear un cifrado válido apropiado que corresponda con la respuesta de la línea base falsificada, porque no conoce el cifrado. De ese modo, ambas estrategias posibles de plagio fallan.

Por eso, de conformidad con varios aspectos de la invención, se describe un método práctico de generar y leer una firma aleatoria usando materiales magnéticos estructurados artificialmente el cual, para propósitos prácticos, es imposible de copiar y, por tanto, proporciona un dispositivo de seguridad que puede autenticar originales y evitar la falsificación por el plagio de esos originales.

Los elementos magnéticos de diferentes realizaciones comprenden capas delgadas de material magnético, preferiblemente menores de 1 μm de espesor y más preferiblemente menores de 100 nm de espesor. Pueden ser de 10 nm de espesor o menos pero, por preferencia, generalmente serán de alrededor de 40 nm de espesor.

Todos los elementos pueden ser nominalmente idénticos en forma y con una distribución regular, o las diferencias entre ellos y/o patrones irregulares de

distribución pueden haber sido introducidos intencionalmente. Se debe hacer énfasis en que la naturaleza aleatoria de la respuesta magnética es una consecuencia inherente de la fabricación del material, y no depende de la forma, la configuración y el patrón de distribución de los elementos.

- 5 Generalmente, los elementos pueden ser de forma rectangular, en particular rectangular alargados, por ejemplo, que comprenden un arreglo de elementos rectangulares elongados magnéticos generalmente paralelos, o puede comprender áreas de material magnético, por ejemplo cuadradas o circulares, o de alguna otra forma geométrica regular, la cual puede, por ejemplo, estar
- 10 formada en una red de dos dimensiones.

Como se usan en el presente, en la referencia a alambres magnéticos, microalambres o nanoalambres se considerará que dichos elementos son de forma elongada, y en particular son elementos rectangulares elongados y/o elementos elongados en una red generalmente paralela, pero no restringidos a los

15 ejemplos rectangulares paralelos dados en el presente con propósitos de ilustración. Como se usan en el presente, en la referencia a puntos magnéticos, micropuntos o nanopuntos, se considerará que dichos elementos comprenden áreas de material magnético de forma más cuadrada, menos elongada, y en particular de forma geométrica regular, y/o formados en una red de dos

20 dimensiones, pero no restringidos a la geometría circular de los ejemplos dados en el presente con propósitos de ilustración.

Los elementos pueden ser discretos, sin ningún material magnético que los conecte, o pueden estar parcialmente conectados con material magnético en varias redes, o pueden estar completamente conectados con material magnético

25 en una red única.

Los elementos pueden estar hechos de un material magnético, el cual será de preferencia magnéticamente suave, por ejemplo basado en níquel, hierro, cobalto y aleaciones de ellos entre sí o con silicio, como aleación níquel hierro, aleación cobalto hierro, aleación hierro silicio o aleación cobalto silicio.

- 5 Los elementos pueden estar cubiertos con una sobrecapa de protección para evitar la oxidación o el daño mecánico; dicha sobrecapa de protección comprende una capa delgada de material no magnético que tiene propiedades adecuadas de resistencia al medio ambiente y/o mecánicas y/o tratamientos de superficie y/o revestimientos que, por ejemplo, comprenden una capa de cerámica, vidrio o
- 10 material plástico. Dichas sobrecapas son convenientemente transparentes. Ejemplos particulares de sobrecapas de protección incluyen dióxido de titanio, resina epóxica transparente, plástico o vidrio, revestimiento conforme de resina de silicona modificada transparente y revestimiento conforme de acrílico transparente.

- Los elementos están dispuestos sobre un sustrato apropiado. Entre los
- 15 elementos y el sustrato puede existir una capa base. El dispositivo puede estar incorporado directamente en o sobre el artículo que se va a proteger, en cuyo caso el sustrato puede ser el artículo que se va a proteger contra la falsificación misma o algún material de sustrato apropiado dispuesto sobre él o incorporado en él para el propósito. Alternativamente, el dispositivo puede estar incorporado en
- 20 una unidad separada como una etiqueta, rótulo, certificación, etc., acoplable o de otro modo utilizable junto con un elemento que se ha de proteger, la unidad acoplable que comprende o incorpora algún material de sustrato apropiado. Los materiales de sustrato apropiado incluyen silicio, vidrio, plástico o algún otro material con una superficie uniforme.

En el caso de los elementos magnéticos que han de formar una unidad acoplable, la unidad acoplable puede estar unida directamente al artículo que se ha de proteger o puede formar parte de un certificado u otra documentación asociada con el artículo que se ha de proteger. Los mecanismos pueden

5 proporcionarse en asociación con una unidad acoplable para efectuar el acoplamiento entre la unidad que comprende un dispositivo de identificación, de conformidad con la invención, y el artículo que se ha de proteger. Dicho mecanismo puede proporcionar un acoplamiento removible y fácil de desprender de la unidad acoplable con el elemento protegido o un acoplamiento permanente.

10 En el caso anterior, los mecanismos de acoplamiento pueden comprender, además, mecanismos de cierre para garantizar que solamente personas autorizadas puedan retirar la unidad. En cualquier caso, los medios de acoplamiento pueden comprender protección adicional contra manipulación no autorizada y/o mecanismos para indicar la manipulación por parte de personas no

15 autorizadas.

Los usos apropiados para dicha unidad acoplable incluyen, sin limitación, rótulos para artículos de valor, de importancia para la seguridad, o de otro modo con importancia crítica, por ejemplo para permitir la identificación del artículo, la autenticación del artículo como genuino, la verificación de la procedencia del

20 artículo y similares, y/o para rotular el artículo de una manera segura y controlada, por ejemplo con información sobre el artículo, información sobre precios, información sobre control de inventarios, etc.

En el caso de elementos magnéticos que se forman directamente sobre un artículo que se ha de proteger, también se pueden contemplar usos similares. Sin

25 embargo, la incorporación directa del dispositivo en el elemento que se ha de proteger será singularmente efectiva para prevenir la reproducción no autorizada,

dada la naturaleza aleatoria y, por tanto, reproducible e intrínsecamente incontrolable del dispositivo de firma y, por consiguiente, será particularmente útil en asociación con artículos que podrían ser susceptibles a la producción de copias falsificadas, dado que el dispositivo proporcionará una autenticación rápida de un artículo como original.

Los elementos pueden estar formados por litografía óptica, por ejemplo, usando el método descrito en el presente, aunque se puede usar la grabación o alguna otra forma de impresión por contacto.

La diversidad de elementos que constituyen el dispositivo puede ser, generalmente, del mismo tamaño y forma, o puede tener un tamaño y/o forma que difieran continuamente o discontinuamente en el dispositivo. Preferiblemente, en un ensamble se presentaran varios tamaños para el elemento.

En una realización, varios grupos discretos de elementos con forma y/o tamaños diferentes, los elementos que han de ser generalmente similares en tamaño o forma dentro de cada grupo, se proporcionan de modo que puedan identificarse varios campos de conmutación diferentes. Por ejemplo, un ensamble de elementos rectangulares en red paralela puede comprender varios grupos discretos con diferentes anchos.

Un ejemplo apropiado comprende 100 elementos rectangulares, cada uno de 1 mm de longitud, 10 serán de 5.0 μm de ancho, 20 serán de 2.5 μm de ancho, 30 serán de 1.7 μm de ancho, 40 serán de 1.2 μm de ancho. La respuesta magnética de un montaje mostrará entonces cuatro grupos distintos de campos de conmutación, cada uno de los cuales exhibirá una variación estadística de una etiqueta a la siguiente, lo cual se puede usar para formar una firma aleatoria.

Un segundo ejemplo comprende 450 elementos rectangulares, cada uno de 1 mm de longitud; 150 serán de 1.0 μm de ancho, 120 serán de 1.25 μm de ancho, 90 serán de 1.67 μm de ancho, 60 serán de 2.5 μm de ancho y 30 serán de 5 μm de ancho. La respuesta magnética del ensamble mostrará entonces cinco grupos
5 distintos de campos de conmutación.

En los ejemplos, el número de elementos en cada grupo es tal que cada grupo debe cubrir generalmente la misma área. La intensidad de la señal detectada desde el lector, usualmente depende del total del área de cobertura, de modo que los cuatro o cinco grupos de campos de conmutación registrarán la
10 misma intensidad en el lector. Esta es una característica preferida para muchas aplicaciones, pero puede contemplarse que para otras aplicaciones, varios grupos discretos de elementos de diferente tamaño y/o forma se pueden proporcionar cuando diferentes grupos ocupan áreas diferentes del dispositivo.

En una realización alterna, elementos de diferente forma y/o tamaño
15 proporcionan una red que varía continuamente, de modo que las variaciones en tamaño y/o forma entre un elemento y sus vecinos se minimizan para evitar grandes discontinuidades. Por ejemplo, el área de un elemento debe variar con respecto a sus vecinos en no más de 5%, y en particular alrededor de 1%. Como resultado, se produce una colección uniformemente variable de campos de
20 conmutación. La variación podría ajustarse de acuerdo con una forma funcional apropiada que puede ser lineal o no lineal.

Por ejemplo, en un dispositivo análogo al descrito arriba con elementos rectangulares en red en paralelo, el ancho de los elementos varía como una función uniforme a través de la red. Un ensamble podría comenzar con un alambre
25 de 2.5 μm de ancho; el siguiente tendría 2.53 μm de ancho; el siguiente sería de

2.56 μm de ancho, etc., hasta que 56 alambres después, el ancho haya alcanzado 5 μm . En este ejemplo, el ancho total del alambre es de 200 μm . Un montaje alterno podría comenzar con un alambre de 1 μm de ancho; el siguiente sería de 1.01 μm ; el siguiente, de 1.02 μm , etc., hasta que 450 alambres después el ancho haya alcanzado 5 μm . Diferentes formas funcionales, por ejemplo, lineales, cuadradas, etc., podrían usarse para determinar la progresión de los anchos a través del ensamble. A diferencia del ejemplo anterior, esto no daría grupos distintos de campos de conmutación, sino una colección uniforme de campos de conmutación.

En una realización, el dispositivo, además de la red de la firma que comprende una gran variedad de elementos de firma, comprende un elemento magnético único de área relativamente grande para usarlo como un elemento de referencia; por ejemplo, un nanoalambre magnético relativamente ancho o un microalambre magnético. En los ejemplos anteriores, un alambre de ancho único podría ser de 1 mm de longitud y 150 μm de ancho. Para un alambre con un ancho grande, la propiedad magnética es casi idéntica al material en bloque, el cual usualmente está muy bien definido. Por eso, además de los cinco bloques que tienen campos de conmutación erráticos, se proporciona un campo de conmutación bien definido que se puede usar para calibrar el lector. Esta calibración podría incluir hacer ajustes basados en las condiciones del medio ambiente, como restar la influencia del campo magnético de la Tierra, por ejemplo, o compensar los cambios de temperatura.

Es necesario que se suministre una respuesta de firma magnética de línea base predeterminada, en combinación con un dispositivo de seguridad de conformidad con varios de las realizaciones de la invención. Sin embargo se entenderá que no es necesario proporcionar una respuesta de firma magnética de

línea base predeterminada, en asociación física con el dispositivo de seguridad, sino simplemente que esté disponible para el usuario autorizado del dispositivo con fines de comparación, para dar una respuesta "esperada" que se comparará con una respuesta real cuando el dispositivo se lea por medios apropiados, como

5 los medios de lectura de la firma magnética descritos en el presente.

Se pueden proporcionar varias realizaciones. En una primera de ellas se puede proporcionar la línea base prerregistrada en asociación física con el dispositivo o artículo protegido. En una segunda realización, la línea base prerregistrada puede ser almacenada por un lector para dispositivos. En una

10 tercera realización, la línea base prerregistrada puede ser almacenada a distancia del dispositivo y del lector del dispositivo, de una manera asequible para una persona autorizada de tal manera que se pueda hacer la comparación necesaria entre las lectura de línea base esperada (es decir prerregistrada) y real (medida) para propósitos de autenticación.

15 En la primera realización mencionada arriba, la respuesta de línea base prerregistrada se proporciona en estrecha asociación física con el dispositivo o artículo protegido. En una alternativa, la línea base prerregistrada se almacena en cercanía física al dispositivo, en una forma legible por máquina. Por ejemplo, la línea base prerregistrada se almacena como una parte del dispositivo; o se

20 almacena adyacente al dispositivo o debajo del dispositivo en un sustrato común, o se almacena cerca del dispositivo como parte de una unidad que incorpora el dispositivo de seguridad de la invención, opcionalmente con otras características de seguridad o información, como una tarjeta inteligente, documento de identificación, tarjeta clave, llave clave o similares, o un rótulo para un artículo que

25 se ha de proteger, o se almacena con o en un artículo que se ha de proteger al cual también se le ha proporcionado un dispositivo de conformidad con la

invención; o se almacena como parte de un certificado u otra documentación asociada con un elemento que se ha de proteger, los cuales también pueden incorporar dicho dispositivo de conformidad con varias realizaciones de la invención.

5 En esta realización, la línea base prerregistrada deberá almacenarse en forma legible pero cifrada. Por ejemplo, la respuesta de la línea base condensada o no procesada se firma digitalmente usando un algoritmo de cifrado asimétrico, como el RSA. La clave privada, que se usa para cifrar, la conoce solamente la compañía fabricante; la clave pública, que se usa para descifrar, se encuentra en
10 todas las terminales de lectura que podrían ser usadas para leer el dispositivo.

La respuesta de la línea base cifrada y firmada digitalmente se almacena en el artículo, preferiblemente con los elementos magnéticos, por ejemplo impresa debajo o paralela a los elementos o, alternativamente, grabándola en un banda de datos magnéticos o en un código de barras óptico o en el chip de una tarjeta
15 inteligente o por algún otro medio. Otra información como, pero no limitada a, el nombre del propietario o un código de identificación único o un control de validación (*checksum*) también se puede cifrar dentro de la misma corriente de datos y la firma digital, para prevenir que los elementos magnéticos sean transferidos a otro artículo o que información importante de un documento o
20 certificado sea modificada.

En la segunda realización a que se hace referencia arriba, la respuesta de la línea base prerregistrada/premedida se almacena en, por o en estrecha asociación con un lector para dispositivos. Dicha realización se presta en sí misma, en particular, para sistemas del tipo "cerradura y llave", donde el dispositivo actúa
25 como una llave y se usa en asociación con un lector que actúa como una

cerradura para limitar el acceso a áreas particulares, la operación de artículos particulares, o el uso de servicios particulares para el tenedor(es) de la llave especificada.

En esta realización no es necesario que los datos de la firma de la línea base prerregistrada se almacenen en o en estrecha asociación con el dispositivo mismo o un artículo protegido. Sin embargo, opcionalmente, los datos se pueden almacenar en forma cifrada por seguridad, por ejemplo en la manera descrita arriba, o pueden protegerse por seguridad de otro modo.

En la tercera realización a que se hace referencia arriba, los datos de la firma de la línea base prerregistrada/premedida se almacenan a distancia del dispositivo, el artículo protegido y el lector para dispositivos. Este modo de operación se presta en sí mismo, en particular para, pero no está limitado a, sistemas donde se contempla una red que comprende un número grande de lectores que esperan interrogar a un número grande de dispositivos como, por ejemplo, podría ser el caso con tarjetas de crédito y similares con múltiples puntos de ventas, sistemas de seguridad e identificación con múltiples puntos de acceso, etc.

De acuerdo con esta realización, los datos de la firma prerregistrada con respecto al dispositivo y en particular acerca de una diversidad de dispositivos diferentes, preferiblemente se almacenan en un almacén de datos central, por ejemplo, conectado a varios lectores en una red distribuida. En dicha red se pueden contemplar dos modos alternos de operación. En el primero, se adapta un lector para leer un dispositivo, interrogar un almacén central de datos para los datos de la firma prerregistrada y hacer la comparación. En el segundo, el lector para dispositivos se adapta para leer el dispositivo y pasar los datos de la firma

real a dicho almacén central de datos para propósitos de verificación. Los principios esenciales siguen siendo los mismos.

En un aspecto adicional de la invención, se proporciona un sistema de seguridad que incluye, por lo menos, un dispositivo como se describió antes en el presente y, por lo menos, un lector para dispositivos; dicho lector para dispositivos comprende un mecanismo para leer la respuesta magnética del dispositivo. En particular, el lector para dispositivos comprende o se proporciona en asociación con un generador de campo magnético, para aplicar un campo magnético variable en el tiempo a los elementos, y tiene un registrador de respuesta magnética para registrar la respuesta del elemento magnético ante ese campo magnético aplicado. Una realización de un lector para dispositivos se describe en el presente.

Para aplicaciones diferentes, los sistemas apropiados pueden comprender diversidad de lectores y/o una diversidad de dispositivos. Un sistema que comprende una diversidad de lectores puede estar organizado de tal manera que cada lector funcione independientemente aislado, o de tal manera que algunos o todos los lectores estén conectados en una red distribuida.

Los lectores proporcionados para un sistema operado de conformidad con el primer modo de operación señalado arriba, preferiblemente comprenden, además, mecanismos para leer la respuesta de la firma de la línea base predeterminada preregistrada, en particular la respuesta de la firma preregistrada y cifrada, almacenada en, con, o en asociación con un dispositivo o artículo protegido y, preferiblemente, comprenden un mecanismo comparador para comparar las respuestas de la firma de la línea base preregistrada y medida. Los lectores adaptados para un sistema para usarlos de conformidad con el segundo modo de operación descrito arriba, preferiblemente comprenden, además, mecanismos de

almacenamiento para almacenar la(s) respuesta(s) de la línea base predeterminada del dispositivo(s) que se intente(n) usar con ellos, y preferiblemente comprende medios de comparación para hacer una comparación entre las respuestas de la línea base almacenada y medida. Los lectores que se pretendan usar de conformidad con el tercer modo de operación descrito arriba, preferiblemente comprenden mecanismos para recibir datos relacionados con una respuesta de la firma de la línea base predeterminada almacenada a distancia, por ejemplo vía entrada directa de datos por un usuario o por medio de interrogación de una base de datos remota en una red distribuida, junto con un mecanismo comparador para comparar la respuesta predeterminada con la respuesta medida; o en una alternativa, un mecanismo para transmitir la respuesta medida a un comparador remoto, el cual incorpora o está en comunicación de datos con un almacén de respuestas predeterminadas.

En todos los casos, el lector para dispositivos preferiblemente hace una comparación entre las respuestas de la firma magnética de la línea base medida y predeterminada, por ejemplo contra un límite de tolerancia predeterminado, y activa un mecanismo de respuesta, dependiendo de si las firmas son idénticas, por ejemplo, dentro de esos límites de tolerancia.

El mecanismo de respuesta puede comprender un mecanismo simple de presentación, de cualquier forma apropiada, incluidos indicadores visuales, de audio, alfanuméricos y similares o si el dispositivo está autenticado. Adicionalmente o alternativamente, se pueden proporcionar otras respuestas. Por ejemplo, la autenticación podría servir para abrir una cerradura real o virtual, permitiendo el acceso a un área restringida, la operación de un artículo de equipo restringido, el acceso a un servicio particular o similares.

De acuerdo con un aspecto adicional de la invención, se describe un dispositivo simple el cual puede medir la respuesta magnética de un área pequeña de material magnético de película delgada. El dispositivo está bien ajustado, pero no limitado, para medir la firma magnética aleatoria de un dispositivo como el descrito arriba. El área pequeña tendrá de preferencia un tamaño de 0.2 mm x 0.2 mm o mayor; el espesor del material magnético estará en el rango de 1mm a 500 mm y, por preferencia estará en el rango de 1 nm a 50 nm. El material magnético puede ser una película continua o puede ser una colección de elementos magnéticos. El material magnético puede tener una sobrecapa de protección transparente. En varias realizaciones el material magnético se mantiene ópticamente reflectivo.

En varias realizaciones de acuerdo con este aspecto de la invención, un dispositivo para medir la respuesta magnética de un área de material magnético, cuando un campo magnético variable en el tiempo se aplica al material magnético, comprende una fuente de iluminación y en particular una fuente de iluminación infrarroja; un colimador para enfocar la iluminación sobre la superficie del material magnético y un colector para recoger la iluminación reflejada y monitorear la variación de la respuesta de esta reflexión con el paso del tiempo, cuando se aplica el campo magnético variable en el tiempo. Opcionalmente, el dispositivo incorpora o está provisto con un generador de campo magnético para generar dicho campo.

En varias realizaciones, el efecto magneto-óptico transversal Kerr se usa para medir la respuesta magnética del área del material magnético cuando al material magnético se le aplica un campo magnético variable en el tiempo. Este efecto es bien conocido en la literatura. El dispositivo que mide la respuesta puede incorporar mecanismos adicionales para aplicar un campo magnético variable en

el tiempo al área del material magnético bajo investigación, o se puede usar un dispositivo separado para aplicarlo.

En varias realizaciones, el dispositivo opera sin luz polarizada. Convencionalmente, el efecto transversal Kerr requiere que la luz de entrada esté en un plano polarizado. Usualmente, esto se logra insertando una hoja de Polaroid a algún otro elemento óptico polarizante en la trayectoria del haz de entrada. Sorprendentemente, se ha encontrado que en la aplicación para esta invención, el polarizador se puede retirar para disminuir los costos de fabricación y reducir el tamaño del dispositivo. En la realización preferida del presente dispositivo no se cuenta con un polarizador. Esto es apropiado para muchas aplicaciones. No obstante, se entenderá que puede estar incluido un polarizador, por ejemplo en la trayectoria del haz de entrada de manera convencional, cuando esto es deseable o necesario.

Preferiblemente, el colimador comprende una abertura diminuta. A la escala de operación del dispositivo esto se encuentra para enfocar efectivamente la luz sin necesidad de usar una lente. De nuevo, esto reduce el costo de fabricación y el tamaño del dispositivo. Convenientemente, el diámetro de la abertura diminuta está en el rango de 0.2 mm a 5 mm.

La luz se refleja, entonces, fuera de la superficie de la película magnética delgada. Preferiblemente, se proporciona una segunda abertura diminuta, con un diámetro en el rango de 0.2 mm a 5 mm, para enfocar la luz reflejada. Se prefiere que la segunda abertura diminuta tenga el mismo diámetro de la primera. La luz pasa a un colector que comprende un dispositivo fotosensible a la luz, el cual es de preferencia un fototransistor o un fotodiodo sensible a la radiación producida por la fuente de luz.

En varias realizaciones, la fuente de luz comprende un diodo emisor de luz. Esto contrasta con la técnica anterior de dispositivos a gran escala para medir el efecto magneto-óptico Kerr, donde se usa un láser, una lámpara de descarga o una lámpara incandescente. El presente dispositivo es más pequeño, más económico y retira los peligros asociados con un producto que contenga un rayo láser.

Se prefiere un diodo de emisión de luz infrarroja (LED) a un espectro visible LED por dos razones: las intensidades ópticas altas se logran en el infrarrojo debido a las corrientes más altas que los LED infrarrojos pueden sostener; el receptor óptico puede ser insensible a la luz visible y esto reduce la interferencia de la luz del ambiente.

En varias realizaciones, la fuente de luz comprende un diodo láser. Los diodos láser son relativamente baratos y pueden proporcionar una luz de alta intensidad.

En un aspecto adicional de la invención, un método de fabricación de un dispositivo de seguridad comprende formar por lo menos uno, y preferiblemente un gran número, de elementos magnéticos como se describen arriba; obtener una respuesta magnética de la firma de la línea base para los elementos, almacenar la respuesta de la línea base como una respuesta de la línea base predeterminada en una forma asequible para un usuario del servicio, opcionalmente mediante cifrado y almacenamiento, en asociación física con el dispositivo en cualquier forma legible.

En varias realizaciones, los elementos están formados por litografía óptica.

En varias implementaciones de acuerdo con este aspecto de la invención, se puede lograr un ahorro de costos en el proceso de litografía en el caso de los elementos magnéticos que comprenden una red de estructuras generalmente rectangulares. La sustancia protectora fotosensible se aplica en el sustrato de la manera usual y se sigue un patrón mediante una exposición óptica seguida por el desarrollo. Luego, el material magnético se deposita sobre la sustancia protectora fotosensible que sigue el patrón. Usualmente, la sustancia protectora fotosensible se disolverá en un solvente (proceso de levantamiento). Sin embargo, la sustancia protectora fotosensible puede quedar en su lugar debido a que el material magnético depositado en la parte superior de ella forma un segundo conjunto de elementos magnéticos rectangulares. Por ejemplo, supóngase que la resistencia se ha organizado en estructuras rectangulares con 0.5 μm de ancho con un espaciado de centro a centro de 1.5 μm . Si la sustancia protectora fotosensible se queda en su lugar, entonces las estructuras comprenden un conjunto de alambres de 0.5 μm acoplados al sustrato y un número igual (menos 1) de alambres de 1 μm acoplados a la parte superior del sustrato.

En un aspecto adicional, la invención comprende un método para marcar un artículo con propósitos de seguridad, identificación o autenticación, mediante el uso del dispositivo señalado y/o el sistema y/o el método y, en particular, mediante la asociación de un dispositivo como se describe ante sen el presente.

La invención en un aspecto adicional comprende un método de identificación o autenticación de un elemento mediante el uso del dispositivo anterior y/o el sistema y/o el método y, en particular, mediante asociación con un dispositivo como se describió antes en el presente, aplicando un campo magnético variable en el tiempo a los elementos de aquel, para obtener una respuesta de firma magnética de línea base medida, por ejemplo usando el lector descrito antes en el

presente, y comparando la respuesta medida con una respuesta de la firma magnética de la línea base registrada predeterminada.

Las realizaciones de la invención se describirán ahora, a manera de ejemplo solamente, con referencia a las figuras anexas en las cuales:

5 Las Figuras 1 a 4 muestran realizaciones de dispositivos de seguridad de acuerdo con la presente invención en vista en perspectiva;

La Figura 5 muestra una realización adicional de un dispositivo de seguridad de acuerdo con la presente invención en vista en planta;

10 La Figura 5a muestra otra realización de un dispositivo de seguridad de acuerdo con la presente invención en vista en planta;

La Figura 6 muestra otra realización de un dispositivo de seguridad de acuerdo con la presente invención presentada en vista transversal;

Las Figuras 7a a 7d ilustran modos de conmutación magnética de elementos magnéticos que se pueden usar en varias realizaciones de la presente invención;

15 Las Figuras 8a y 8b muestran curvas de histéresis idealizadas, esquemáticas, reales y promediadas para la conmutación magnética de un material permalloy que se puede usar en varias realizaciones de la presente invención;

20 Las Figuras 9a a 9h ilustran una técnica de fabricación para producir varias realizaciones de dispositivos de seguridad de acuerdo con la presente invención;

La Figura 10 muestra un montaje de lectura que forma parte de un sistema de seguridad para dispositivos de lectura, de acuerdo con varias realizaciones de la invención;

La Figura 11 muestra un activador de espejo para uso en un sistema de lectura para dispositivos de seguridad, de acuerdo con varias realizaciones de la invención;

La Figura 12 muestra una parte adicional que forma parte de un sistema de lectura para dispositivos de seguridad, de acuerdo con varias realizaciones de la invención;

La Figura 13 muestra una señal que activa un generador de campo magnético, de acuerdo con varias realizaciones de la invención;

La Figura 14 muestra una señal que activa el activador de espejo, de acuerdo con varias realizaciones de la invención;

La figura 15 muestra un ciclo de la señal de la Figura 13;

La Figura 16 muestra una señal detectora unipolar que representa una respuesta característica, de acuerdo con varias realizaciones de la invención;

La Figura 17 muestra una señal de sincronización para sincronizar diferentes sistemas de lectura para dispositivos de seguridad, de acuerdo con varias realizaciones de la invención;

La Figura 18 es una ilustración de una primera colección de elementos magnéticos usados para una firma magnética aleatoria/respuesta característica, de conformidad con la invención;

La Figura 19 es una ilustración de una segunda colección de elementos magnéticos;

La Figura 20 es una ilustración de una tercera colección de elementos magnéticos;

5 La Figura 21 es una ilustración de un dispositivo para medir la respuesta magnética de un área pequeña de película magnética delgada;

La Figura 22 es una ilustración de una realización de la invención en una tarjeta inteligente;

La Figura 23 es una ilustración de una realización de la invención en una
10 llave electrónica;

La Figura 24 es una ilustración de una realización de la invención en una etiqueta de identificación para un artículo que se ha de proteger;

La Figura 25 es una ilustración de una realización de la invención incorporada en un CD/DVD para propósitos de autenticación; y

15 La Figura 26 es una ilustración de una realización de la invención incorporada en un certificado para propósitos de autenticación.

En varias realizaciones, los materiales magnéticos se usan para formar elementos magnéticos sensibles a un campo magnético aplicado. La respuesta característica de estos elementos magnéticos ante el campo magnético aplicado da origen a una respuesta característica medible o una firma, para identificar un dispositivo de seguridad, incluido un conjunto de esos elementos magnéticos.

Están disponibles muchos tipos de materiales magnéticos, que podrían usarse para formar elementos magnéticos en diferentes formas bidimensionales y tridimensionales: por ejemplo, alambres magnéticos, alambres aplanados, barras, puntos, puntos aleatorios, centros dispersores aleatorios, etc. Aunque muchos de esos materiales se pueden usar en realizaciones de la invención, algunos materiales dan una mejor respuesta magnética que otros cuando están sujetos a un campo magnético aplicado; particularmente si las propiedades de conmutación magnética del material se van a usar como la respuesta característica medible, o como parte de ella.

Cuando las realizaciones de la invención usan las propiedades de conmutación magnética del material para producir una respuesta característica, los materiales magnéticamente suaves resultan útiles. Los materiales magnéticamente suaves son materiales ferromagnéticos en los cuales la magnetización se puede reversar con facilidad. Generalmente, estos materiales tienen ciclos de histéresis estrechos de forma cuadrada. Por eso, la magnetización de un elemento magnético hecho con estos materiales cambia de dirección en respuesta a un campo aplicado relativamente intenso. La coercitividad de estos materiales (es decir el campo inverso necesario para dirigir la magnetización de un elemento magnético fabricado en uno de estos materiales a cero después de saturado) tiende a ser relativamente baja, garantizando por ello que imanes con un

campo de intensidad relativamente baja se puedan usar para causar un cambio en la dirección de la magnetización del elemento magnético. Estos imanes con un campo de intensidad relativamente baja pueden ser bastante económicos, generalmente compactos y destinados a producir fácilmente un campo magnético controlado de buena uniformidad.

La Figura 1 muestra un dispositivo de seguridad (100). El dispositivo de seguridad (100) comprende varios elementos magnéticos (102) formados sobre un sustrato de silicio (104). Los elementos magnéticos (102) están hechos de permalloy.

La Figura 2 muestra un dispositivo de seguridad (200). El dispositivo de seguridad (200) comprende varios elementos magnéticos (202) formados sobre un sustrato de silicio (204). Los elementos magnéticos (202) están hechos de permalloy. El área de datos (206) se proporciona en el sustrato (204) para almacenar información de la respuesta característica premedida cifrada y/o un identificador único para identificar el dispositivo de seguridad (200).

El área de datos (206) de esta realización comprende un conjunto de agujeros grabados (no se muestran) que codifican datos binarios que corresponden a información de la respuesta característica premedida cifrada y/o un identificador único que se puede leer, por ejemplo, mediante un lector óptico (no se muestra) de una manera análoga a un disco compacto.

En variantes adicionales de esta realización, el área de datos (206) puede alternativamente, o adicionalmente, incluir circuitos electrónicos (no se muestran) que conservan la respuesta característica y/o la información de un identificador único.

La Figura 3 muestra un dispositivo de seguridad (300). El dispositivo de seguridad (300) comprende varios elementos magnéticos (302) formados sobre un sustrato de silicio (304). Los elementos magnéticos (302) están hechos de permalloy. El área de datos (306) se proporciona en el sustrato (304) para almacenar información de la respuesta característica premedida y cifrada y/o un identificador único para identificar el dispositivo de seguridad (300).

En el área de datos (306) de esta realización se proporcionan indicios (308). Los indicios (308) codifican datos que corresponden a información de la respuesta característica premedida cifrada y/o un identificador único que se puede leer mediante un lector (no se muestra). En una variante de esta realización, los indicios visibles (308) son proporcionados mediante un código de barras legible por máquina (no se muestra) que codifica la respuesta característica premedida cifrada y la información del identificador único. En otra variante de esta realización, los indicios visibles (308) son proporcionados mediante una máquina de código de barras legible (no se muestra) que codifica solamente la información del identificador único.

La Figura 4 muestra un dispositivo de seguridad (400). El dispositivo de seguridad (400) comprende varios elementos magnéticos (402) formados sobre un sustrato de silicio (404). Los elementos magnéticos (402) están hechos de permalloy. Cada elemento magnético (402) está cubierto con una capa reflectiva (410) hecha de oro, aluminio, cromo y/o tantalio, por ejemplo. Las capas reflectivas (410) aumentan el contraste de reflectividad entre los elementos magnéticos (402) y el sustrato (404). De ese modo, esta realización proporciona una relación señal a ruido mejorada (SNR), cuando el dispositivo de seguridad (400) está siendo interrogado por un dispositivo de lectura como, por ejemplo, un aparato de lectura del tipo descrito en el presente. Una ventaja de la SNR

aumentada es que permite que un dispositivo de seguridad (400) sea interrogado rápidamente para determinar si es o no una falsificación, y/o necesita niveles más bajos de luz incidente (por ejemplo, de ultravioleta a infrarrojo de 200 nm a 1500 nm) para ser interrogado.

5 La Figura 5 muestra una realización adicional de un dispositivo de seguridad (500) en una vista de planta. El dispositivo de seguridad (500) comprende varios elementos magnéticos (502a a 502e) formados sobre un sustrato de silicio (504). Los elementos magnéticos (502a a 502e) están hechos de permalloy en forma de alambres o alambres aplanados. Los extremos de los elementos magnéticos (505-
10 507) tienen formas angulares.

En esta realización, el ancho de los elementos magnéticos (502a a 502e) en la dirección A-A se puede hacer con varios anchos. En este caso, el ancho de los elementos magnéticos (502c y 502e) es aproximadamente el doble de los elementos magnéticos (502a, 502b y 502d). Dado que la magnitud de la señal de
15 la respuesta característica producida por cualquier elemento particular es proporcional al volumen del material del que está hecho el elemento, elementos más grandes dan origen a una señal más grande que, en consecuencia, es más fácil de medir.

Además, los elementos magnéticos (502a a 502e) por sí mismos se pueden
20 usar para codificar un identificador. En la realización ilustrada, los cinco elementos magnéticos (502a a 502c) ocupan un área de aproximadamente 1 mm x 1 mm con espacio suficiente para cerca de siete a doce elementos magnéticos con un ancho de 40 μm y una longitud de 900 μm de los elementos magnéticos (502a, 502b y 502d). El patrón de los cinco elementos magnéticos (502a a 502e) se usa para
25 proporcionar un identificador para el dispositivo de seguridad (500). Este patrón es

análogo a un código de barras que identifica un dispositivo de seguridad particular (500) y puede ser único para cada dispositivo de seguridad individual (500) que se fabrique.

El número de identificadores únicos que se pueden proporcionar mediante
5 variantes de esta realización, depende del número y densidad de los elementos magnéticos (502). Por ejemplo, realizaciones que tienen 32 elementos magnéticos posibles proporcionan una cantidad posible de 2^{32} identificadores únicos (es decir 4.294.967.296). Además, cuando los elementos magnéticos son identificables usando un patrón de barrido bidimensional, por ejemplo cuando los elementos
10 magnéticos (502) se proporcionan en una red de 32 x 32 puntos, esta figura puede ser cuadrada.

La Figura 5a ilustra otra realización. Se proporcionan varios elementos magnéticos (81 y 82) de diferentes longitudes. En esta realización, una respuesta característica se puede medir incluso a partir de lo que parece parte de un patrón
15 identificador como "espacios", dado que los bits efectivos de un identificador proporcionado por los elementos magnéticos (81) aún proporcionan una respuesta. La lectura se logra usando un haz de rayos láser que solamente puede ser enfocado en una dimensión, por ejemplo 1 mm de longitud y 20 micrones de ancho. Por consiguiente, cuando la intensidad reflejada se mide, por ejemplo,
20 usando el efecto magneto-óptico Kerr como se describe en el presente, cambia de acuerdo con la longitud de la barra. Típicamente, se pueden proporcionar barras de 30 μm de ancho con barras más largas (82) de alrededor de 700 μm de largo y barras más cortas (81), por ejemplo, algunas con 300 nm de longitud.

La Figura 6 muestra una realización de un dispositivo de seguridad (600) en
25 vista transversal. Aunque esta realización incorpora materiales que aumentan la

efectividad y el contraste, estos se pueden proporcionar por separado en otras realizaciones.

El dispositivo de seguridad (600) esta formado de un sustrato de silicio (604). El sustrato (604) incorpora capas reflectivas (603) formadas debajo de
5 elementos magnéticos (602) hechos de, por ejemplo, oro, aluminio, cromo, y/o tantalio. Las capas reflectivas (603) aumentan la señal óptica (incluida la señal del efecto Kerr, como se describe a continuación) reflejada desde los elementos magnéticos (602), en comparación con los elementos magnéticos formados directamente sobre un material de sustrato.

10 Adyacente a los elementos magnéticos (602) se forman las capas absorbentes (605) hechas de, por ejemplo, carbón. Las capas absorbentes (605) tienen una baja reflectividad y de ese modo aumentan el contraste entre la luz reflejada desde ellas y los elementos magnéticos adyacentes (602).

Otra variante de la realización que se muestra en la figura (6) usa, por
15 ejemplo, una superficie rugosa formada por deposición o grabado, como un material disperso en lugar de las capas absorbentes (605). El efecto del material disperso es atenuar cualquier señal óptica reflejada de las áreas adyacentes a los elementos magnéticos (602), con la ventaja adicional de que el dispositivo de seguridad (600) no necesita absorber tanta energía óptica.

20 Para caracterizar varios materiales que pueden tener respuestas deseables ante un campo magnético aplicado, en este punto es útil describir parte de la física involucrada en la conmutación de dirección de la magnetización de diferentes tipos de materiales ferromagnéticos. Esos materiales ferromagnéticos se pueden usar en varias realizaciones.

Con referencia a la figura 7a, se muestra un elemento magnético (102). En este ejemplo, el elemento magnético (102) está hecho de un material ferromagnético con la forma de un alambre aplanado. El elemento magnético (102) tiene una magnetización M con una magnitud y dirección iniciales indicadas por la flecha (150). Un campo magnético aplicado H se muestra aplicado al elemento magnético (102) en una dirección sustancialmente paralela a un eje longitudinal de elemento magnético (102), y con una polaridad opuesta a la magnetización inicial.

El campo magnético aplicado H actúa para invertir la polaridad de la magnetización del elemento magnético (102). Existen varios mecanismos físicos mediante los cuales se puede invertir la magnetización del elemento magnético (102). Cada uno de ellos conduce a una característica de conmutación magnética diferente de la magnetización M .

En un primer modo de conmutación (a veces referido como un modo de rotación coherente, que se muestra esquemáticamente en la figura 7b) las magnetizaciones individuales de varios dominios magnéticos (152) rotan en forma coherente, como se muestra esquemáticamente por las flechas entrecortadas (154). Así, en este modo, la magnetización general del elemento magnético (102) sigue una rotación direccional uniforme y la magnitud de la magnetización cambia para alinearse con el campo magnético aplicado H .

En un segundo modo de conmutación (en ocasiones referido como un modo de nucleación múltiple, que se muestra esquemáticamente en la figura 7c) muchos dominios magnéticos (156) dominan la conmutación de la magnetización del elemento magnético (102) cuando está presente un campo magnético aplicado H . Las magnetizaciones de los dominios individuales (156) inicialmente rotan para

alinearse con el campo magnético aplicado H , como se ilustra en la figura 7c. Posteriormente, los dominios crecen en tamaño. Sin embargo, en este modo la evolución temporal de la magnetización de la totalidad del elemento magnético (102) no se puede discernir fácilmente y puede cambiar en forma aleatoria en respuesta a condiciones del medio ambiente, tales como la temperatura.

Por eso, aunque los materiales que funcionan de acuerdo con el segundo modo de conmutación se pueden usar para elementos magnéticos de varias realizaciones, no son óptimos dado que, debido a que existe una variación menor en las propiedades de conmutación magnética para proporcionar una respuesta característica medida, resultan relativamente fáciles de copiar.

En un tercer modo de conmutación (en ocasiones referido como la paradoja de Brown, una conmutación intensa o un modo intermitente, se muestra esquemáticamente en la figura 7d), el crecimiento de un dominio magnético único (158) domina el cambio de magnetización del elemento magnético (102). Ese dominio (158) puede estar asociado con un defecto estructural en el elemento magnético (102) que se introduce en forma aleatoria durante un proceso de fabricación, por ejemplo mediante el ruido de fabricación incontrolable que surge de defectos aleatorios de materiales a nanoescala (por ejemplo defectos que ocurren en una escala de tamaño desde 0.5 nm hasta cerca de 500 nm) que son virtualmente imposibles de reproducir en forma controlada o predecible. En este modo, el crecimiento del dominio (158) domina la conmutación de la magnetización del elemento magnético (102) sobre una amplia variedad de condiciones ambientales y físicas. En consecuencia, los materiales que operan de acuerdo con el tercer modo son idealmente apropiados para el suministro de propiedades de conmutación magnéticas estables pero no predeterminadas, que proporcionan una respuesta característica reproducible y medible.

Varios defectos posibles pueden formar un centro de nucleación; estos defectos pueden incluir uno o más de los siguientes: fallas locales en la definición litográfica, por ejemplo, pequeños nodos (en micrones o submicrones) en los bordes de las puntas de los elementos; defectos cristalográficos locales como dislocaciones, inclusiones, anulaciones a escala nanométrica; variaciones locales en la composición química o la estequiometría, que conducen a un cambio local en la anisotropía magnética, y variaciones locales de corta escala en el espesor, que conducen a una indentación de la superficie lo cual puede generar campos de piel de naranja como lo contempló Brown.

- 10 La referencia *Introduction to the Theory of Ferromagnetism* de Amikam Aharony (ISBN 0 19 851791 2), pp. 204 a 214, presenta una visión general útil de muchos de los conceptos antes mencionados.

La Figura 8a muestra un ciclo de histéresis único idealizado (160) que indica la manera en que la magnetización M de un elemento magnético (102) hecho de permalloy varia como una función de un campo magnético aplicado H . Las líneas punteadas (169) indican la manera en que el ciclo de histéresis único idealizado (160) puede variar respecto al ideal para un elemento magnético real (102). El elemento magnético (102) comienza con una magnetización inicial (172). El campo aplicado H se aumenta hasta que llega a un valor (170). De ahí en adelante, el campo aplicado H aumenta hasta un valor de conmutación (168) donde, debido a la histéresis, el elemento magnético (102) cambia rápidamente su magnetización M de la magnetización inicial (172) a una magnetización (164). Después de esto, el campo magnético aplicado H disminuye hasta un valor de conmutación (174) donde, debido a la histéresis, el elemento magnético (102) rápidamente cambia su magnetización M de la magnetización (164) para regresar a la magnetización inicial (162).

Como se observa en la Figura 8a, las características de conmutación magnética del elemento magnético (102) hecho de permalloy se ven para funcionar en el modo de conmutación intensa, incluso cuando los ciclos de histéresis reales se desvían del ideal, cuando las transiciones de la magnetización de una polaridad a otra aún están intensamente definidas.

La figura 8b ilustra un ciclo de histéresis promediado (180) para muchos (por ejemplo, ~100) ciclos del elemento magnético (102) hechos de permalloy alrededor de los ciclos de histéresis de la figura 8a. Se observa que el ciclo de histéresis promediado (180) no muestra transiciones fuertes en el estado de magnetización del elemento magnético (102), aunque ocurren transiciones intensas para cada ciclo magnético individual (160). La razón para esto es que los valores de conmutación (168 y 174) de cada ciclo magnético individual (160) varían entre ciclos, lo cual da origen a fluctuaciones.

La magnitud Δ de la fluctuación (196) determinada como la desviación estándar de las diferencias en los valores de conmutación (168) para los diversos ciclos magnéticos (160) se muestra en relación con el ciclo de histéresis promediado (180). A su turno, la magnitud de la fluctuación Δ proporciona una respuesta característica para el elemento magnético (102) que la genera. La magnitud de la fluctuación depende del volumen preciso y de la energía del centro de nucleación que es responsable de la inversión de la magnetización. Por tanto, varía de un elemento magnético a otro, dado que no es probable que dos defectos nucleantes sean iguales.

La coercitividad también es una medida característica que indica unicidad. En varias realizaciones, la coercitividad suministra una respuesta característica mejor que la fluctuación. En esas realizaciones, la fluctuación se puede medir como un

parámetro adicional de la respuesta característica. Vista desde una perspectiva, una función de distribución que representa el campo de reversión/conmutación (de un elemento magnético único), cuando se observa a través de muchas reversiones/conmutaciones, tiene un valor central de la distribución que
5 corresponde a la coercitividad y una distribución amplia, representativa de la fluctuación.

Varias realizaciones de un dispositivo de seguridad que incorporan elementos magnéticos pueden proporcionarse. A manera de ejemplo, ahora se describirá un proceso de fabricación de varios dispositivos de seguridad en un
10 substrato de silicona, usando litografía óptica.

El proceso de fabricación se ilustra en las figuras 9a a 9h. El proceso comienza en la Figura 9a con una rodaja de silicio limpia y pulida (704). En varias realizaciones, el substrato de silicio tiene aproximadamente 0.5 mm de espesor para facilitar el manejo y proporcionar un dispositivo de seguridad resistente. Una
15 capa de la sustancia protectora fotosensible (714) se distribuye sobre la rodaja para dar una cobertura uniforme como se muestra en la figura 9b. La rodaja y la capa de la sustancia protectora fotosensible (714) se homean para fijar dicha capa (714).

La Figura 9c ilustra el dispositivo de la Figura 9b después de la exposición a
20 la radiación UV o casi radiación UV (por ejemplo, a 405 nm). Las regiones (708) representan las regiones expuestas. Las regiones expuestas (708) están escritas directamente sobre la superficie superior (701) de la capa de sustancia protectora fotosensible (714) que usa un sistema directo de litografía óptica de barrido de escritura, disponible comercialmente como, por ejemplo, un sistema NanoMOKE2
25 con un accesorio LaserWriter suministrado por Durham Magneto Optics Ltd. De

esta manera, un patrón individual unidimensional o bidimensional se puede escribir sobre la capa de la sustancia protectora fotosensible (714) para cada dispositivo de seguridad que se fabrique. Este patrón puede definir una variedad de formas de alambre como, por ejemplo, las que se ilustran en la Figura 1

- 5 La Figura 9d muestra el dispositivo de la Figura 9c después de que ha sido desarrollado para retirar la sustancia protectora fotosensible expuesta (708). La remoción de la sustancia protectora fotosensible expuesta (708) expone partes (710) del substrato de silicio subyacente (704).

Posteriormente, como se muestra en la Figura 9e, los elementos magnéticos
10 (702) formados de permalloy como, por ejemplo $\text{Ni}_{80}\text{F}_{20}$ (véase, por ejemplo Bozorth, *Ferromagnetism*, ISBN 0-7803-1032-2, para información adicional) se depositan en las partes expuestas (710) mediante deposición por sublimación catódica o un proceso de evaporación, típicamente para un espesor en el rango de cerca de 10 a cerca de 100 nm, por ejemplo, cerca de 40nm. También se forman
15 capas adicionales (712) de permalloy en la película protectora fotosensible restante que no está expuesta (706), durante el proceso de deposición por sublimación catódica.

A continuación, sobre las capas de permalloy (712) y los elementos magnéticos (702), se forman capas metálicas aislantes (716, 718) de oro o
20 aluminio, como se ilustra en la Figura 9f. La capa aislante (718) esta diseñada para proteger la capa de permalloy de la oxidación y además proporciona una reflectividad óptica ampliada.

La sustancia protectora fotosensible no expuesta (706) junto con las capas superpuestas de permalloy (712) y las capas aislantes (716) se retiran usando un
25 solvente apropiado, por ejemplo acetona, para dejar la estructura ilustrada en la

Figura 9g. La estructura resultante comprende los elementos magnéticos (702) formados sobre el substrato de silicio (704) separados por las regiones del substrato de silicio expuestas (720). Las superficies superiores de los elementos magnéticos 702 están aisladas mediante capas aislantes (718).

5 La estructura resultante arriba mencionada se pone dentro de una cámara de deposición química en fase vapor ampliada por plasma (PECVD), donde una capa de dióxido de silicio (SiO_2) (722) se deposita sobre las regiones superiores del substrato de silicio expuestas (720) y las capas aislantes (718). La capa de dióxido de silicio (722) forma una capa ópticamente transparente (incluyendo, entre otras,
10 una capa que es sustancialmente transparente a la radiación electromagnética infrarroja). El dispositivo de seguridad resultante (700) se muestra en la Figura 9h.

Cuando se fabrican varios dispositivos de seguridad (700) sobre un substrato de silicio único (704), el substrato de silicio (704) puede dividirse posteriormente en varios dispositivos de seguridad individuales (700).

15 Los solicitantes han producido varios prototipos de dispositivos de seguridad usando el proceso descrito antes en el presente. Durante la producción de estos dispositivos de seguridad prototipo, los parámetros del proceso deposición por sublimación catódica usados fueron como sigue: energía de 250W; presión base 5×10^{-7} mbar; gas argón, presión del gas 1 a 12 mTorr; flujo de 5 cc por minuto;
20 velocidad de rotación del substrato 10 rpm; velocidad de deposición 1 a 1.5 Angstroms por segundo; y una temperatura del substrato de 22 °C a 27 °C. También es posible aplicar un campo magnético paralelo al plano del dispositivo durante el proceso de fabricación.

Los solicitantes indican a partir de un análisis de sus dispositivos de
25 seguridad prototipo, que el ajuste adecuado de la velocidad de crecimiento y/o la

presión de la sublimación catódica para los elementos magnéticos puede producir mejoras en las características de conmutación magnética del modo de conmutación intensa. Los solicitantes también han indicado a partir de un análisis de sus dispositivos de seguridad prototipo que materiales magnéticamente suaves
5 tienden a producir propiedades de conmutación magnética deseables.

Una vez que un dispositivo de seguridad se ha fabricado, se somete a prueba, bien sea solo o como parte de un lote de dichos dispositivos de seguridad, para determinar su respuesta característica. La respuesta característica se mide para garantizar que proporciona una identificación adecuada del dispositivo de
10 seguridad en particular.

Los elementos magnéticos se prueban primero para determinar si operan o no en el modo de conmutación intensa. Un magnetómetro Kerr, como se describe en *Applied Physics Letters*, Vol. 73, p. 3947, 1998, se usa para medir la coercitividad en varios puntos de cada elemento magnético individual. Por
15 ejemplo, se pueden usar cinco puntos en cada elemento y medir la coercitividad en cada punto. Se considera que existe conmutación magnéticamente intensa si la variación entre los valores de coercitividad medidos de un elemento magnético es pequeña en comparación con la variación entre las coercitividades medidas a través de varios elementos. En la práctica, las estructuras magnéticamente
20 intensas cambian con un variación menor de 0.2 Oe, a través del elemento, mientras que un elemento puede diferir en coercitividad respecto a otro, aproximadamente de 1 a 2 Oe.

Una medida de la fluctuación también se puede tomar para cada elemento magnético, o para un grupo de dichos elementos, repitiendo medidas de ese
25 elemento/grupo y determinando cuánto varía la coercitividad entre conjuntos de

medidas. Estos conjuntos de medidas se repiten muchas veces para cada grupo/elemento magnético del dispositivo de seguridad. En un ejemplo, la coercitividad se puede medir en un punto en un dispositivo de seguridad, cien veces por cada elemento magnético/grupo de elementos magnéticos a 5 temperatura ambiente. Los valores de coercitividad medidas se ajustan entonces a una curva en la campana de Gauss, y se calculan la coercitividad media y la fluctuación (como se indica por la media y la desviación estándar Δ de la curva gaussiana ajustada, respectivamente).

Los solicitantes han encontrado que para varias realizaciones, sobre una 10 temperatura de operación probablemente típica (por ejemplo de $-20\text{ }^{\circ}\text{C}$ a $50\text{ }^{\circ}\text{C}$ cuando en un lector se proporcionan medidas antiempañamiento), la fluctuación exhibió solamente una dependencia de temperatura débil.

En varias realizaciones hay una dependencia medible de la coercitividad media respecto de la temperatura. Sin embargo, considerando que la coercitividad 15 media de varios elementos magnéticos varia en la misma forma con la temperatura, las diferencias de coercitividad entre elementos magnéticos se mantienen casi constantes. Así, cuando se comparan la coercitividad media medida contra la respuesta característica premedida, se puede hacer una concesión para una compensación constante entre los dos conjuntos para 20 compensar las temperaturas diferentes.

Sin embargo, si se desea o requiere para otras realizaciones, se pueden tomar medidas de coercitividad y fluctuación a diferentes temperaturas, incluidas temperaturas fuera del rango de temperatura normal de operación. Por ejemplo, se podrían tomar grupos de medidas en cada elemento magnético a $-50\text{ }^{\circ}\text{C}$, $0\text{ }^{\circ}\text{C}$ y

65 °C, para un dispositivo de seguridad calificado para operación entre -20 °C hasta cerca de 50 °C.

En la práctica se debe establecer un límite superior en la variación permitida entre los valores de coercitividad medidos para un elemento magnético único. Este puede ser un valor absoluto (por ejemplo, 0.2 Oe) o estar determinado en relación con la magnitud de la fluctuación (por ejemplo, 10% del valor de fluctuación medido). Deben ser rechazados los dispositivos de seguridad que tengan uno o más elementos magnéticos que causen valores de variación de coercitividad mayores que la variación permitida.

Una característica deseable es que cualquier variación debida a la fluctuación sea menor, para que la coercitividad media sea más fácil de medir. La coercitividad media puede usarse, entonces, como un parámetro para una respuesta característica premedida. La fluctuación también se puede usar como parámetro para la respuesta característica premedida, por ejemplo, además de la coercitividad media para elementos magnéticos respectivos o grupos de tales elementos.

En varias realizaciones, la respuesta característica premedida de los dispositivos de seguridad puede estar definida por un valor de coercitividad media y/o un valor de fluctuación Δ , para varios elementos magnéticos o grupos de elementos magnéticos. En otras realizaciones se usa, por ejemplo, un valor de coercitividad media o un valor de fluctuación para representar una respuesta característica premedida. En el uso, la respuesta característica premedida de un dispositivo de seguridad se compara con su respuesta característica medida para determinar si ese dispositivo de seguridad es una falsificación.

La respuesta característica premedida se puede codificar, por ejemplo, digitando los valores de coercitividad media y/o el valor de fluctuación Δ . En varias realizaciones, estos valores se cifran para almacenarlos en el dispositivo de seguridad correspondiente, con o sin un identificador que puede ser único. En

5 otras realizaciones, estos valores se almacenan a distancia del dispositivo de seguridad correspondiente. En varias realizaciones, durante una operación de lectura (como se describe adelante) los valores digitados de coercitividad media y/o el valor de fluctuación Δ que representan una respuesta característica premedida se pueden recuperar/recobrar para un dispositivo de seguridad en

10 particular y comparar con los valores medidos de coercitividad media y/o el valor de fluctuación Δ , para un dispositivo de seguridad que pretende ser el mismo dispositivo, para determinar si el dispositivo de seguridad cuya respuesta característica se ha medido, es una falsificación o no..

Los dispositivos de seguridad pueden estar acoplados a artículos para

15 ayudar a identificar esos artículos como genuinos o no falsificados. En el uso, es necesario leer la respuesta característica de un dispositivo de seguridad en particular, para que se pueda comparar con una respuesta característica premedida como, por ejemplo, una respuesta de la línea base. Cualquier diferencia entre la respuesta medida y la respuesta premedida, por fuera de

20 cualquiera de los límites permisibles, indica que el dispositivo de seguridad que se ha leído es una falsificación. Como la producción de centros de nucleación magnética está fuera del control del fabricante, cualquier copia del dispositivo casi invariablemente dará como resultado una respuesta característica diferente como, por ejemplo, valores de coercitividad media y de fluctuación.

Se contemplan varias realizaciones de sistemas, tanto manuales como de otro modo. Varias de tales realizaciones se describen adelante en relación con las Figuras 10 a 17 de los dibujos.

La Figura 10 muestra un montaje para lectura (930) que forma un
5 componente de un sistema de lectura para dispositivos de seguridad, para obtener una respuesta característica medida de un dispositivo de seguridad (900), mientras el dispositivo de seguridad (900) está sujeto a un campo magnético aplicado (932). El montaje para lectura (930) puede detectar cambios en la polarización de la luz reflejada por los elementos magnéticos, usando el efecto
10 magneto-óptico Kerr (MOKE).

El montaje para lectura (930) comprende un bloque de aluminio (934), cuyas superficies interna y externa se oscurecen usando una pintura antirreflexiva negro mate. El tamaño del bloque de aluminio (934) es típicamente de 2 cm x 2 cm x 1 cm. El bloque de aluminio (934) comprende los canales de trayectoria del haz
15 (938, 940, 942). Un diodo de láser visible o cerca al infrarrojo (936), que se proporciona con un sistema óptico colimador (no se muestra) puede funcionar para producir un haz de rayos láser colimado (944) con una longitud de onda de, por ejemplo, 600 a 1550 nm. En una realización se usa un diodo láser que funciona a 670 nm. El haz de rayos láser (944) atraviesa un primer canal de
20 trayectoria del haz (938), antes de salir del bloque de aluminio (934) y es incidente sobre un espejo (950).

El haz de rayos láser (944) se refleja desde el espejo (950) hacia un segundo canal de trayectoria del haz (940) que se forma en el bloque de aluminio (934). Un polarizador (952) colocado en el segundo canal de trayectoria del haz (940)
25 convierte el haz de rayos láser (944) en un haz de rayos láser polarizado en un

plano (947). Entonces, el haz de rayos láser polarizado en un plano (947) deja el segundo canal de trayectoria del haz (940).

El bloque de aluminio (934) también comprende un tercer canal de trayectoria del haz (942). El tercer canal de trayectoria del haz (942) está orientado de manera que recoge la luz reflejada (949) desde un dispositivo de seguridad (900) cuando se hace la lectura. Típicamente, si un dispositivo de seguridad (900) tiene elementos magnéticos con forma de alambre o alambre aplanado (902), el campo aplicado (932) se aplica en una dirección fundamentalmente paralela al eje de los elementos magnéticos (902).

Un analizador (954), usado en varias realizaciones, incorpora una placa de cuarto de onda opcional y un polarizador que se pone en el tercer canal de trayectoria del haz (942). El analizador (954) deja pasar la luz de una primera polaridad y bloquea la luz de una segunda polaridad ortogonal. La luz de la primera polaridad se refleja desde un elemento magnético (902) cuando se encuentra en un primer estado de magnetización saturado, y la luz de la segunda polaridad se refleja desde el elemento magnético (902) cuando está en un segundo estado de magnetización saturado, que tiene una polaridad principalmente inversa o intensidad modificada con respecto al primer estado de magnetización.

El polarizador (952) y el analizador (954) están distribuidos para medir la señal longitudinal del efecto magneto-óptico Kerr que se produce cuando el haz de rayos láser polarizado en un plano (947) es incidente sobre los elementos magnéticos (902). También se pueden usar otras distribuciones del efecto magneto-óptico Kerr, por ejemplo, que incluyen distribuciones sin un polarizador y/o un analizador y/o que usan una distribución transversal o polar. Sin embargo,

un beneficio de usar una distribución longitudinal del efecto magneto-óptico Kerr es que generalmente proporciona una señal mejorada en comparación con las distribuciones transversal o polar.

Con el tercer canal de trayectoria del haz (942) está alineada una unidad
5 detectora (956) la cual, en esta realización incorpora una lente de enfoque y un
circuito fotodiódico o un circuito de fototransistor, sensible a la radiación de
iluminación. El circuito fotodiódico es sensible a la luz transmitida a través del
analizador (954) para proporcionar una señal proporcional a la magnetización de
cualesquier elementos magnéticos (902) iluminados por el haz de rayos láser
10 polarizado en un plano (947).

La Figura 11 muestra un activador de espejo (969) para mover un espejo
(950). Dicho activador de espejo (969) se puede usar junto con el montaje para
lectura (930) descrito en el presente. El activador de espejo (969) comprende un
electroimán (971) que funciona para desviar un elemento de desviación (982) en
15 acero dulce acoplado a él. El electroimán (971) comprende una primera bobina
activadora (986) enrollada en una primera región de un núcleo magnético (980), y
una segunda bobina activadora (988) enrollada en una segunda región de un
núcleo magnético (980). El núcleo magnético (980) incluye una abertura (992) en
la cual se produce un campo de desviación magnética cuando el electroimán se
20 energiza.

El elemento de desviación (982) está conectado al núcleo magnético (980)
por medio de una tuerca roscada (984). Al apretar la tuerca roscada (984) se
asegura el elemento de desviación (982), al núcleo magnético (980) en el extremo
proximal del elemento de desviación (982). Por consiguiente, el extremo distal del
25 elemento de desviación (982) que no está asegurado a la bobina roscada (984) se

puede mover con respecto al núcleo magnético (980) bajo la influencia del campo de desviación magnética, debido a la fuerza de atracción generada entre el campo de desviación magnética y el acero dulce del material del elemento de desviación (982). El espejo (950) está montado sobre una parte del elemento de desviación (982) y se mueve en respuesta al movimiento del elemento de desviación (982).

En operación, una corriente de excitación pasa a través de la primera y segunda bobinas activadoras (986, 988). La primera y segunda bobinas activadoras (986, 988) se pueden conectar en serie, de manera que la misma corriente de excitación pasa a través de ambas bobinas. El paso de una corriente de excitación inicial a través de la primera y segunda bobinas activadoras (986, 988) hace que el elemento de desviación (982) se desvíe en la dirección mostrada por la flecha (990), desviando con ello también el espejo (950).

La Figura 12 muestra un sistema de generación del campo (935), un sistema de detección (937), un sistema de procesamiento y control (939) y un sistema de barrido por haces (941) que forman, junto con el montaje para lectura (930) descrito arriba, una parte adicional de una realización de un sistema de lectura para dispositivos de seguridad.

El sistema de generación del campo (935) comprende componentes para producir un campo magnético aplicado variable en el tiempo (932), para aplicar a un dispositivo de seguridad (900). El sistema de generación del campo (935) comprende un circuito excitador (966) que funciona con las bobinas impulsoras para generación del campo (933a, 933b) en respuesta a una señal excitadora de la bobina (970). La señal excitadora de la bobina (970) es una señal sinusoidal periódica, compuesta de varias formas de onda sinusoidales individuales (972) que oscilan a una frecuencia de 100 Hz (véase Figuras 13 y 15), que activa las

bobinas impulsoras de generación del campo (933a, 933b) para producir un campo magnético con oscilación sinusoidal que oscila a 100 Hz. En esta realización, la forma de onda sinusoidal de 100 Hz se produce mediante un circuito oscilador electrónico convencional (no se muestra)

5 El sistema de generación del campo (935) adicionalmente comprende un detector transversal (968) para detectar cambios de polaridad en la señal excitadora de la bobina (970). El detector transversal (968) produce una señal de sincronización (981) como respuesta al ser excitado por el circuito excitador (966), como se muestra en la Figura 17. La señal de sincronización (981) está
10 compuesta por una secuencia de picos (983) producidos en el momento en que cambia la polaridad de la señal excitadora de la bobina (970). En otras realizaciones, el mismo microcontrolador que registra la señal de Kerr se usa para generar la secuencia del campo aplicado (por medio de un convertidor digital-analógico), de modo que el microcontrolador pueda controlar la sincronización que
15 se presenta entre ellos.

El sistema de detección (937) comprende una unidad detectora (956) para producir una señal en respuesta a la luz incidente (948). La unidad detectora (956) está acoplada a un amplificador (958). Las señales producidas por la unidad detectora (956) son amplificadas por el amplificador (958) para proporcionar una
20 señal detectora unipolar (973) (véase Figura 16). La señal detectora unipolar (973) alimenta entonces un convertidor analógico-digital (ADC) (960) para digitalización. El ADC (960) es un dispositivo de 10 bits que funciona con una frecuencia de muestreo de 10 kHz, con lo cual da 1024 niveles de datos discretos posibles para cada una de las 100 muestras tomadas con el paso del tiempo para un periodo de
25 un ciclo de 100 Hz a completar.

En una realización, el ADC (960) funciona a 10 kHz y adquiere cerca de 100 puntos de datos por ciclo del campo magnético aplicado. El campo aplicado se aplica a una frecuencia de cerca de $10 \text{ kHz} / 100 = 100 \text{ Hz}$. Los datos se promedian para cerca de 0.5 sec; es decir, que hay 50 grupos de datos promediados para un solo elemento magnético. A partir de esto se miden la coercitividad media y la fluctuación. El proceso entonces se repite para otro elemento magnético. En total, de esta manera se analizan alrededor de 8 elementos magnéticos.

El sistema de procesamiento y control (939) se usa para adquirir datos medidos representativos de la respuesta característica del dispositivo de seguridad (900) del sistema de detección (937), para analizar los datos medidos y compararlos con una respuesta característica premedida, para determinar si el dispositivo de seguridad (900) es genuino. En varias realizaciones, el sistema de procesamiento y control (939) también controla un sistema de barrido por haces (941) que hace que el haz de rayos láser polarizado en un plano (947) se mueva a través de la superficie del dispositivo de seguridad (900).

El sistema de procesamiento y control (939) comprende una unidad de procesamiento (962) que tiene un almacén de datos asociado (974). En varias realizaciones, la unidad de procesamiento (962) comprende un microprocesador o un microcontrolador y memoria asociada (no se muestra), incluido un separador de anillo, los cuales son alimentados constantemente con muestras de datos del ADC (960), cuando el separador de anillo es habilitado por el microprocesador.

Cuando arranca el sistema de lectura para dispositivos de seguridad, el microprocesador deshabilita el separador de anillo. Para comenzar a acumular datos en el separador de anillo, el microprocesador recibe un primer pico (983). Esto activa el microprocesador para comenzar un conteo del número de picos de

sincronización (983) que son recibidos y simultáneamente habilitar el separador de anillo. Así, los datos comienzan a acumularse en el separador de anillo en sincronía con una transición de polaridad que se presenta en el campo magnético aplicado (932). Cuando el microprocesador detecta el pico enésimo (983) (por ejemplo, el 100) se envía una señal para inhibir la acumulación de datos adicionales en el separador de anillo. En este momento, el separador de anillo contendrá N conjuntos de datos acumulados durante la mitad del ciclo del campo magnético aplicado (972), y cada conjunto de datos representa una parte respectiva digitalizada (975, 977) de la señal detectora unipolar (973), en un momento dado durante el tiempo de duración t ($t = N \times \text{frecuencia del campo magnético aplicado} / 2$) de la acumulación de datos. (Por ejemplo, $t = 0.5$ segundos de duración para 100 ciclos a 100 Hz con $N = 100$, y se toman 5,000 medidas individuales con una velocidad del ADC establecida en 10 kHz)

Para una realización que incluye un sistema de barrido por haces (941) acoplado a un activador de espejo (969), también se puede usar una unidad procesadora (962) para proporcionar señales de control para mover la posición de un espejo (950). El sistema de barrido por haces comprende un circuito excitador (964) que incluye un convertidor digital-analógico, que establece la corriente proporcionada a través de la primera bobina activadora (986) y la segunda bobina activadora (988). El conjunto de circuitos de conmutación está configurado para conectar en serie la primera y segunda bobinas activadoras (986, 988), y para aplicar una corriente excitadora en proporción a una tensión de control (994) (véase Figura 14) proporcionada por la unidad procesadora (962).

En una realización, el separador de anillo acumula varios conjuntos que comprenden de N conjuntos de datos. Una vez que se ha acumulado un conjunto de N conjuntos de datos, el microprocesador deshabilita el separador de anillo

hasta que los N conjuntos de datos quedan almacenados en el almacén (974). Entonces, la unidad procesadora (962) aumenta la tensión de control (994) para hacer que el espejo (950) desvíe un haz polarizado en un plano (947) hacia otra área del dispositivo de seguridad (900). Después de un periodo de retraso corto para permitir que el activador de espejo (969) se estabilice, el microprocesador espera un primer pico (983) y posteriormente comienza a adquirir los siguientes N conjuntos de datos. Este proceso continúa hasta que se han acumulado N conjuntos de datos y se han almacenado para cada posición del espejo (950).

Como se indicó arriba, los conjuntos de datos pueden acumularse de varias maneras. Una vez adquiridos, los datos se pueden procesar para extraer información variada con respecto a la respuesta de la señal característica medida. A los conjuntos de datos se les pueden aplicar algoritmos estándar para calcular la coercitividad media medida y/o la fluctuación como dadas por una medida de la desviación estándar de las medidas de coercitividad. Ejemplos de los algoritmos pueden encontrarse en *Numerical Recipes in C: The Art of Scientific Computing*, W. H. Press, S.A. Teukolsky, W. T. Vetterling and B. P. Flannery, (Cambridge University Press, Cambridge, 1993).

El ajuste de los datos se puede hacer con el mismo microprocesador/microcontrolador que determina la respuesta de la señal característica medida, o mediante un sistema de computador conectado. Por ejemplo, cuando una base de datos remota almacena la respuesta característica premedida, los datos brutos de la respuesta de la señal característica medida puede ser transmitidos a un procesador remoto para realizar un ajuste gaussiano. De manera similar, cuando se usa como parte de un sistema para detectar fraudes, un lector puede conectarse a un computador tipo palm-top que almacena los datos de la respuesta característica premedida descargándola de internet, y la

compara con la respuesta de la señal característica medida. En varias realizaciones, las computadoras tipo palm-top se pueden usar como la pantalla interactiva del lector, y también como un medio de acceso a bases de datos remotas; por ejemplo, usando teléfonos GSM.

- 5 Existen varias formas para determinar la respuesta característica premedida de un dispositivo de seguridad. Estas formas varían de acuerdo con el tipo de dispositivo de seguridad y dependen, por ejemplo, de si la respuesta característica premedida se almacena/codifica o no en el dispositivo de seguridad; de si la respuesta característica premedida está cifrada o no; y de si se proporciona o no
- 10 un identificador único en asociación con el dispositivo de seguridad. Todas estas posibilidades proporcionan realizaciones factibles.

En varias realizaciones, un identificador único y una respuesta característica premedida cifrada, que comprenden datos codificados que representan una coercitividad media y una desviación estándar en la fluctuación medida, se

15 codifican en un dispositivo de seguridad como una secuencia de puntos diminutos. Los puntos diminutos se forman en una dirección colineal con una dirección de barrido por haces, proporcionados por un activador de haz (969). Antes de determinar la respuesta característica medida, el activador de haz (969) está dirigido a proporcionar un haz de puntos sobre el dispositivo de seguridad, en

20 donde se considera que están los puntos diminutos. En cada uno de esos puntos, se mide una señal de la unidad detectora (956). Una reflectividad alta indica un cero lógico para el bit de datos que corresponde con el punto respectivo, y una reflectividad baja indica un cero lógico.

De hecho, el haz de rayos láser polarizado en un plano (947) de varias

25 realizaciones puede enfocarse usando un sistema de lentes para tener un foco de

tamaño pequeño en un dispositivo de seguridad (900). De manera similar, puede proporcionarse un conjunto de elementos ópticos en el canal de la trayectoria del haz (942) para ayudar a reunir la luz reflejada desde el dispositivo de seguridad (900).

5 En otras realizaciones, una tarjeta inteligente cuenta con un dispositivo de seguridad, y un identificador único e información cifrada de una respuesta característica premedida están almacenados en la tarjeta inteligente. La tarjeta inteligente se lee de una manera convencional y se mide una respuesta característica medida, como se describe en el presente.

10 En ciertas realizaciones, los mismos elementos magnéticos de un dispositivo de seguridad pueden usarse para codificar información adicional. Ellos pueden, por ejemplo, codificar un identificador único mediante la formación de un patrón de formas. Dichos dispositivos de seguridad pueden ser barridos para ver primero si hay algún elemento magnético en varias ubicaciones posibles. Entonces se puede
15 usar un patrón de barrido lineal de la señal reflejada, para obtener un identificador de valor binario para el dispositivo de seguridad. Una manera de visualizar esto es considerar el patrón de los elementos magnéticos para representar una forma de código de barras.

20 Para realizaciones de un dispositivo de seguridad que comprende elementos magnéticos que codifican un identificador único, se puede medir una respuesta característica como se describe antes en el presente, para cada elemento individual. Sin embargo, varios lectores solamente pueden medir la respuesta característica de un subconjunto de los elementos magnéticos para acelerar el proceso de lectura.

En una realización de un sistema de lectura para dispositivos de seguridad, la información de la respuesta característica premedida se almacena en una base de datos a la cual tienen acceso una o más unidades de procesamiento. La información de la respuesta característica premedida preferiblemente está cifrada.

- 5 Dicho sistema puede ser distribuido y comprende un servidor remoto acoplado a través de una red a uno o más lectores para dispositivos de seguridad. Un sistema de acuerdo con esta realización funciona para determinar un identificador único para cada dispositivo de seguridad a partir del patrón de elementos magnéticos, o por otros medios, y recuperar la información de la respuesta característica
- 10 premedida que corresponda con el identificador único determinado por el sistema de lectura para dispositivos de seguridad. Entonces, la información de la respuesta característica premedida puede descifrarse, según sea necesario, por un lector del dispositivo de seguridad respectivo.

- En realizaciones del sistema de lectura para dispositivos de seguridad, una
- 15 vez que la información relacionada con la respuesta de la señal característica medida ha sido extraída, se compara por medio del microprocesador con la respuesta característica premedida, posiblemente descifrada usando una clave privada de datos asimétricos, para determinar si el dispositivo de seguridad puede ser clasificado o no como no falsificado. Esa comparación se hace dentro de un
- 20 margen de error permitido para variaciones que se introducen, por ejemplo, por fluctuaciones de temperatura. Por ejemplo, para la coercitividad media/fluctuación, esto puede ser cuando la coercitividad/fluctuación medidas no difieran de la coercitividad/fluctuación premedidas en más de una desviación estándar de la distribución de los valores de la coercitividad media/fluctuación.

- 25 Con referencia a las Figuras 18: a 20, se proporcionan una vista en planta de tres ejemplos de estructuras de elementos magnéticos.

En la primera se muestra una colección de elementos magnéticos (1) regulares rectangulares, en forma esquemática y no a escala. El material de los elementos es $\text{Ni}_{80}\text{Fe}_{20}$, que se extiende con un grosor de 40 nm. El área total de la parte de la firma es de 1 mm por 1 mm. La ilustración solamente es esquemática y no a escala. En particular se debe apreciar que cada área de 1 mm por 1 mm comprenderá una gran cantidad de elementos con un ancho en escala de micrones.

Además, cualquier representación en que los elementos sean iguales de ancho solamente es esquemática. Una red en que el ancho de los alambres sea de 1 μm , podría ser apropiada para algunas aplicaciones. Sin embargo, como se indicó arriba, con frecuencia se preferirá una red de grupos discretos de alambres de diferente ancho que den varios campos de conmutación discretos (por ejemplo como se describió arriba), o una red continuamente variable de manera lineal o de otra manera funcional (por ejemplo como se describe arriba).

La Figura 19 muestra una estructura generalmente similar que, por lo general, tiene dimensiones similares. De nuevo se aplican las advertencias anteriores sobre la naturaleza esquemática de los anchos de las ilustraciones. Sin embargo, en este caso, las partes rectangulares (2) no tienen extremos cuadrados sino que cuentan con extremos en punta. Los extremos con formas diferentes pueden afectar el campo de conmutación, y por eso se prefieren para ciertas aplicaciones. Se puede usar cualquier extremo con forma apropiada, sin que se aleje de los principios de la invención.

En la Figura 20 se muestra una alternativa más, la parte de la firma que comprende generalmente una red cuadrada de 1 mm por 1 mm de micropuntos magnéticos circulares (3). En este caso el grosor del material es cerca de 100 nm.

Cada micropunto tiene 100 μm de diámetro. De nuevo, esto solamente es ilustrativo. Pueden considerarse formas alternativas y, de nuevo, elementos que varían discretamente o continuamente en tamaño y/o forma, considerando que se satisfaga el requerimiento básico para un dispositivo, de conformidad con la invención, de que se obtenga una respuesta de la firma de la línea base medible y reproducible.

La película se extiende por cualquier método apropiado, en particular por litografía óptica, tal como se usa el método descrito en el presente.

La Figura 21 ilustra un dibujo mecánico de un ejemplo de un dispositivo pequeño apropiado para medir la respuesta magnética de un área pequeña de película magnética delgada, tal como una película magnética que comprende una firma magnética de conformidad con la invención; por ejemplo, las firmas que se ilustran en las Figuras 18 a 20.

El dispositivo para medir la respuesta magnética comprende una fuente luminosa de alta intensidad; en este caso, un diodo dentro de la caja (11) que emite luz infrarroja. La luz es colimada por un solo agujero diminuto (12), con un diámetro que está en el rango de 0.2 mm a 5 mm. Luego, la luz se refleja en la superficie de la película magnética delgada en posición (15) contra ella y pasa a través de un segundo agujero diminuto (13) con un diámetro que está en el rango de 0.2 mm a 5 mm, y preferiblemente con el mismo diámetro del primer agujero.

La luz reflejada pasa luego a un dispositivo fotosensible dentro de la caja (14), la cual de preferencia es un fototransistor o un fotodiodo sensible a la radiación infrarroja. En la ilustración de esta realización, el dispositivo fotosensible se selecciona para baja sensibilidad a la luz visible, permitiendo usar el dispositivo

sin apantallamiento óptico. El dispositivo también se puede pintar de negro para reducir las reflexiones de luz parásita.

Las bobinas del campo magnético (no se muestran) están acopladas al dispositivo para aplicar campos magnéticos en el rango de 0 a 500 Oe al material magnético que está bajo prueba. En el caso del material magnético bajo prueba que comprende una red de elementos elongados, tales como rectángulos, de preferencia las bobinas del campo magnético están orientadas para aplicar un campo en el plano de la película y paralelas al eje largo de las estructuras elongadas o en un ángulo con respecto al eje largo que esté en el rango de 0° a 60°. Puede haber bobinas adicionales del campo magnético para aplicar un campo adicional transversalmente al eje largo del alambre.

El fototransistor u otro dispositivo que reciba la luz está conectado a elementos electrónicos apropiados (no se muestran), los cuales registran la intensidad reflejada desde material magnético mientras una corriente alterna pasa a través de las bobinas que generan el campo magnético aplicado. Los elementos electrónicos que procesan la señal usando un chip procesador de señal digital o un chip microcontrolador registran las respuestas medidas durante un número de ciclos del campo magnético aplicado y los agregan en forma coherente para reducir el ruido. El número de ciclos registrados será tal que el tiempo de adquisición total no excede 10 segundos, y por conveniencia no excederá de 5 segundos. Entonces, los elementos electrónicos que procesan la señal identifican el campo de conmutación medio para cada una de las transiciones de conmutación importantes en la señal registrada. Estas pasan después a otros elementos electrónicos (no se muestran), los cuales adquieren y, si es necesario, descifran la respuesta de la línea base prerregistrada en una banda magnética, tarjeta inteligente, código de barras óptico o desde una fuente de texto remota o

almacén de datos electrónicos u otros medios, o alternativamente transmiten la respuesta medida a un comparador de datos remoto con acceso a la respuesta de la línea base prerregistrada, y se hace una comparación.

La Figura 22 ilustra la aplicación de la presente invención a una tarjeta con chips inteligentes, de diseño generalmente convencional de otro modo. La tarjeta (21), que típicamente tiene el tamaño de una tarjeta de crédito o similar, y que de hecho se puede usar como una tarjeta de crédito o similar, se ilustra en una vista en planta desde arriba (A) y desde abajo (B). La tarjeta lleva información alfanumérica, pero su principal sistema de almacenamiento de información es el chip inteligente (22). Este está protegido por un código de barras opcional (23) y una banda magnética (24), la cual típicamente se proporciona para compatibilidad inversa con sistemas únicamente de banda magnética.

En la parte posterior de la tarjeta se aplica un dispositivo de firma magnética (26) que comprende una red de elementos magnéticos de 1 mm por 1 mm, de diseño apropiado de conformidad con la invención. Por conveniencia, en el ejemplo mostrado, está dentro del ángulo sólido del haz del chip inteligente mismo, como se ilustra con la línea entrecortada (28). Para muchas aplicaciones podría ser conveniente poner el elemento magnético (26) dentro de este ángulo sólido del haz. Un enfoque alterno para lograr el mismo efecto podría ser incorporar el dispositivo de firma magnética con un ancho relativamente pequeño de 1 mm, en un espacio especialmente ampliado entre los contactos del chip inteligente. Sin embargo, dicha ubicación es puramente por conveniencia, y los elementos magnéticos (26) podrían colocarse en algún otro lugar de la tarjeta.

Al momento de la fabricación de la tarjeta, se toma una lectura inicial de la firma de la línea base. Una manera de hacerlo es usando un magnetómetro de

barrido. En la ilustración de la realización de una tarjeta inteligente, la respuesta de la línea base se almacena en la tarjeta, que ha sido firmada primero digitalmente usando un algoritmo de cifrado asimétrico, como el RSA. La clave pública entonces puede estar disponible para un usuario y/o quedar almacenada en una terminal lectora e incluso en la tarjeta misma, sin comprometer la seguridad. La firma puede usarse, entonces, para verificar que la tarjeta es un producto genuino del fabricante y eliminar la amenaza de uso fraudulento de copias clonadas de la tarjeta, lo cual constituye una fuente creciente de fraude en transacciones financieras y fraude de identificación.

En el uso, la tarjeta se lee con un lector de tarjetas apropiado, en particular con un lector de tarjetas que incorpora un lector para dispositivos de firmas, como el que se ilustra en la figura 21. El lector para dispositivos puede estar incorporado en un lector de tarjetas inteligentes existente. Por ejemplo, con la realización mostrada, el dispositivo de lectura para el elemento magnético debe leer el lado opuesto de la tarjeta respecto al que lee el lector de tarjetas inteligentes, y de ese modo se puede incorporar en un lector convencional para tarjetas inteligentes, relativamente con pocas dificultades de ingeniería. De esta manera, las tarjetas y los lectores se mantienen compatibles hacia atrás con la tecnología convencional de tarjeta/lector que no tiene el sistema de identificación y autenticación descrito en el presente.

El lector mide una respuesta real de la tarjeta. En la tarjeta también se almacena una respuesta de línea base esperada. Esta se puede almacenar en cualquier forma legible pero está convenientemente incorporada en uno de los dispositivos existentes para almacenamiento de datos. Por ejemplo, la firma de la línea base se puede registrar en su forma cifrada en el chip inteligente (22), el código de barras (23) o la banda magnética (24). Así, el lector puede leer la firma

magnética real y la firma magnética esperada prerregistrada y predeterminada. El lector está adaptado para comparar las dos firmas, dentro de ciertos límites de tolerancia, y para indicar si la tarjeta está autenticada o no, como resultado de esa comparación.

- 5 La tarjeta inteligente, de conformidad con varias realizaciones de la invención, será aplicable a todas las circunstancias en que se esté usando la tecnología convencional de tarjetas inteligentes incluyendo, sin limitación, tarjetas de crédito y bancarias, tarjetas de identificación y autenticación, y similares. Proporciona un mecanismo para autenticar la tarjeta como genuina y de ese modo
- 10 proporciona un obstáculo significativo contra el uso fraudulento de copias falsificadas de tarjetas originales.

- El sistema representado por la realización que se muestra en la Figura 22 es un sistema simple, en el cual un dispositivo, de conformidad con varias realizaciones de la invención, sirve simplemente para autenticar la tarjeta como un
- 15 producto de fabricación genuina y así detectar copias falsificadas y, en consecuencia, la respuesta de la línea base predeterminada está convenientemente almacenada en la tarjeta. Se entenderá fácilmente que dicho sistema es solamente un ejemplo del modo de operación. En una alternativa, la firma original "esperada" podría estar almacenada en cualquier otro lugar. Por
- 20 ejemplo, en relación con el uso de una tarjeta como la que se ilustra en la Figura 22, como parte de un sistema de servicios financieros, por ejemplo una tarjeta de crédito, se puede contemplar un sistema en donde se emiten variedad de tarjetas, donde hay muchos lectores en uso y donde los lectores comprenden una red distribuida con un almacén central de datos que mantendrá los detalles del cliente
- 25 que se adaptarán más adelante para procesar la información de la firma para propósitos de verificación, de conformidad con los principios descritos en el

presente. Otros modos de operación también se sugerirán rápidamente por sí mismos.

En la Figura 23 se proporciona una ilustración del uso de una de las realizaciones de la presente invención en un montaje de cerradura y llave. Una tarjeta de clave (31) de material sólido apropiado, por ejemplo un material plástico apropiado, se proporciona con el dispositivo (36) que comprende una red de elementos magnéticos de 1 mm por 1 mm, como se describió previamente.

La tarjeta de clave se proporciona en asociación con un montaje de lector de tarjetas/cerradura ilustrado esquemáticamente en el resto de la Figura 23.

La cerradura (32) incorpora una ranura (33) en la cual se puede introducir el extremo de la tarjeta de clave (31). Cuando se pone apropiadamente en este sitio, el dispositivo (36) queda adyacente a un lector (34) del diseño general que se ilustra en la Figura 21.

El lector (34) obtiene una lectura de la respuesta magnética del dispositivo (36) en la manera predescrita, y pasa esta respuesta a una unidad de control (35). La unidad de control (35) almacena o de otro modo tiene acceso a la respuesta esperada predeterminada, por ejemplo almacenando ésta dentro de la cerradura, opcionalmente en forma cifrada. La comparación se realiza y en caso de que se encuentre correspondencia dentro de las tolerancias predeterminadas, se pasa una instrucción a los mecanismos de control (38) para activar las palancas de cierre (39) y abrir la cerradura.

Aunque el ejemplo ilustrado en la Figura 23 es una cerradura electromecánica, de hecho se entenderá que los principios de la presente invención son igualmente aplicables en todas las circunstancias en que se pudiera

considerar un mecanismo de cierre físico o virtual u otro mecanismo de control. De acceso. Por ejemplo, sin limitación, un dispositivo paralelo a las líneas de la realización que se ilustra en la Figura 23 se podría usar junto con una cerradura electrónica para una puerta u otro cierre, junto con un encendido electrónico para un vehículo, junto con un inmovilizador electrónico para un vehículo, como un mecanismo para controlar el acceso a una pieza de equipo electrónico, por ejemplo exigiendo la inserción antes de que el equipo funcione, como un mecanismo para restringir el acceso a un servicio en particular, etc.

En la realización ilustrada, se ilustra una tarjeta en asociación con la cerradura. En la práctica, incluso para cerraduras simples para un solo usuario, probablemente sea necesario proporcionar varias claves. Está en la naturaleza de la presente invención que éstas tendrán dispositivos de firma diferentes. De acuerdo con ello, la cerradura necesitaría almacenar y responder a las firmas de la línea base para cada uno de estos dispositivos. También se pueden contemplar modos más complejos de operación cuando una cerradura proporciona acceso a varios usuarios o, cuando se proporcionan varias cerraduras en asociación con varios usuarios.

En un primer ejemplo de dicha operación, se proporcionan varias cerraduras y varias llaves en asociación con un sistema de entrada para múltiples usuarios en un área segura. En un segundo ejemplo de dicho modo de operación, se proporcionan varias tarjetas de operador para la operación de control de equipo de oficina para múltiples usuarios. En estos ejemplos, todas las firmas de la línea base autorizadas pueden estar almacenadas en todas las cerraduras, o alternativamente las cerraduras pueden estar conectadas sobre una red distribuida a una base de datos central que almacena detalles de las tarjetas de todos los usuarios autorizados. Dicho sistema permite no sólo una buena seguridad debido

a la dificultad de producir tarjetas falsificadas, sino que también permite controlar y monitorear el acceso en una forma activa.

En la Figura 24 se ilustra una realización adicional de la invención. En la Figura 24, un dispositivo de seguridad de conformidad con la invención (46) está incorporado en un rótulo acoplable a un artículo que se va a identificar/proteger. El rótulo comprende una pestaña plástica (41), la cual incorpora, opcionalmente, información alfanumérica, un código de barras (44), etc. para almacenar, por ejemplo, información de identificación, información de origen, información de precios o similares, acerca del artículo que se va a rotular. La pestaña (41) está acoplada a un elemento que se va a rotular, por medio de la banda de acoplamiento (42). En la realización ilustrada, la banda de acoplamiento (42) se pretende como un acoplamiento de cinta simple. El acoplamiento puede ser removible o permanente. Cuando la seguridad y permanencia del acoplamiento del rótulo tienen particular importancia, rápidamente se contemplaría un acoplamiento más complejo, que incluiría, por ejemplo, mecanismos de cierre, mecanismos de prevención de manipulación no autorizada, mecanismos de indicación de manipulación no autorizada, y similares.

La realización de la Figura 24 permite rotular artículos de manera temporal o permanente, cuando no es práctico o deseable incorporar un dispositivo de conformidad con la invención, directamente en el artículo mismo. Ejemplos de modos de uso incluyen, sin limitación, rótulos mejorados de seguridad para equipajes de líneas aéreas, rótulos de autenticidad para artículos de marca de alto valor, en particular ropa y similares, rótulos de origen e identificación para los mismos, para propósitos de control de inventarios y, por ejemplo, para identificar originales y, por consiguiente, controlar la importación no autorizada de artículos genuinos de marca dirigidos para otro mercado; marcado de artículos con

propósitos de control de inventarios, marcado de precios de artículos, rótulos que se usan de manera que dificultan que un comprador cambie el ticket de precio (por uno más bajo) de otro artículo, para obtener bienes con un precio bajo fraudulento.

5 El modo normal de operación de un rótulo del tipo ilustrado en la Figura 24 será la autenticación. De acuerdo con esto, la información de la firma prerregistrada usualmente se almacenará en la pestaña (41). La información prerregistrada se almacenará en una forma apropiada legible por máquina. En el ejemplo dado se podría incorporar en el código de barras. Se proporcionará un
10 lector adaptado para leer la firma magnética del dispositivo (46) y la firma cifrada esperada, y para efectuar una comparación para autenticar el rótulo. La efectividad de la seguridad del rótulo se basa en que es muy difícil de copiar, dado que la naturaleza aleatoria de la firma significa que un rótulo plagiado será identificable como tal.

15 La Figura 25 ilustra un disco de almacenamiento de datos, tal como un CD, DVD o similares, a los cuales se ha aplicado un dispositivo, de conformidad con la invención. El disco (51) incorpora una pestaña de firma magnética (56) que comprende elementos magnéticos como se describió arriba, preferiblemente dentro del área muerta (53), sin llevar datos de otro modo. En otra parte del disco
20 se proporciona una lectura predeterminada cifrada de la firma (56).

En su forma más simple, en un primer modo de operación, el sistema le permite al fabricante autenticar CD/DVD originales, identificar copias falsificadas y en asociación con un sistema de control de inventarios apropiado, rastrear el origen y destino de los originales genuinos, e identificar importaciones no
25 autorizadas y similares.

En un modo de operación más avanzado, los lectores de disco se pueden fabricar incorporando lectores de dispositivos para leer el dispositivo (56) y autenticar el disco, y los cuales quedarán deshabilitados para ejecutar copias no autorizadas. También es posible contemplar un sistema en el que dichos lectores
5 modificados se puedan usar en conjunto con el sistema de identificación/autenticación como parte de un contrato de licencia para usuario final.

La Figura 26 es un ejemplo del uso de la invención en un documento de identificación formal. Dicho documento podría ser un documento de identificación
10 o de autorización, como un pasaporte, licencia de conducción, certificado de autorización o calificación o similares, una certificación de identificación o autorización dirigida a acompañar, verificar o identificar de otro modo un artículo, o cualquier otro documento en el que las copias falsificadas pudieran ser un problema.

15 El documento (61) del ejemplo incluye información visual (62), por ejemplo, una fotografía, información escrita (63) y un código de barras (64). Podría incluir otros dispositivos de seguridad o almacenamiento de datos.

Un dispositivo que comprende elementos magnéticos como los de arriba (66) está incorporado en el documento. Este dispositivo es legible en la manera
20 descrita arriba. En un modo de operación, el dispositivo (66) sirve para un propósito de autenticación simple, y en el documento también está incorporada una lectura preregistrada cifrada de la respuesta magnética esperada. Convenientemente en el ejemplo dado, esto se podría incorporar en el código de barras o almacenar de otro modo en una forma legible. Sin embargo, se apreciará
25 que en sistemas más sofisticados fuera posible almacenar a distancia la firma

magnética esperada, opcionalmente con identificación adicional y/u otros detalles de seguridad.

El dispositivo de conformidad con la invención, aplicado a la documentación en esta forma sirve básicamente como una forma de protección contra el plagio.

- 5 Por consiguiente, sirve como un dispositivo de autenticación económico y conveniente en todas las circunstancias en que exista vulnerabilidad ante el fraude por la falsificación de originales genuinos, por ejemplo en relación con documentos de identificación, certificados formales, documentos financieros como cheques, papel moneda y similares, documentos legales importantes y otra documentación
- 10 de esa clase.

Visto desde otro aspecto, se proporciona un mecanismo de un dispositivo de seguridad que comprende, por lo menos, un mecanismo de elemento magnético, en donde dicho mecanismo de elemento magnético es sensible ante un campo magnético aplicado para proporcionar una respuesta característica.

- 15 Visto desde un aspecto adicional, se proporciona un método de fabricación de un dispositivo de seguridad que comprende el paso de proporcionar, por lo menos, un elemento magnético, en donde dicho por lo menos un elemento magnético proporciona una respuesta característica en respuesta a un campo magnético aplicado.

- 20 Visto desde otro aspecto adicional, se considera un sistema para leer un mecanismo de un dispositivo de seguridad que comprende un mecanismo de generación de un campo magnético para aplicar un campo magnético aplicado a un dispositivo de seguridad, y un mecanismo de detección para medir uno o más parámetros representativos de una respuesta característica medida de dicho
- 25 dispositivo de seguridad, en respuesta a dicho campo magnético aplicado, en

donde dicho sistema funciona para comparar dicho(s) parámetro(s) representativo(s) de una respuesta característica medida con uno o más parámetros respectivos de una respuesta característica premedida, para determinar si respecto de dichos parámetros son sustancialmente equivalentes.

- 5 Visto desde otro aspecto, se proporciona un método para leer un dispositivo de seguridad que comprende el paso de aplicar un campo magnético aplicado a un dispositivo de seguridad; el paso de medir uno o más parámetros representativos de una respuesta característica medida de dicho dispositivo de seguridad en respuesta a dicho campo magnético aplicado; y el paso de comparar
- 10 dicho(s) parámetro(s) representativo(s) de una repuesta característica medida con uno o más parámetros respectivos de una repuesta característica premedida, para determinar si con respecto a dichos parámetros son sustancialmente equivalentes.

Visto desde un aspecto adicional, se proporciona un mecanismo de producto que comprende el mecanismo del dispositivo de seguridad como se describe en el

15 presente.

Quienes tienen destreza común en la técnica, entenderán que se pueden usar otras técnicas para producir dispositivos de seguridad. Por ejemplo, en lugar de producir dispositivos de seguridad que usen un proceso de levantamiento/grabado en húmedo, se puede usar el grabado con un haz de

20 iones. Quienes tienen destreza común en la técnica, también serán conscientes de que varias realizaciones de dispositivos de seguridad pueden fabricarse usando distintos sustratos, incluidos, por ejemplo, silicio, vidrio, plástico, metales, etc.

Aunque algunos de los materiales de ejemplo descritos en el presente son ferromagnéticos, quienes tienen destreza común en la técnica entenderán que se

25 pueden usar otros tipos de elementos magnéticos y/o no magnéticos,

considerando que ocasionan una respuesta característica medible apropiada. Por ejemplo, pueden usarse elementos no magnéticos cuando dichos elementos producen una respuesta medible en un campo magnético aplicado, donde esa respuesta se puede medir para proporcionar una respuesta característica.

- 5 Quienes tienen destreza común en la técnica serán conscientes de que se pueden usar varias técnicas para fabricar y caracterizar elementos magnéticos apropiados para dispositivos de seguridad. Un ejemplo de una de dichas técnicas de fabricación y uno de dichos procesos de caracterización pueden encontrarse en *Optimised process for the fabrication of mesoscopic magnetic structures*, Adeyeye et al, Journal of Applied Physics, Vol. 82, No. 1, pp. 469-473, 1 July 1997, en el
- 10 cual se investiga el efecto del tamaño del elemento magnético sobre las propiedades magnéticas de este.

- Realizaciones producidas de conformidad con la invención, pueden incorporar medidas para aumentar la reflectividad/contraste, bien sea solas o en
- 15 alguna combinación. Materiales como oro, aluminio, cromo y/o tantalio se pueden disponer debajo y/o arriba de elementos magnéticos para aumentar su reflectividad y/o la señal Kerr que proporcionan los elementos magnéticos. Las áreas de un dispositivo de seguridad pueden ser tratadas para reducir su reflectividad con el fin de mejorar la reflectividad/contraste entre los elementos
- 20 magnéticos y las áreas que los circundan.

- En varias realizaciones se proporcionan elementos magnéticos en forma de alambres o alambres aplanados. La forma del extremo de esos alambres puede ser controlada durante la fabricación de un dispositivo de seguridad. Por ejemplo, se puede proporcionar un extremo inclinado en un ángulo de 60° hasta cerca de
- 25 90°. En otras realizaciones, pueden proporcionarse extremos aplanados y/o

semicirculares para influir en la nucleación magnética. La forma de los extremos puede elegirse para proporcionar características de conmutación magnética mejoradas.

Aunque la invención ha sido descrita en relación con realizaciones
5 particulares, se apreciará que no está limitada a ellas, y que es posible que muchas variaciones se encuentren dentro del alcance de esta invención.

Se apreciará que algunas realizaciones de la invención descrita arriba se pueden implementar y/o configurar, por lo menos en parte, usando un aparato para procesamiento de datos como, por ejemplo, hardware, programas cableados
10 y/o un computador configurado con un programa de computador. El programa de computador puede almacenarse en un medio transportador en una forma que sea útil para el aparato para procesamiento de datos. El medio transportador puede ser, por ejemplo, memoria de estado sólido, memoria óptica o magneto-óptica como un disco legible y/o inscribible, por ejemplo un disco compacto y un disco
15 versátil digital, o memoria magnética como un disco o cinta, y el aparato para procesamiento de datos puede utilizar el programa para configurarlo para operación. El programa de computador puede proporcionarse desde una fuente remota incorporada en un medio transportador, tal como una señal electrónica, incluida una onda portadora de alta frecuencia o una onda portadora óptica.

20 Quienes tienen destreza común en la técnica, serán conscientes de que la descripción en el presente se relaciona simplemente con ejemplos ilustrativos de cómo puede tener efecto la invención, y que pueden contemplarse muchas realizaciones que incorporan uno o más componentes, por ejemplo de otras realizaciones, junto con realizaciones adicionales que no están descritas
25 explícitamente en el presente. Por ejemplo, velocidades de adquisición de datos,

velocidades de muestreo, número y tamaño de niveles de cuantificación de muestras, velocidades de ciclo del campo magnético aplicado, el número de conjuntos de datos acumulados, etc. todos pueden ser variados/seleccionados como se desee. Esos parámetros pueden ser programados en forma variable, por ejemplo, bajo el control de un microprocesador, posiblemente dependiendo de varias condiciones medidas, como, por ejemplo, temperatura.

El alcance de la presente invención incluye cualquier característica novedosa o combinación de características divulgadas en el presente explícitamente o implícitamente o cualquier generalización de ellas, sin considerar si se relacionan o no con la invención reivindicada o alivia alguno o todos los problemas abordados por la presente invención. Por el presente, el solicitante da aviso de que se pueden formular nuevas reivindicaciones a dichas características durante el proceso de esta solicitud o de cualquier solicitud adicional derivada de ella. En particular, con referencia a las reivindicaciones, cláusulas, aspectos y párrafos anexos, las características de reivindicaciones, cláusulas, aspectos y/o párrafos dependientes pueden combinarse con las reivindicaciones, cláusulas, aspectos y/o párrafos independientes, y las características de reivindicaciones, cláusulas, aspectos y/o párrafos independientes respectivos pueden combinarse de cualquier manera apropiada, y no solamente en las combinaciones específicas enumeradas.

REIVINDICACIONES

1. Un dispositivo de seguridad que comprende, por lo menos, un elemento magnético, en donde dicho elemento magnético es sensible ante un campo magnético aplicado para proporcionar una respuesta característica.
- 5 2. El dispositivo de seguridad de la Reivindicación 1, en donde por lo menos un elemento magnético está sostenido por un substrato.
3. El dispositivo de seguridad de la Reivindicación 2, en donde por lo menos un elemento magnético está sostenido en dicho substrato.
4. El dispositivo de seguridad de cualquier Reivindicación precedente, en
10 donde por lo menos un elemento magnético es sensible ante el campo magnético aplicado para cambiar la magnetización o la polarización magnética de por lo menos un elemento magnético.
5. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está hecho de un material que
15 funciona en un modo de conmutación intensa.
6. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está hecho de un material magnéticamente suave.
7. El dispositivo de seguridad de la Reivindicación 6, en donde por lo menos
20 un elemento magnético comprende un material magnéticamente suave seleccionado de uno o más de: níquel, hierro, cobalto y aleaciones de ellos entre sí o con silicio, como aleación níquel hierro, aleación cobalto hierro, aleación hierro silicio o aleación cobalto silicio.

8. El dispositivo de seguridad de las Reivindicaciones 6 ó 7, en donde el material magnéticamente suave es un permalloy.
9. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético tiene sustancialmente forma de alambre o alambre aplanado.
10. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está protegido con una capa que refleja la luz.
11. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está cerca de una parte con reflectividad reducida a la luz del dispositivo de seguridad.
12. El dispositivo de seguridad de cualquier Reivindicación precedente que comprende varios elementos magnéticos.
13. El dispositivo de seguridad de la Reivindicación 12, en donde varios elementos magnéticos están distribuidos para proporcionar un patrón lineal.
14. El dispositivo de seguridad de la Reivindicación 12, en donde varios elementos magnéticos están distribuidos para proporcionar un patrón bidimensional.
15. El dispositivo de seguridad de la Reivindicación 13 o de la Reivindicación 14, en donde el patrón codifica un identificador.
16. El dispositivo de seguridad de cualquier Reivindicación precedente que comprende además un identificador único incorporado en él

17. EL dispositivo de seguridad de la Reivindicación 16, en donde el identificador único se proporciona por medio de uno o más códigos de barras legibles ópticamente; uno o más indicios ópticos; un identificador codificado magnéticamente, y un identificador electrónico.

5 18. El dispositivo de seguridad de la Reivindicación 17, montado en una tarjeta inteligente, en donde el identificador electrónico está en un chip de tarjeta inteligente, que se encuentra en dicha tarjeta inteligente.

10 19. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde la información de la respuesta característica premedida que representa uno o más parámetros medibles de dicha respuesta característica se almacena en el dispositivo de seguridad.

20. El dispositivo de seguridad de la Reivindicación 19, en donde la información de la respuesta característica premedida está en forma cifrada.

21. Un método de fabricación de un dispositivo de seguridad que comprende:

15 proporcionar por lo menos un elemento magnético, en donde por lo menos un elemento magnético proporciona una respuesta característica en respuesta a un campo magnético aplicado.

22. El método de la Reivindicación 20 que comprende proporcionar por lo menos un elemento magnético en un sustrato.

20 23. El método de la Reivindicación 21 o de la Reivindicación 22, que comprende formar por lo menos un elemento magnético usando un proceso de levantamiento o grabado en húmedo.

24. El método de la Reivindicación 21 o de la Reivindicación 22, que comprende formar por lo menos un elemento magnético usando un proceso de grabado con un haz de iones.

25. El método de cualquiera de las Reivindicaciones 21 a 24 que comprende
5 medir la(s) magnitud(es) de uno o más parámetros magnéticos de por lo menos un elemento magnético.

26. El método de la Reivindicación 25, que comprende medir uno o más valores de coercitividad y fluctuación.

27. El método de la Reivindicación 25 o de la Reivindicación 26, que
10 comprende usar la(s) magnitud(es) medida(s) de uno o más parámetros magnéticos para representar la información de la respuesta característica premedida.

28. El método de la Reivindicación 27, que comprende cifrar la información de la respuesta característica premedida.

15 29. El método de la Reivindicación 27 o de la Reivindicación 28 que comprende almacenar la información de la respuesta característica premedida en forma cifrada o descifrada en un dispositivo de seguridad.

30. El método de la Reivindicación 27 o de la Reivindicación 28 que comprende almacenar la información de la repuesta característica premedida en forma cifrada
20 o descifrada en un medio de almacenamiento remoto con respecto a dicho dispositivo de seguridad.

31. El método de la Reivindicación 30 que comprende almacenar dicha información de la respuesta característica premedida en forma cifrada o descifrada en una base de datos.

5 32. El método de cualquiera de las Reivindicaciones 21 a 31, que además comprende proporcionar dicho dispositivo de seguridad con un identificador único.

33. El método de la Reivindicación 32 cuando dependa de cualquiera de las Reivindicaciones 28 a 31 que comprenden almacenar una representación de dicho identificador único en asociación con información de la respuesta característica premedida.

10 34. Un sistema para leer un dispositivo de seguridad que comprende:

un sistema de generación de un campo magnético para aplicar un campo magnético a un dispositivo de seguridad; y

15 un sistema de detección para medir uno o más parámetros representativos de una respuesta característica premedida de un dispositivo de seguridad en respuesta a un campo magnético,

en donde el sistema funciona para comparar uno o más parámetros representativos de una respuesta característica medida con uno o más parámetros respectivos de una respuesta característica premedida, para determinar si los parámetros medidos y premedidos respectivos son sustancialmente equivalentes.

20 35. El sistema de la Reivindicación 34, en donde el sistema de generación del campo magnético funciona para aplicar un campo magnético variable en el tiempo a un dispositivo de seguridad.

36. El sistema de la Reivindicación 34 o la Reivindicación 35, en donde el haz de luz se usa para interrogar un dispositivo de seguridad.

37. El sistema de cualquiera de las Reivindicaciones 34 a 36, en donde dicho haz de luz es un haz visible o cerca al infrarrojo producido por un diodo láser.

5 38. El sistema de cualquiera de las Reivindicaciones 34 a 37, en donde los parámetros representan uno o más valores de coercitividad y fluctuación.

39. El sistema de cualquiera de las Reivindicaciones 36 a 38, en donde el sistema de detección incorpora un dispositivo de detección del efecto magneto-
10 óptico Kerr, para detectar cambios inducidos en el haz de luz por elementos magnéticos del dispositivo de seguridad.

40. El sistema de la Reivindicación 39, en donde el aparato de detección del efecto magneto-óptico Kerr está configurado para operar en modo transversal.

41. El sistema de cualquiera de las Reivindicaciones 36 a 40, que funciona además para desviar un haz de rayos de luz a través de la superficie del
15 dispositivo de seguridad.

42. El sistema de cualquiera de las Reivindicaciones 34 a 41, que funciona además para leer un identificador único del dispositivo de seguridad.

43. El sistema de la Reivindicación 42, en donde el identificador único es identificado por el reconocimiento de un patrón de elementos magnéticos
20 soportados por el dispositivo de seguridad.

44. El sistema de la Reivindicación 42 o de la Reivindicación 43, en donde el identificador único es identificado por leer uno o más de: un código de barras

legible ópticamente, uno o más indicios ópticos, un identificador codificado magnéticamente y un identificador electrónico.

45. El sistema de cualquiera de las Reivindicaciones 34 a 44, que funciona además para determinar uno o más parámetros respectivos de la respuesta
5 característica premedida, mediante la lectura de uno o más parámetros del dispositivo de seguridad.

46. El sistema de cualquiera de las Reivindicaciones 34 a 45, que funciona además para determinar uno o más parámetros de la respuesta característica premedida, mediante la lectura de uno o más parámetros de una base de datos.

10 47. El sistema de la Reivindicación 46, en donde la base de datos está localizada a distancia del sistema de detección.

48. El sistema de cualquiera de las Reivindicaciones 34 a 47 que funciona además para descifrar la información de la respuesta característica premedida cuando se lea o se suministre en una forma cifrada.

15 49. Un método para leer un dispositivo de seguridad, que comprende:

aplicar un campo magnético a un dispositivo de seguridad;

medir uno o más parámetros representativos de una respuesta característica premedida del dispositivo de seguridad en respuesta al campo magnético; y

20 comparar uno o más parámetros representativos de una respuesta característica medida con uno o más parámetros respectivos de una respuesta característica premedida para determinar si los parámetros respectivos medidos y premedidos son sustancialmente equivalentes.

50. El método de la Reivindicación 49 que comprende aplicar un campo magnético variable en el tiempo a un dispositivo de seguridad.

51. El método de la Reivindicación 49 o de la Reivindicación 50, en donde medir uno o más parámetros representativos de una respuesta característica
5 medida del dicho dispositivo de seguridad en respuesta al campo magnético comprende medir uno o más valores de coercitividad y fluctuación.

52. El método de cualquiera de las Reivindicaciones 49 a 51 que comprende interrogar el dispositivo de seguridad usando un haz de luz.

53. El método de cualquiera de las Reivindicaciones 49 a 52 que comprende
10 operar un láser para producir un haz visible o cerca al infrarrojo.

54. El método de la Reivindicación 52 o de la Reivindicación 53 que comprende detectar cambios inducidos en el haz de luz por medio de elementos magnéticos del dispositivo de seguridad, usando el efecto magneto-óptico Kerr.

55. El método de la Reivindicación 54 que comprende usar el modo transversal
15 del efecto magneto-óptico Kerr.

56. El método de cualquiera de las Reivindicaciones 52 a 55 que comprende desviar el haz de luz a través de la superficie de dicho dispositivo de seguridad.

57. El método de cualquiera de las Reivindicaciones 49 a 56 que comprende leer un identificador único del dispositivo de seguridad.

20 58. El método de la Reivindicación 57 que comprende identificar el identificador único mediante el reconocimiento de un patrón de elementos magnéticos soportado por el dispositivo de seguridad.

59. El método de la Reivindicación 57 o de la Reivindicación 58 que comprende identificar el identificador único mediante la lectura de uno o más de: un código de barras legible ópticamente, uno o más indicios ópticos, un identificador codificado magnéticamente y un identificador electrónico.

5 60. El método de cualquiera de las Reivindicaciones 49 a 59 que comprende determinar uno o más parámetros respectivos de la respuesta característica premedida mediante la lectura de uno o más parámetros desde el dispositivo de seguridad.

61. El método de cualquiera de las Reivindicaciones 49 a 60 que comprende
10 determinar uno o más parámetros respectivos de la respuesta característica premedida, mediante la lectura de uno o más parámetros de una base de datos.

62. El método de la Reivindicación 61 que comprende acceder a una base de datos ubicada a distancia del sistema de detección.

63. El método de cualquiera de las Reivindicaciones 49 a 62 que además
15 comprende descifrar la información de la respuesta característica premedida cuando se lee o proporciona en forma cifrada.

64. Un producto que comprende el dispositivo de seguridad de cualquiera de las Reivindicaciones 1 a 20.

65. El producto de la Reivindicación 64 que comprende uno o más de: un
20 documento, un pasaporte, una tarjeta de identificación, un disco compacto, un disco versátil digital, un producto de software, empaque, una prenda de vestir, un artículo de calzado, una tarjeta inteligente, una tarjeta de crédito o bancaria, un producto cosmético, una pieza de ingeniería, un accesorio, y cualesquier otros bienes y /o artículos de comercio, sean fabricados o de otro modo.

SISTEMA Y DISPOSITIVO DE SEGURIDAD

RESUMEN

Un dispositivo de seguridad (100) que comprende, por lo menos, un elemento magnético (102). El elemento magnético (102) es sensible a un campo magnético aplicado para proporcionar una respuesta característica. La respuesta característica puede usarse para identificar un dispositivo de seguridad en particular (100) cuando es interrogado por un sistema de seguridad, de tal modo que ayuda a prevenir la falsificación del dispositivo de seguridad (100).

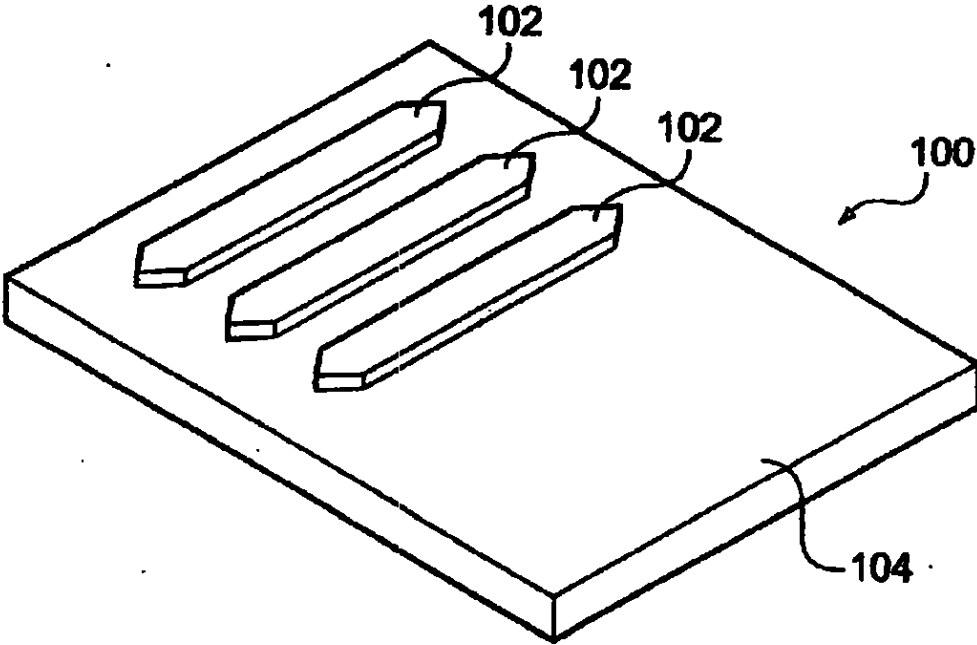


Fig. 1

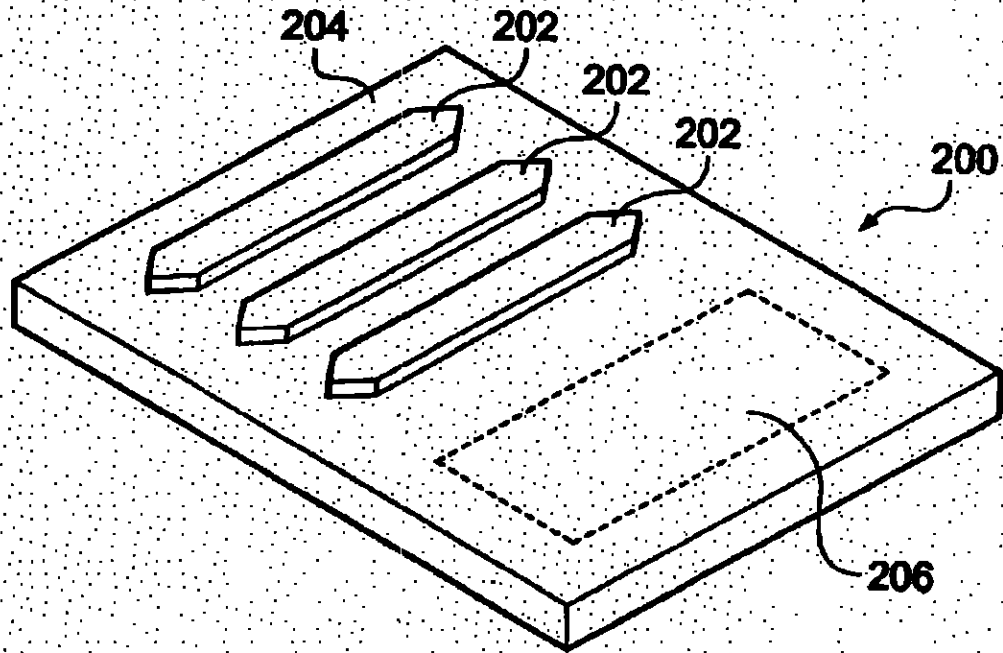


Fig. 2

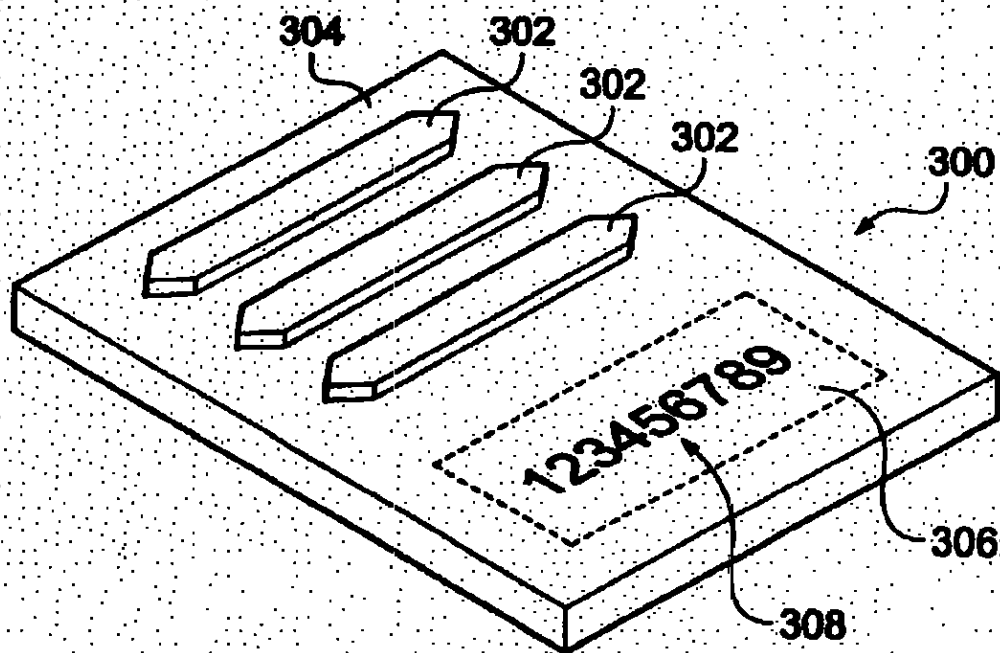


Fig. 3

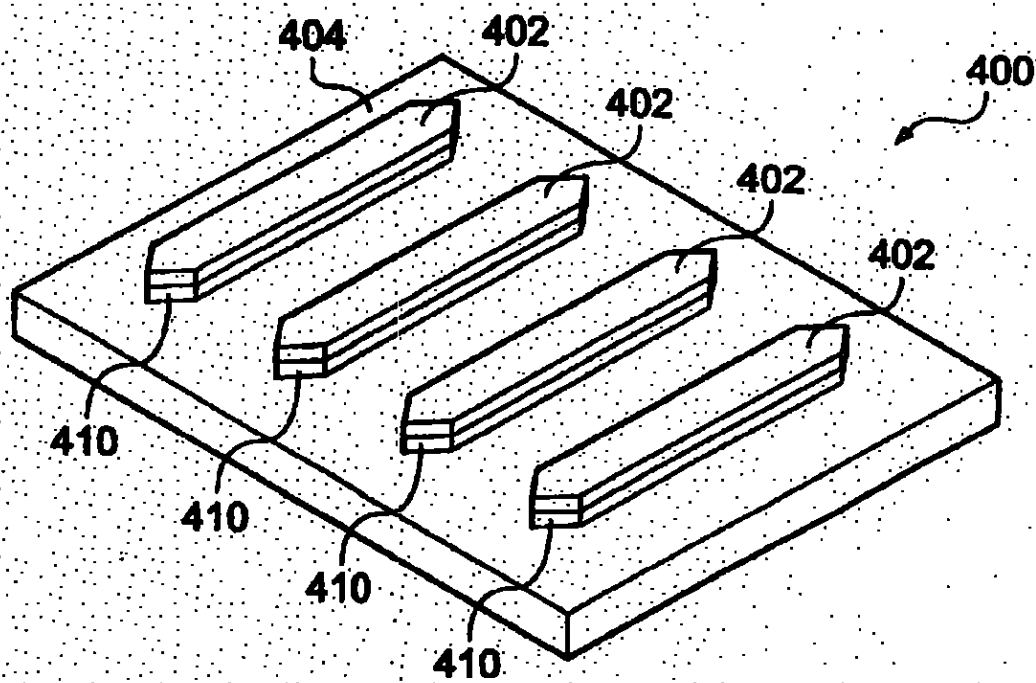


Fig. 4

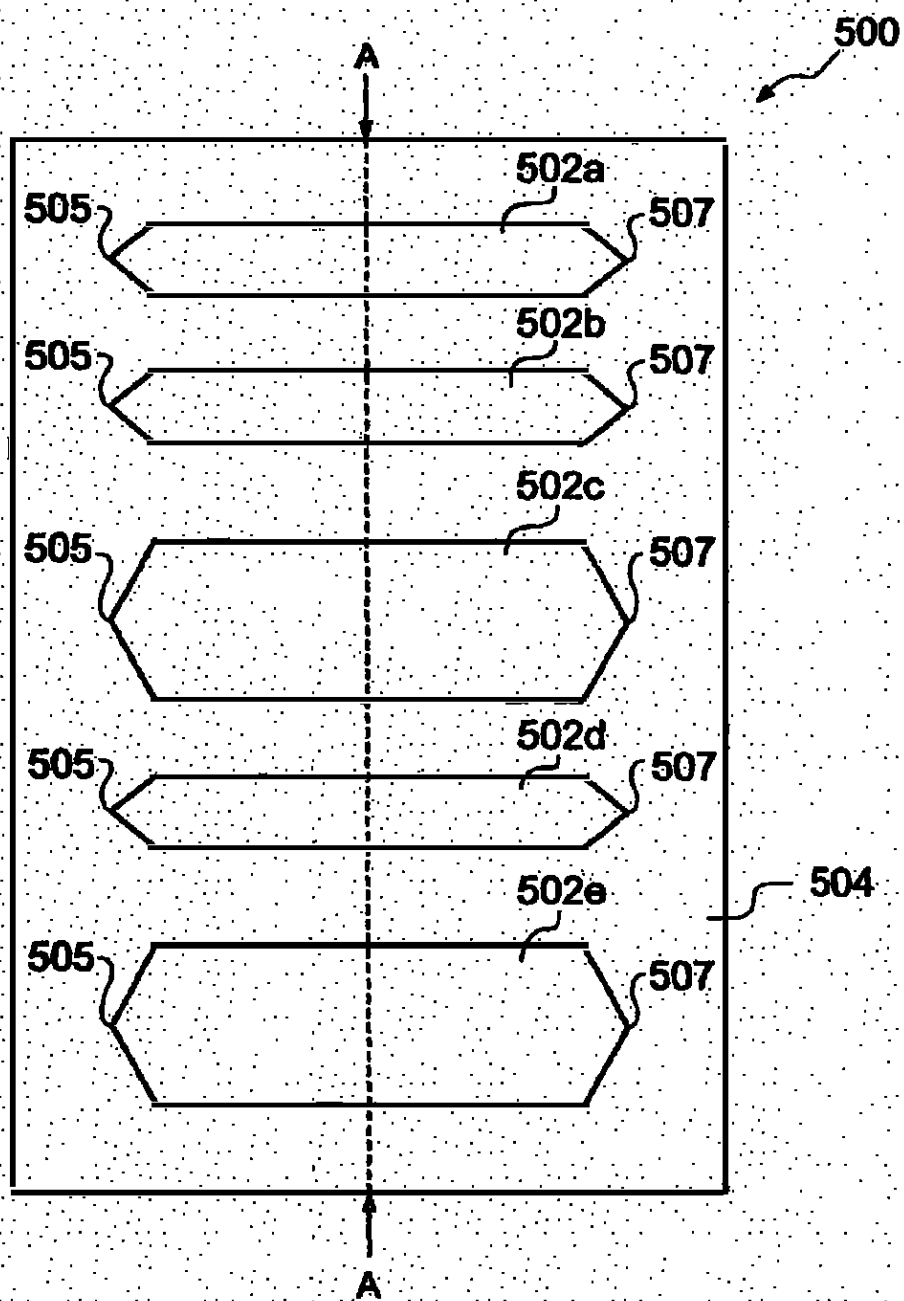


Fig. 5

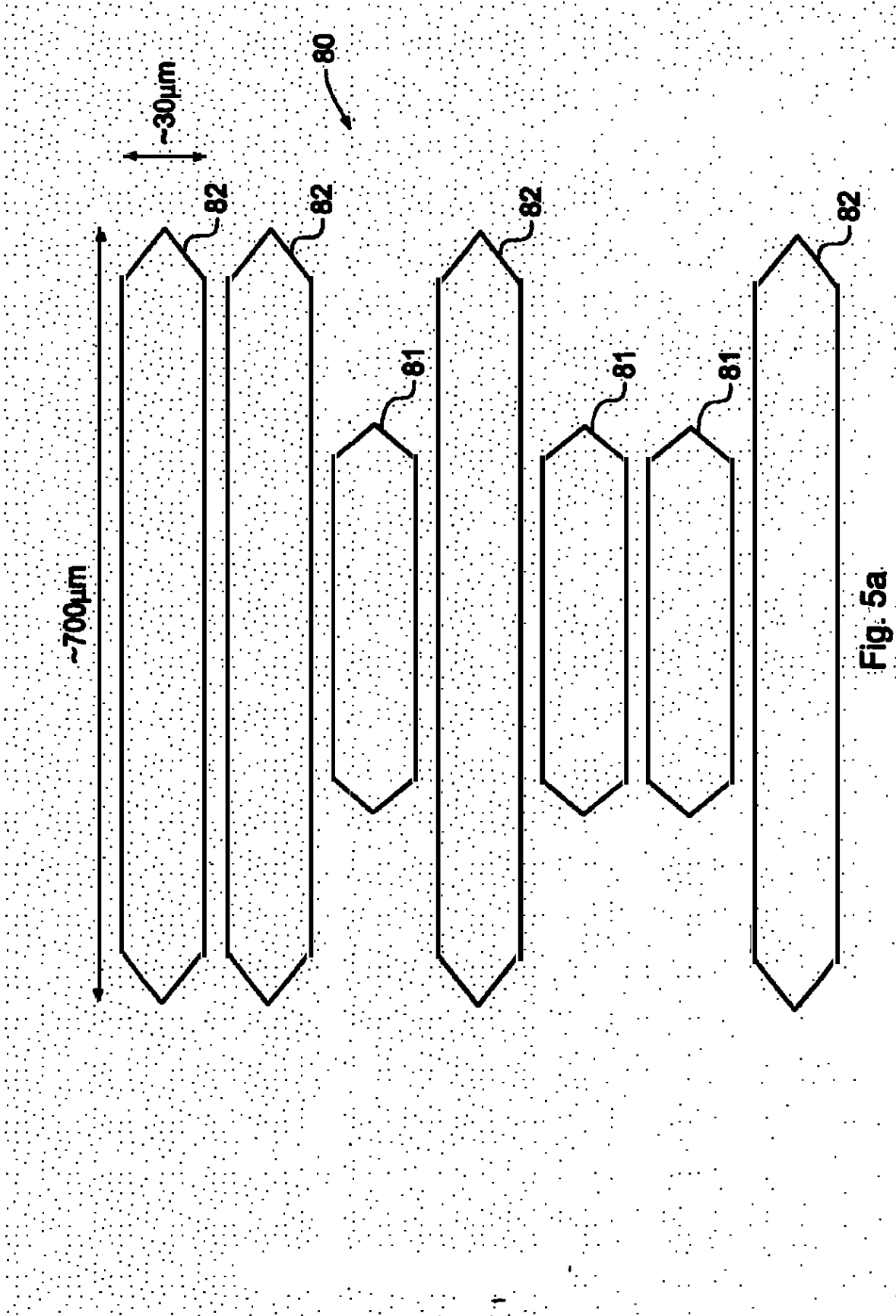


Fig. 5a

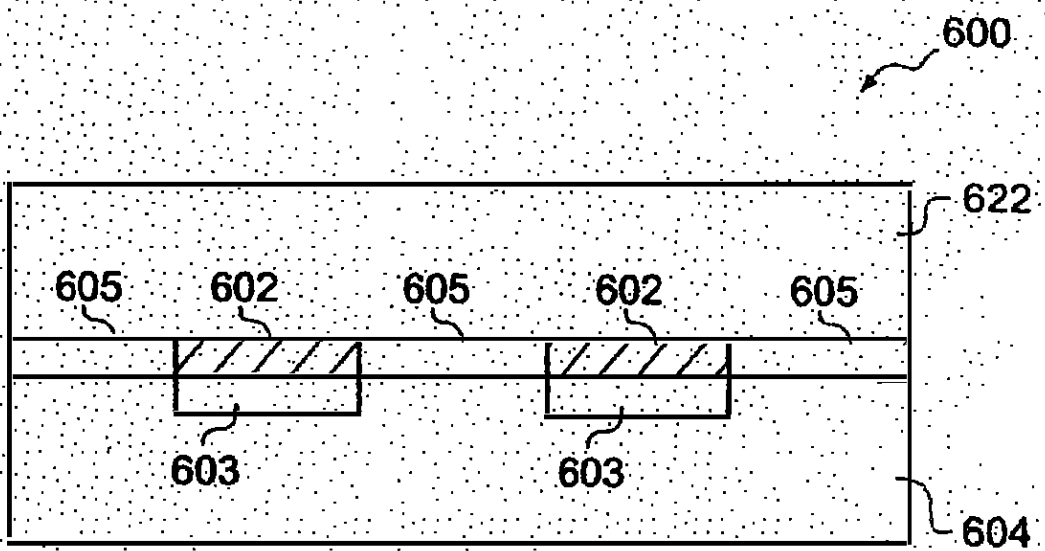


Fig. 6

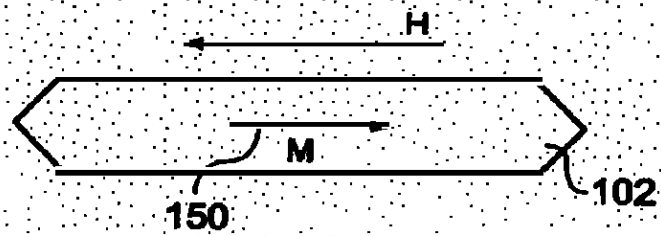


Fig. 7a

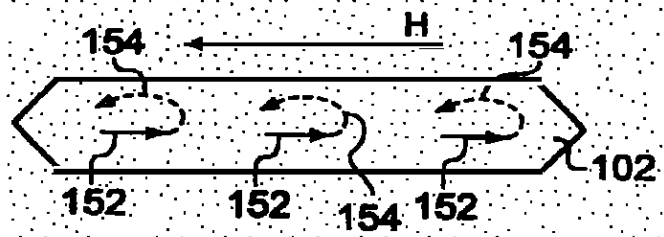


Fig. 7b

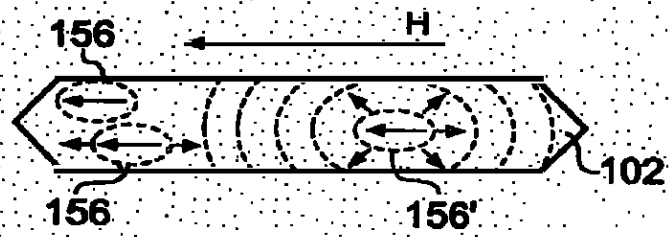


Fig. 7c

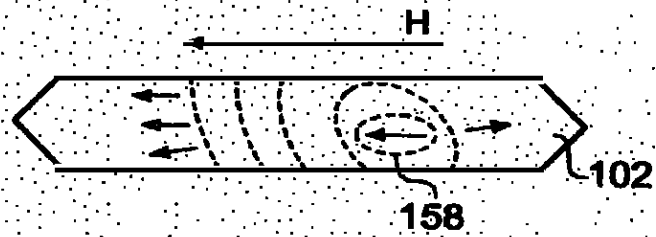


Fig. 7d

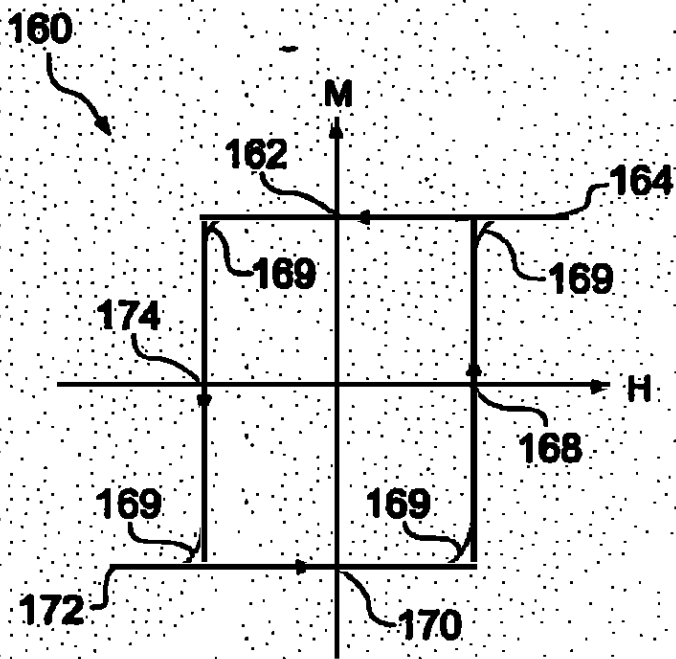


Fig. 8a

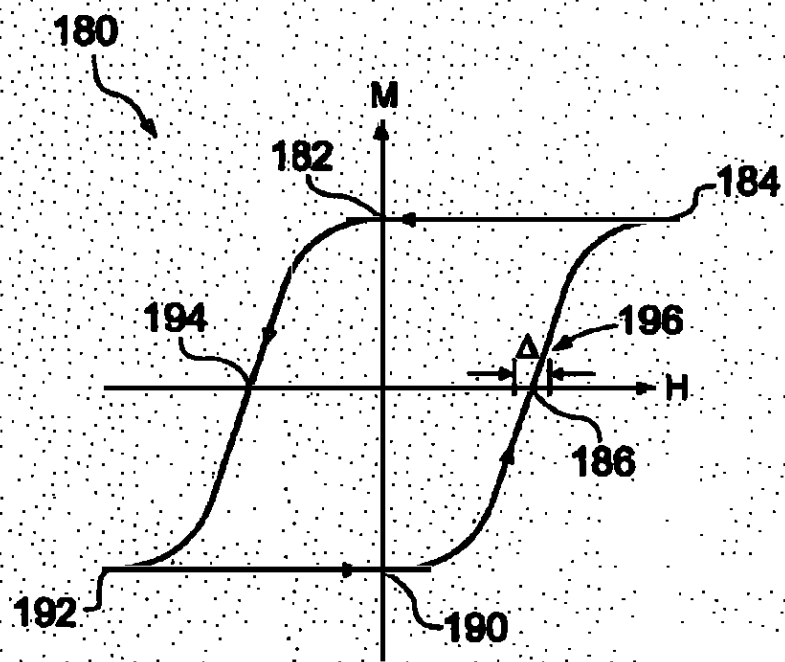


Fig. 8b



Fig. 9a

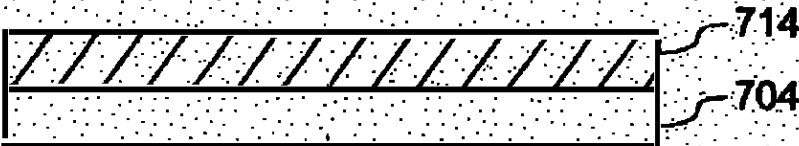


Fig. 9b

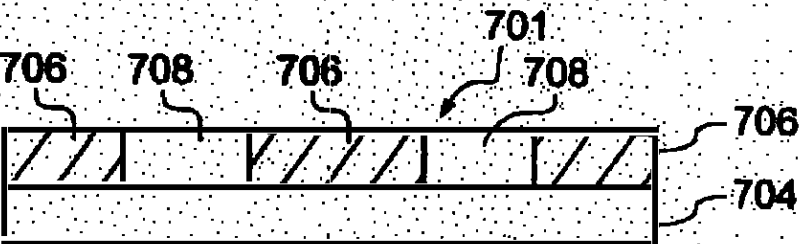


Fig. 9c

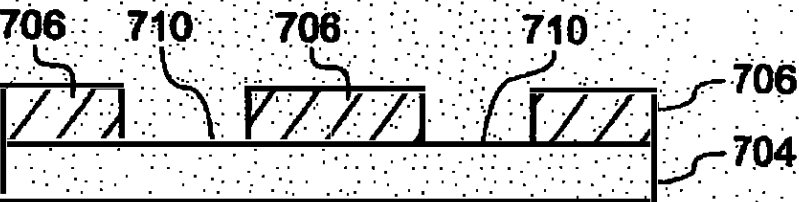


Fig. 9d

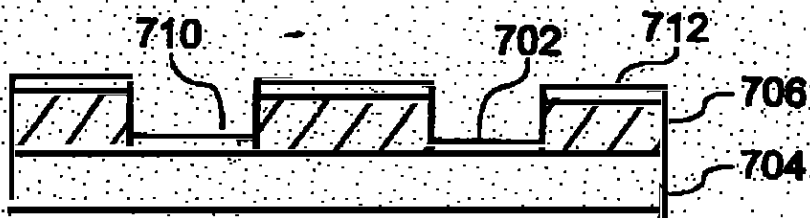


Fig. 9e

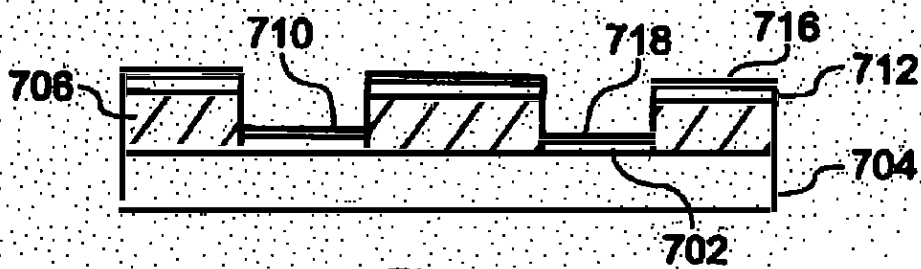


Fig. 9f

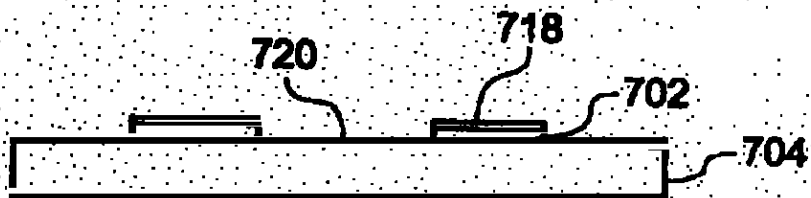


Fig. 9g

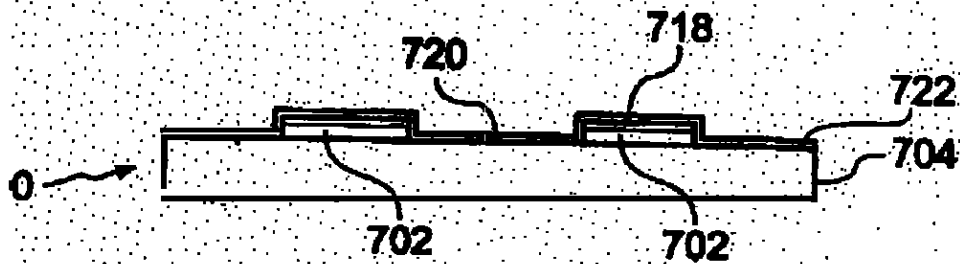


Fig. 9h

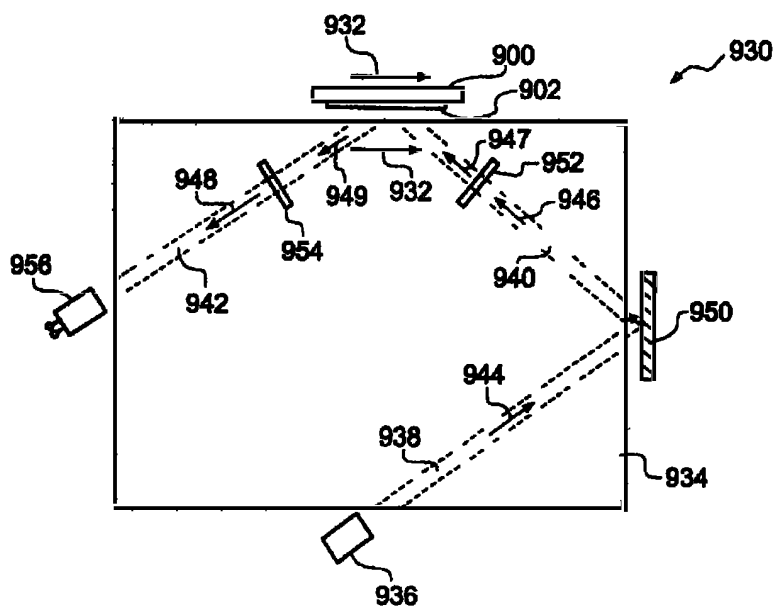


Fig 10

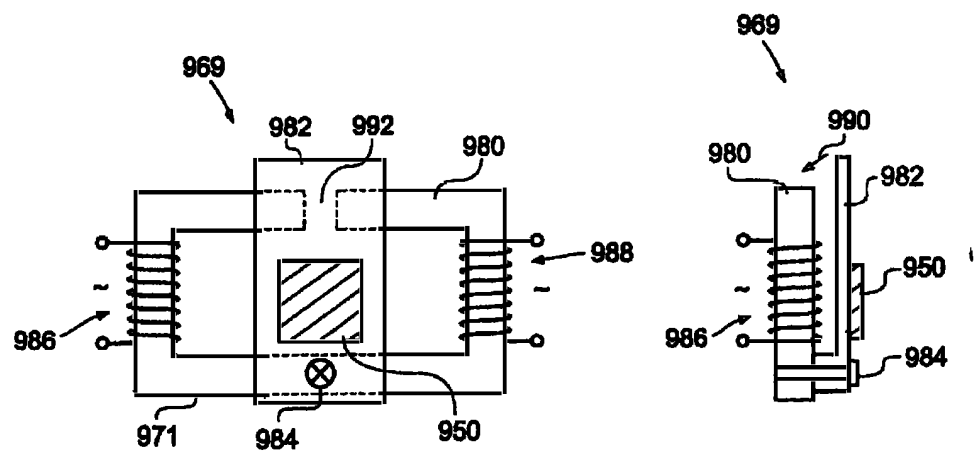


Fig 11

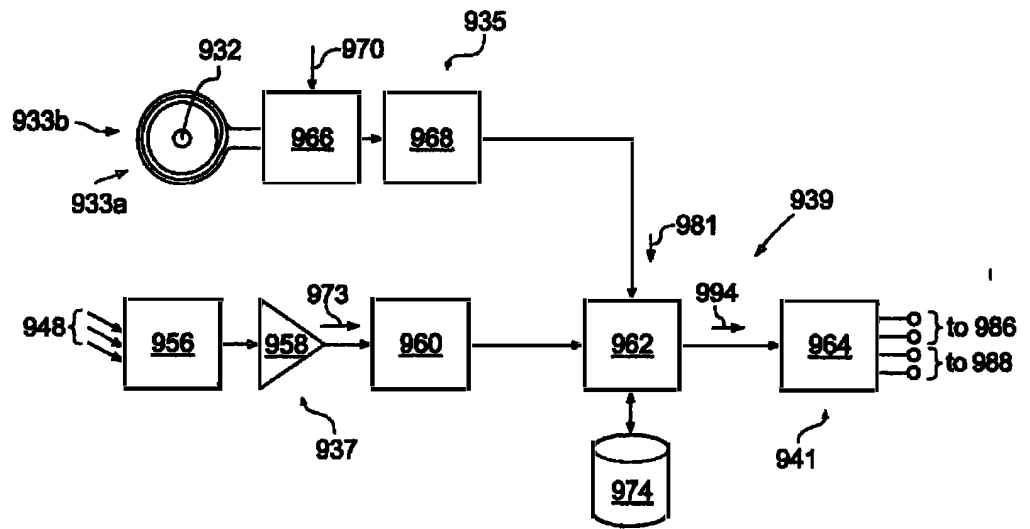


Fig 12

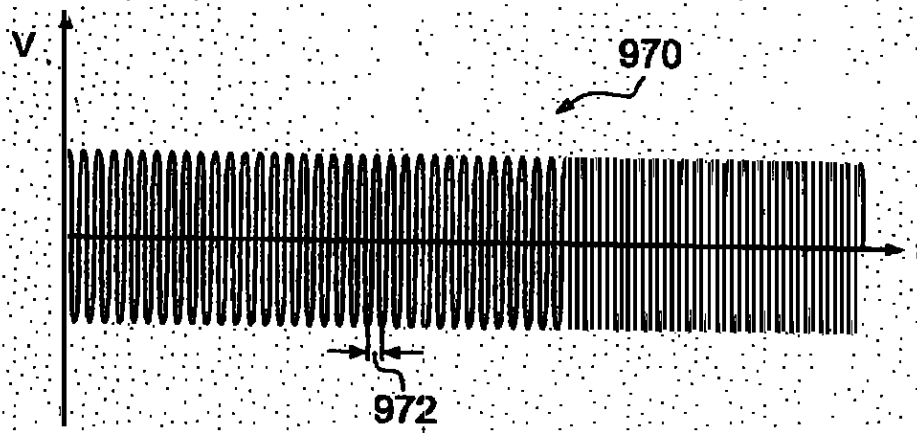


Fig. 13

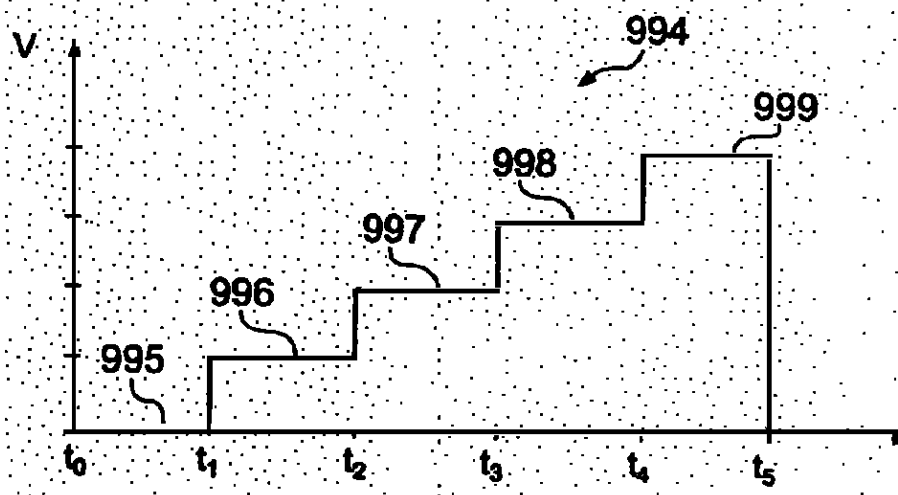


Fig. 14

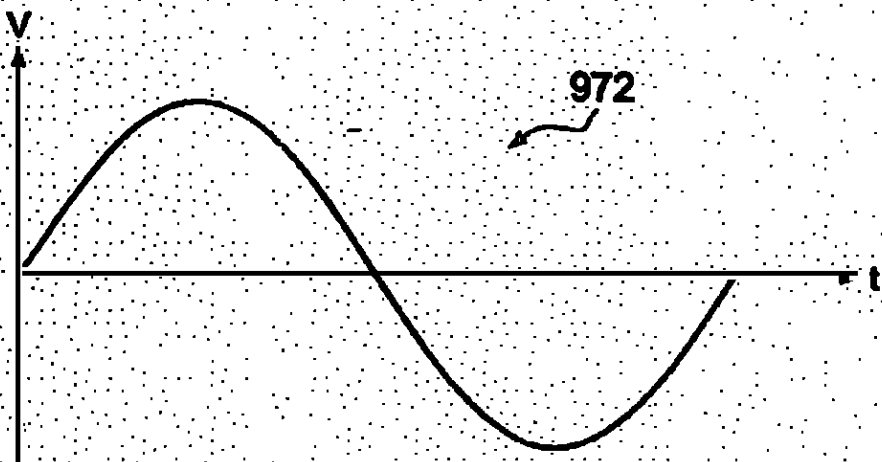


Fig. 15

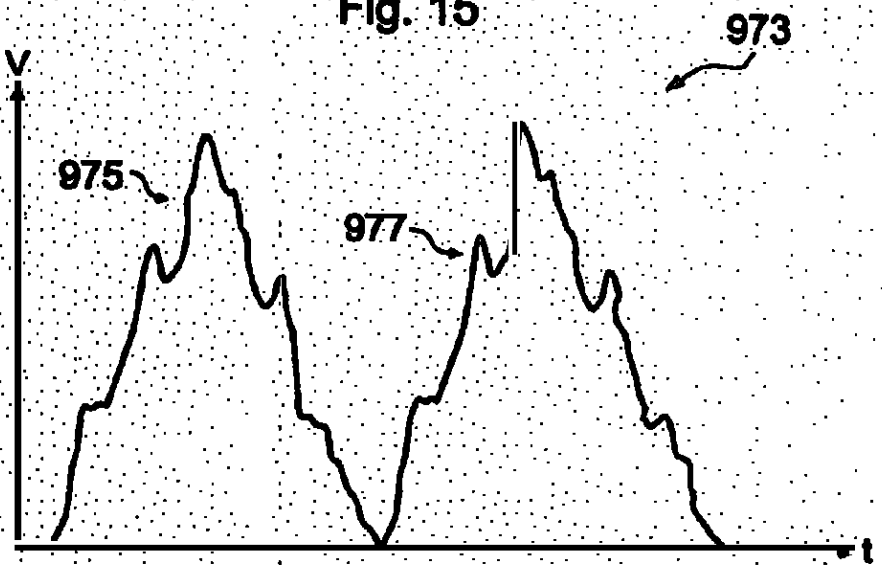


Fig. 16

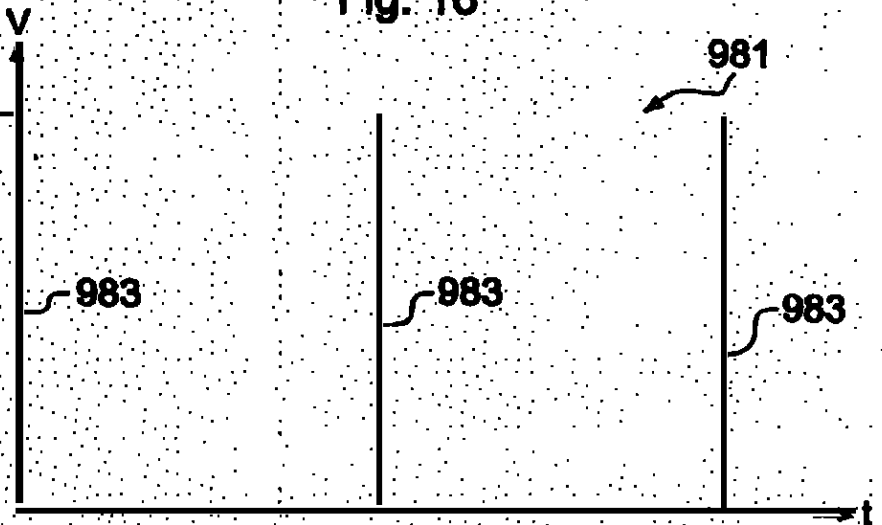


Fig. 17

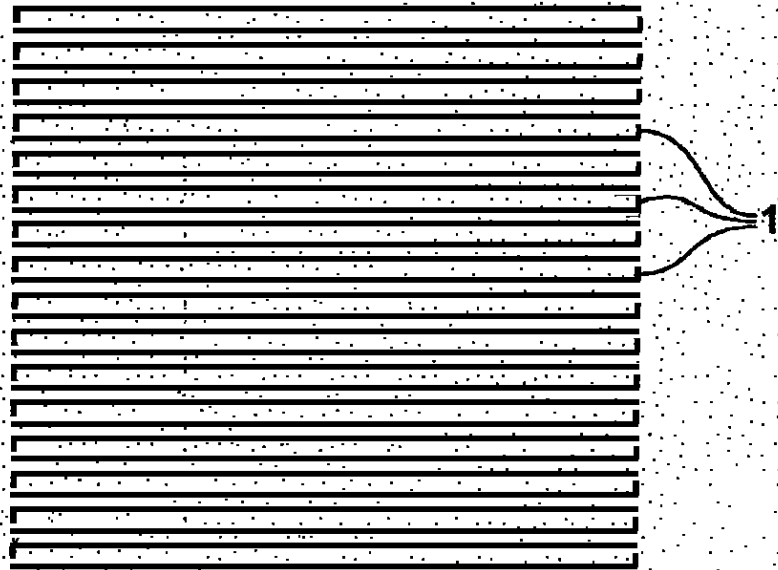


Fig. 18

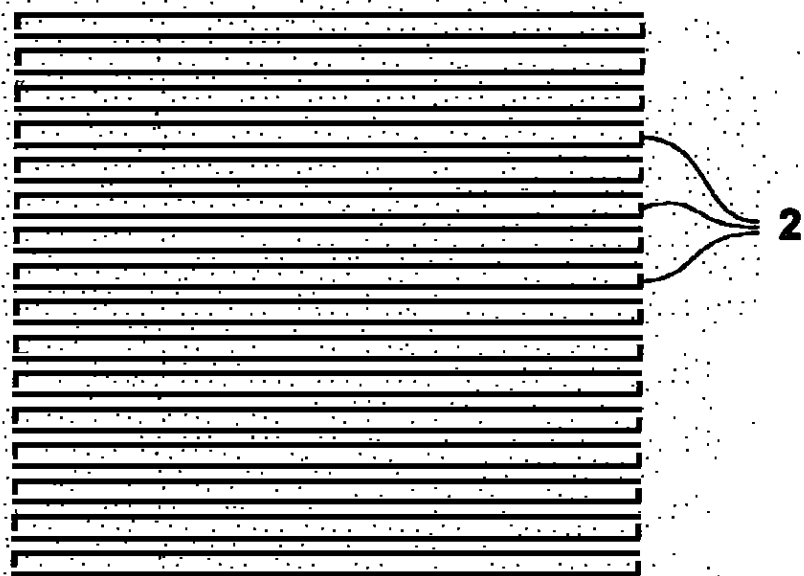


Fig. 19

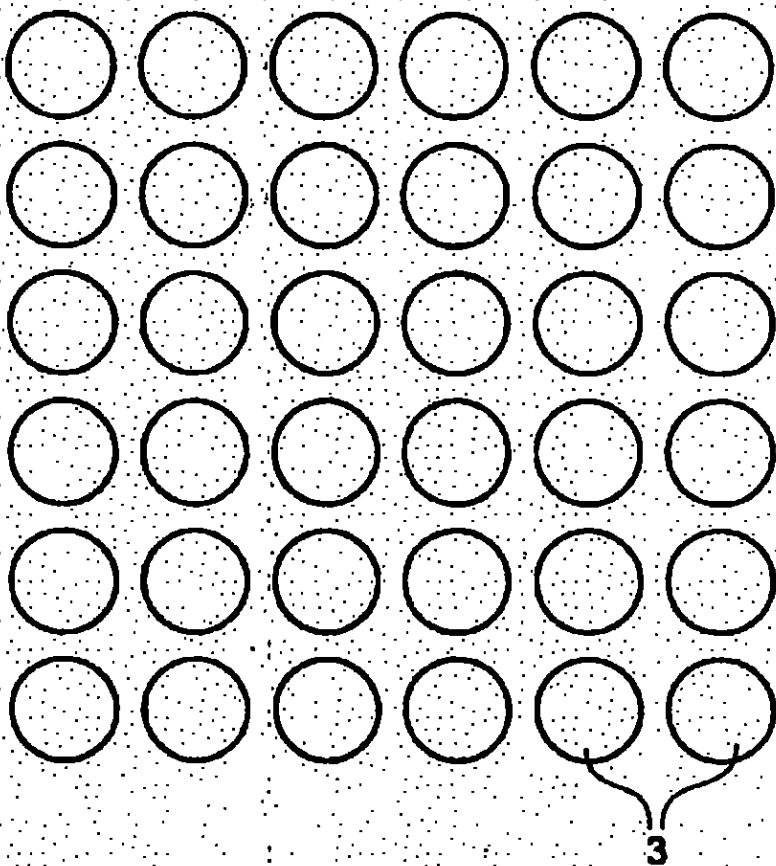


Fig. 20

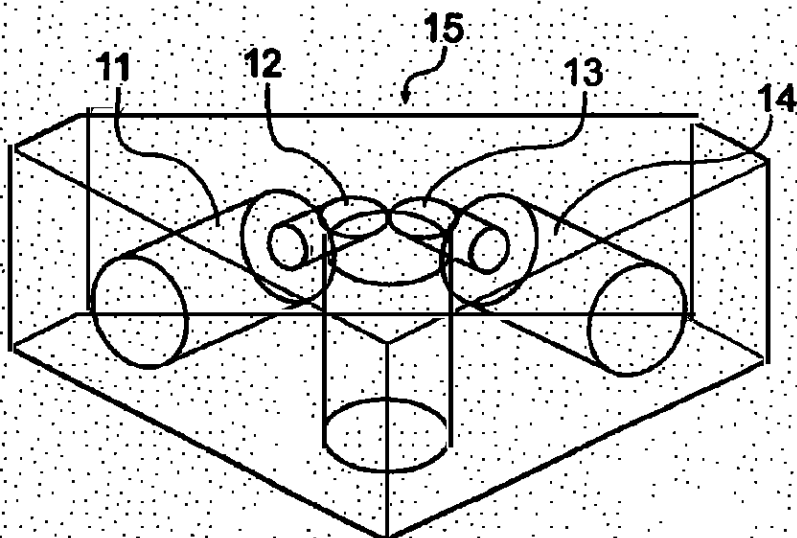


Fig. 21a

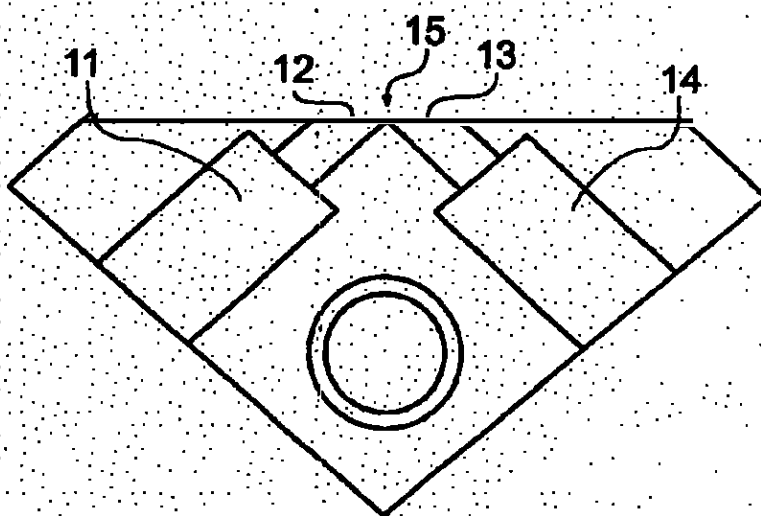


Fig. 21b

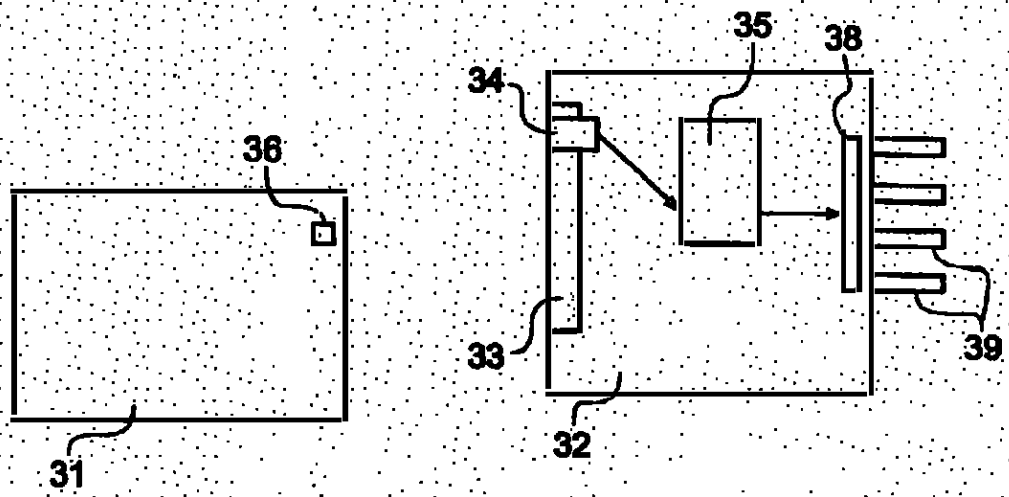


Fig. 23

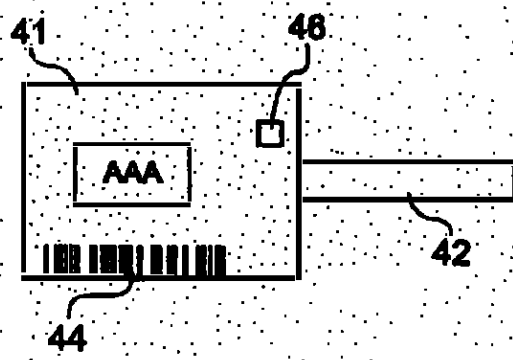


Fig. 24

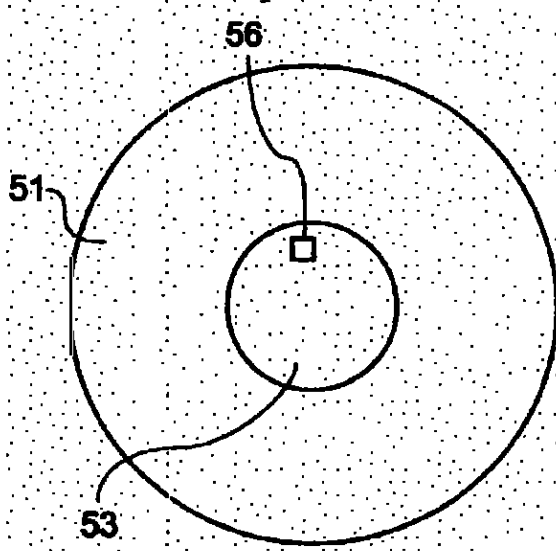


Fig. 25

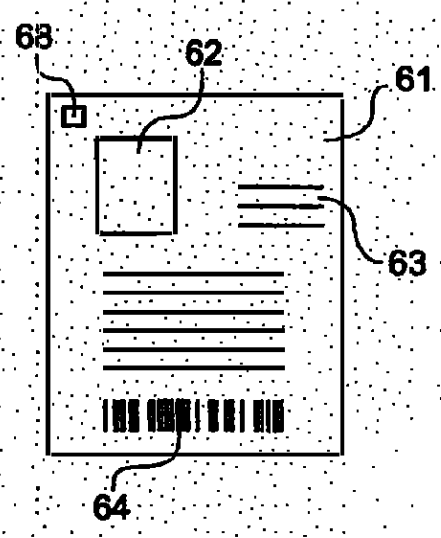


Fig. 26

PATENT COOPERATION TREATY

4976198

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

PCT

To:	MUNICH		
Haines, Miles John, et al	ORDER		
POTTER, Julian, Mark	DIARY		
D. Young & Co			
21 New Fetter Lane	REC'D		
London EC4A 1DA	(LONDON)	- 5 JUL 2004	
GRANDE BRETAGNE			
	ANSO		
	ENTRY		
	FOR		
		Date of mailing (day/month/year)	01.07.2004

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT
(PCT Rule 71.1)

Applicant's or agent's file reference
P018298WOP

IMPORTANT NOTIFICATION

International application No.
PCT/GB 03/03938

International filing date (day/month/year)
10.09.2003

Priority date (day/month/year)
10.09.2002

Applicant
INGENIA HOLDINGS LIMITED et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.
4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

The applicant's attention is drawn to Article 33(5), which provides that the criteria of novelty, inventive step and industrial applicability described in Article 33(2) to (4) merely serve the purposes of international preliminary examination and that "any Contracting State may apply additional or different criteria for the purposes of deciding whether, in that State, the claimed inventions is patentable or not" (see also Article 27(5)). Such additional criteria may relate, for example, to exemptions from patentability, requirements for enabling disclosure, clarity and support for the claims.

Name and mailing address of the International
preliminary examining authority:



European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Sportellini, E

Tel. +49 89 2399-7647



PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P018298WOP		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/GB 03/03938	International filing date (day/month/year) 10.09.2003	Priority date (day/month/year) 10.09.2002	
International Patent Classification (IPC) or both national classification and IPC G06K19/06			
Applicant INGENIA HOLDINGS LIMITED et al.			
1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36. 2. This REPORT consists of a total of 5 sheets, including this cover sheet. ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT). These annexes consist of a total of sheets.			
3. This report contains indications relating to the following items: I ☒ Basis of the opinion II ☐ Priority III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV ☐ Lack of unity of invention V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI ☐ Certain documents cited VII ☐ Certain defects in the international application VIII ☐ Certain observations on the international application			
Date of submission of the demand 08.04.2004		Date of completion of this report 01.07.2004	
Name and mailing address of the International preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465		Authorized Officer Schmidt, R Telephone No. +49 89 2399-2491 	

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB 03/03938

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-56 as originally filed

Claims, Numbers

1-65 as originally filed

Drawings, Sheets

1/23-23/23 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**International application No. **PCT/GB 03/03938**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	10-20,23,24,26-33,36-48,50-63
	No: Claims	1-9,21,22,25,34,35,49,64,65
Inventive step (IS)	Yes: Claims	
	No: Claims	1-65
Industrial applicability (IA)	Yes: Claims	1-65
	No: Claims	

2. Citations and explanations

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/03938

Re Item V.

1. Reference is made to the following documents:

D1: US-A-5 268 043
D2: EP-A-0 836 163
D3: EP-A-0 914 970
D4: US-A-4 146 664
D5: WO-A-01 97168

The documents D1 and D2 were not cited in the international search report.
Copies of the documents are appended hereto.

2. Regarding the subject-matter of claim 1, document D1 discloses a security device comprising at least one magnetic element (12), wherein said magnetic element is responsive to an applied magnetic field to provide a characteristic response (cf. column 5, line 45 - column 6, line 18).

Hence, the subject-matter of claim 1 is not novel (Article 33(2) PCT).

2.1 A device according to claim 1 is also known from each of documents D2 (cf. abstract and figure 2a), D3 (cf. abstract and figure 2) or D4 (cf. figure 2 and associated description).

2.2 According to D1, the magnetic element is supported on a substrate, it switches its magnetisation or magnetic polarisation in response to said applied field in a sharp switching mode (cf. figures 4/5 and associated description), it may be made from a magnetically soft material, selected from nickel, iron, cobalt and alloys thereof (cf. D1, claims 3 - 12), and it is substantially wire-shaped or flattened wire shaped.

Hence, the subject-matter of claims 2 - 9 lacks novelty as well (Article 33(2) PCT).

2.3 The remaining dependent claims 10 - 20 do not add anything inventive because the above mentioned documents do also show security devices with the following features: optical properties like light reflective layers (cf. e.g. D4, abstract), linear or two-dimensional patterns, optically readable bar codes, optical indicia, or encoded identifiers (cf. e.g. D4, figure 1; D5, abstract and figure).

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/03938

Hence, the subject-matter of said claims is at least clearly suggested by said documents so that the requirements of Article 33(2) and (3) are not met.

3. Independent claim 21 is directed to a method of manufacturing a security device consisting of the sole step to provide a device according to claim 1.

Hence, the subject-matter of claim 21 is also completely known from D1 and lacks novelty as well (Article 33(2) PCT).

4. Independent claim 34 is directed to a system for reading a security device. All the features of claim 34 are known from D2, which discloses a system comprising a magnetic field generation system for applying a magnetic field to a security device, a detection system for measuring one or more parameters of a measured characteristic response of said security device, whereby said system compares said measured characteristic response with a premeasured characteristic response to determine whether the respective parameters are substantially equivalent (cf. figure 4a and column 6, lines 23 - 58).

Hence, claim 34 does not meet the requirements of Article 33(2) EPC.

- 4.1 Independent claim 49 is a method claim drafted in analogy to claim 34 so that the same objection applies.
- 4.2 The features added by the remaining dependent claims correspond essentially to features of claims 2 - 20, which are at least suggested by the above mentioned documents. Therefore, these remaining dependent claims do not to meet the requirements of Article 33(2) and (3) as well.

TRATADO DE COOPERACION DE PATENTES

De
LA AUTORIDAD INTERNACIONAL DE EXAMEN PRELIMINAR

PCT

Para:
HAINES, MILES JOHN ET AL
POTTER, JULIAN, MARK
D. YOUNG & CO.
21 New Fetter Lane
Londres EC4A 1DA
GRAN BRETAÑA

NOTIFICACIÓN DE LA TRANSMISIÓN
DEL INFORME DEL EXAMEN
PRELIMINAR INTERNACIONAL
(PCT Regla 71.1)

Fecha de Correo
(día/mes/año) 01/07/2004

Archivo de referencia del solicitante o
del agente
P018298WOP

NOTIFICACIÓN IMPORTANTE

Solicitud internacional No.
PCT/GB 03/03938

Fecha de presentación internacional
(día/mes/año) 10/09/2003

Fecha de prioridad (día/mes/año)
10/09/2002

Solicitante:
INGENIA HOLDINGS LIMITED et al.

- 1 Por el presente se notifica al solicitante, que la Autoridad del Examen Preliminar Internacional, transmite el informe del examen preliminar y sus anexos, en caso de que haya alguno, establecido en la solicitud internacional.
- 2 Será transmitida una copia del informe y de sus anexos, si hay alguno, a la Oficina Internacional para comunicar a todas las oficinas elegidas.
- 3 La Oficina Internacional preparará una traducción en Ingles del informe pero no de los anexos, y transmitirá dicha traducción a las oficinas elegidas que requieran de dicho informe.
- 4 **RECORDATORIO**

El solicitante debe entrar a la fase nacional ante cada oficina elegida llevando a cabo ciertos requerimientos (presentación de traducciones y pago de tasas nacionales) dentro de los 30 meses de la fecha de la prioridad (o más tarde en algunas oficinas)(Artículo 39 (1))(ver también el recordatorio enviado por la Oficina Internacional con el formato PCT/IB/301).

Donde se requiera presentar traducción de la solicitud internacional a una oficina elgida, dicha traducción debe contener la traducción de alguno de los anexos del informe del examen preliminar. Es responsabilidad del del solicitante preparar y suministrar dicha traducción directamente a cada oficina elegida.

Para mayores detalles con relación a los límites de tiempo disponibles y requerimientos de las oficinas elegidas, ver Volumen II de la guía del solicitante del PCT.

Se llama la atención a los solicitante en cuanto al Artículo 33(5), que suministra el criterio de novedad, nivel inventivo y aplicación industrial descrito en el Artículo 33(2) al (4), solamente sirve para propósitos del Examen Preliminar Internacional y "cualquiera de los estados designados pueden aplicar criterios diferentes o adicionales para los propósitos de decidir si, en el Estado, la invención reivindicada es patentable o no" (ver también Artículo 27 (5). Tales criterios adicionales se pueden relacionar, por ejemplo, a excepciones de patentabilidad, requerimientos que permitan la revelación, claridad y sustentación de las reivindicaciones.

Nombre y dirección de correo del IPEA/
Oficina Europea de Patentes
D-80298 Munich

Tel. (+49-89) 2399-0, Tx: 523656 epmu d
Fax: (+49-89) 2399-4465

Funcionario autorizado
SPORTELLINI, E

Teléfono No. (+49-89) 2399 7647

TRATADO DE COOPERACION DE PATENTES

PCT

INFORME DEL EXAMEN PRELIMINAR INTERNACIONAL

(Artículo 36 y Regla 70 del PCT)

Archivo de referencia del solicitante o del agente P018298WOP	PARA ACCION POSTERIOR	Ver Notificación de Transmisión del Informe del Examen Preliminar Internacional (Formato PCT/IPEA/416)
Solicitud internacional No. PCT/GB03/03938	Fecha de presentación internacional (día/mes/año) 10/09/2003	Fecha de prioridad (día/mes/año) 10/09/2002
Clasificación Internacional de Patente (CIP) o Clasificación Nacional y CIP G06K 19/06		
Solicitante: INGENIA HOLDINGS LIMITED et al.		
1 Este informe de examen preliminar internacional ha sido preparado por esta Autoridad Examinadora Preliminar Internacional y se transmite al solicitante de acuerdo con el Artículo 36. 2 Este INFORME consiste en un total de <u>5</u> hojas, incluyendo esta carátula. ☒ Este informe también se acompaña de los ANEXOS, esto es, hojas de descripción, reivindicaciones y/o dibujos que han sido reformados y son la base de este informe y/o hojas que contienen rectificaciones hechas ante esta Autoridad (ver Regla 70.16 y Sección 607 de las Instrucciones Administrativas según el PCT Estos anexos consisten en un total de _____ hojas.		
3 Este informe contiene indicaciones relacionadas con los siguientes ítems: I ☒ Base del informe II ☐ Prioridad III ☐ No establecimiento de opinión con respecto a la novedad, altura inventiva y aplicación industrial IV ☐ Carencia de unidad de la invención V ☒ Declaración razonada según artículo 35(2) con relación a la novedad, altura inventiva o aplicación industrial; citas y explicaciones que apoyan tal declaración VI ☐ Ciertos documentos citados VII ☐ Ciertos defectos en la solicitud internacional VIII ☐ Ciertas observaciones sobre la solicitud internacional		

Fecha de presentación de la demanda 08/04/2004	Fecha de completamiento de este informe 01/07/2004
Nombre y dirección de correo del IPEA/JP Oficina Europea de Patentes D-80298 Munich Tel.: +49 89 2399 - 0 Tx: 523656 epmu d Fax.: +49 89 2399 - 4465	Funcionario autorizado Schmidt, R Teléfono No. 49 89 2399 2491

INFORME DE EXAMEN PRELIMINAR INTERNACIONALSolicitud Internacional No.
PCT/GB 03/03938**I. Base del Informe**

- 1 Con relación a los elementos de la solicitud Internacional (las páginas reemplazadas que han sido presentadas a la oficina receptora en respuesta a la invitación con respecto al Art. 14 están referidas en este informe "originalmente presentadas" y no se anexan a este informe ya que estas no contienen modificaciones (Reglas 70.16 y 70.17):

Descripción, páginas:

1 - 56 como se presentaron originalmente

Reivindicaciones Nos.:

1 - 65 como se presentaron originalmente

Dibujos, páginas:

1/23 - 23/23 como se presentaron originalmente

- 2 Con relación al idioma, todos los elementos antes marcados se pusieron a disposición y se suministraron a esta autoridad en el idioma en el que se presentó la solicitud internacional, a menos que se indique de otra forma en este punto.

Estos elementos se pusieron a disposición o se suministraron a esta autoridad en el siguiente idioma inglés, el cual es:

- ☐ el idioma de una traducción suministrada para fines de investigación internacional (según la Regla 23.1(b)).
- ☐ el idioma de publicación de la solicitud internacional (bajo la Regla 48.3(b)).
- ☐ el idioma de la traducción suministrada para fines de examen preliminar internacional (bajo la Regla 55.2 y/o 55.3)

- 3 Con relación a cualquier nucleótido y/o secuencia amino ácida descubierta en la solicitud internacional, el examen preliminar internacional se llevó a cabo con base en la lista de secuencia:

- ☐ contenida en la solicitud internacional en forma escrita
- ☐ presentado junto con la solicitud internacional en forma legible en computador
- ☐ suministrado con posterioridad a esta autoridad en forma escrita
- ☐ suministrado luego a esta autoridad en forma legible en computador
- ☐ la declaración que el listado de secuencia escrito suministrado posteriormente no va más allá del descubrimiento en la solicitud internacional que se presentó ha sido suministrada
- ☐ la declaración que la información grabada en forma legible en computador es idéntica a la lista de secuencia escrita ha sido suministrada

- 4 Las reformas han dado como resultado la cancelación de:

- ☐ la descripción, páginas
- ☐ las reivindicaciones, Nos.
- ☐ los dibujos, hojas/fig.

INFORME DE EXAMEN PRELIMINAR INTERNACIONAL

Solicitud Internacional No.
PCT/GB 03/03938

5 ☐ Este informe ha sido establecido como si (parte de) las reformas no han sido hechas, ya que se consideran que han ido más allá del descubrimiento que fue presentado, como se indica en la casilla suplementaria (Regla 70.2 (c)).

(Cualquier reemplazo de hoja que contenga tales correcciones debe ser referido al ítem 1 y debe ser anexoado a este informe)

6 Observaciones adicionales, si es necesario:

V. Declaración razonada bajo el artículo 35(2) con relación a la novedad, altura inventiva o aplicación industrial: citas y explicaciones que apoyan tal declaración.

1 Declaración

Novedad (N)	Reivindicaciones	10-20,23,24,26-33,36-48,50-63	Si
	Reivindicaciones	1-9,21,22,25,34,35,49,64,65	No
Altura inventiva (IS)	Reivindicaciones		Si
	Reivindicaciones	1-65	No
Aplicción industrial (IA)	Reivindicaciones	1-65	Si
	Reivindicaciones		No

2 Citas y explicaciones

Ver hoja separada

INFORME DEL EXAMEN PRELIMINAR INTERNACIONAL-HOJA ANEXA
Solicitud Internacional No. PCT/GB 03/03938

Numeral V.

1. Se hace referencia a los siguientes documentos:

D1: US-A-5 268 043
D2: EP-A-0 836 163
D3: EP-A-0 914 970
D4: US-A-4 146 664
D5: WO-A-01 97168

Los documentos D1 y D2 no fueron citados en el informe de búsqueda internacional. Se anexan copias de los documentos.

2. Con respecto al objeto de la reivindicación 1, el documento D1 revela un dispositivo de seguridad que comprende al menos un elemento magnético (12), donde dicho elemento magnético es sensible al campo magnético aplicado para suministrar una respuesta característica (ver columna 5, línea 45- columna 6, línea 18).

Por lo tanto, el contenido de la reivindicación 1 no es novedoso (Artículo 33 (2) PCT).

2.1 Un dispositivo de conformidad con la reivindicación 1 se conoce también de cada uno de los documentos D2 (ver resumen y figura 2 a), D3 (ver resumen y figura 2) o D4 (ver figura 2 y descripción asociada).

2.2 De conformidad con D1, el elemento magnético está sostenido por un sustrato, esto cambia su magnetización o polarización magnética en respuesta a dicho campo aplicado en un modo de conmutación intensa (ver figuras 4/5 y descripción asociada), este puede ser hecho de un material magnéticamente suave, seleccionado a partir de níquel, hierro, cobalto y aleaciones de estos (ver D1, reivindicaciones 3-12), y este es sustancialmente de forma de alambre o alambre aplanado.

Por lo tanto, el contenido de las reivindicaciones 2 a 9 no poseen tampoco novedad (ver artículo 33 (2) PCT).

2.3 Las restantes reivindicaciones dependientes 10 a 20 no aportan nada inventivo ya que los anteriores documentos también muestran dispositivos de seguridad con las siguientes características: propiedades ópticas como capas que reflejan la luz (ver por ejemplo D4, y resumen), patrones lineal y bidimensional, códigos de barras de lectores ópticos, indicios ópticos o identificadores codificados. (ver por ejemplo D4, figura 1; D5, resumen y figura).

Por lo tanto, el contenido de dichas reivindicaciones es al menos claramente sugerido por dichos documentos, por lo que no se cumple con los requerimientos de el Artículo 33(2) y (3).

3. La reivindicación 21 se relaciona con un método para fabricar un dispositivo de seguridad que consiste en solo un paso de suministrar un dispositivo de conformidad con la reivindicación 1.

Por lo tanto, el contenido de la reivindicación 21 es completamente también conocida por D1 y no tiene novedad (Artículo 33 (2) PCT).

4. La reivindicación independiente 34 se relaciona con un sistema para leer un dispositivo de seguridad. Todas las características de la reivindicación 34 se conocen de

D2, que revela un sistema que comprende un sistema de generación de campo magnético para aplicar un campo magnético a un dispositivo de seguridad, un sistema de detección para medir uno o más parámetros de una respuesta característica medida de dicho dispositivo de seguridad, por lo cual dicho sistema compara dicha respuesta característica medida con una característica premedida para determinar si los parámetros respectivos son sustancialmente equivalentes (ver figura 4 a y columna 6, líneas 23 a 58).

Por lo tanto, la reivindicación 34 no cumple con los requerimientos del Artículo 33 (2) EPC.

4.1 La reivindicación 49 independiente es un método que preparó lo reivindicado en analogía a la reivindicación (34), por lo que se aplica la misma objeción.

4.2 Las características adicionales por las restantes reivindicaciones dependientes corresponden esencialmente a las características de las reivindicaciones 2 a 20, que al menos son sugeridas por los documentos arriba citados. Por lo tanto, estas reivindicaciones dependientes restantes no cumplen con los requerimientos del Artículo 33 (2) y (3).

PATENT COOPERATION TREATY

11 days for fax

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: Haines, Miles POTTER, Julian, Mark D. Young & Co 21 New Fetter London EC4A GRANDE BRETAGNE	MONEY	£	SOUTHAMPTON	PCT
	ORDER			
	DIARY	John et al		
	REC'D	29 NOV 2004		
	ENTRY			
	FOR			
29 NOV 2004				NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Rule 71.1)
Date of mailing (day/month/year)				25.11.2004

Applicant's or agent's file reference P018298WOP			IMPORTANT NOTIFICATION	
International application No. PCT/GB 03/03938	International filing date (day/month/year) 10.09.2003	Priority date (day/month/year) 10.09.2002		
Applicant INGENIA HOLDINGS LIMITED et al.				

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

The applicant's attention is drawn to Article 33(5), which provides that the criteria of novelty, inventive step and industrial applicability described in Article 33(2) to (4) merely serve the purposes of international preliminary examination and that "any Contracting State may apply additional or different criteria for the purposes of deciding whether, in that State, the claimed inventions is patentable or not" (see also Article 27(5)). Such additional criteria may relate, for example, to exemptions from patentability, requirements for enabling disclosure, clarity and support for the claims.

Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Sportellini, E Tel. +49 89 2399-7647	
---	---	---

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P018298WOP	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/GB 03/03938	International filing date (day/month/year) 10.09.2003	Priority date (day/month/year) 10.09.2002
International Patent Classification (IPC) or both national classification and IPC G06K19/06		
Applicant INGENIA HOLDINGS LIMITED et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets; including this cover sheet.
- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
- These annexes consist of a total of 7 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Rule 68.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 08.04.2004	Date of completion of this report 25.11.2004
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Schmidt, R Telephone No. +49 89 2398-2491 

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB 03/03938

I. Basis of the report

1. With regard to the elements of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-56 as originally filed

Claims, Numbers

1-64 received on 17.11.2004 with letter of 15.11.2004

Drawings, Sheets

1/23-23/23 as originally filed

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/GB 03/03938**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement



Novelty (N)	Yes: Claims	1-64
	No: Claims	
Inventive step (IS)	Yes: Claims	1-64
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-64
	No: Claims	



2. Citations and explanations

see separate sheet



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/03938

Re Item V.

1. Reference is made to the following document:

D1: US-A-5 268 043

Document D1 was not cited in the international search report. A copy of said document has already been provided to the Applicant.

2. Regarding the subject-matter of claim 1, document D1 discloses a security device comprising at least one magnetic element (12), wherein said magnetic element is responsive to an applied magnetic field to provide a characteristic response (cf. column 5, line 45 - column 6, line 18).

Since the available documents do neither disclose nor suggest to make said magnetic element from a material that comprises structural defects that cause brittle mode switching in which the magnetic growth of a single magnetic domain dominates the change in magnetisation of a respective magnetic element, the subject-matter of claim 1 meets the requirements of Article 33(2) and (3) PCT.

- 2.1 The same applies for independent claims 20, 33, and 48 since they contain corresponding features related to brittle mode switching characteristics.

CLAIMS

1. A security device comprising at least one magnetic element, wherein said at least one magnetic element is responsive to an applied magnetic field to provide a characteristic response, characterised in that said at least one magnetic element is made from a material that comprises structural defects that cause brittle mode switching in which the growth of a single magnetic domain dominates the change in magnetisation of a respective magnetic element.
2. The security device of Claim 1, wherein said at least one magnetic element is supported by a substrate.
3. The security device of Claim 2, wherein said at least one magnetic element is supported on said substrate.
4. The security device of any preceding Claim, wherein said at least one magnetic element is responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of said at least one magnetic element.
5. The security device of any preceding Claim, wherein said at least one magnetic element is made from a magnetically soft material.
6. The security device of Claim 5, wherein said at least one magnetic element comprises a magnetically soft material selected from one or more of: nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.
7. The security device of Claim 5 or 6, wherein said magnetically soft material is a permalloy material.
8. The security device of any preceding Claim, wherein said at least one magnetic element is substantially wire-shaped or flattened wire shaped.
9. The security device of any preceding Claim, wherein said at least one magnetic element is backed by a light reflective layer.

17-11-2004

GB0303938

10. The security device of any preceding Claim, wherein said at least one magnetic element is provided proximal a reduced light reflectivity portion of said security device.
11. The security device of any preceding Claim, comprising a plurality of said at least one magnetic elements.
12. The security device of Claim 11, wherein said plurality of magnetic elements is arranged to provide a linear pattern.
13. The security device of Claim 11, wherein said plurality of magnetic elements is arranged to provide a two-dimensional pattern.
14. The security device of Claim 12 or Claim 13, wherein said pattern encodes an identifier.
15. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.
16. The security device of claim 15, wherein said unique identifier is provided by way of one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.
17. The security device of claim 16, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.
18. The security device of any preceding Claim, wherein premeasured characteristic response information representing one or more measurable parameters of said characteristic response is stored on said security device.
19. The security device of Claim 18, wherein said premeasured characteristic response information is in encrypted form.
20. A method of manufacturing a security device, comprising:

providing at least one magnetic element comprising structural defects, wherein said at least one magnetic element provides a brittle mode switching characteristic response in response to an applied magnetic field.

21. The method of Claim 19, comprising providing said at least one magnetic
5 element on a substrate.

22. The method of Claim 20 or Claim 21, comprising forming said at least one magnetic element using a lift-off or wet etching process.

23. The method of Claim 20 or Claim 21, comprising forming said at least one magnetic element using an ion beam etching process.

10 24. The method of any one of Claims 20 to 23, comprising measuring the magnitude(s) of one or more magnetic parameters of said at least one magnetic element.

25. The method of Claim 24, comprising measuring one or more of coercivity and jitter values.

15 26. The method of Claim 24 or Claim 25, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.

27. The method of Claim 26, comprising encrypting said premeasured characteristic response information.

20 28. The method of Claim 26 or Claim 27, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.

25 29. The method of Claim 26 or Claim 27, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.

17-11-2004

GB0303938

30. The method of Claim 29, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.

31. The method of any one of Claims 20 to 30, further comprising providing said security device with a unique identifier.

5 32. The method of Claim 31 when dependant upon any one of Claims 27 to 30, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.

33. A system for reading a security device, comprising:

10 a magnetic field generation system for applying a magnetic field to a security device; and

a detection system for measuring one or more parameters representative of a brittle mode switching measured characteristic response of said security device in response to said magnetic field,

15 wherein said system is operable to compare said one or more parameters representative of a brittle mode switching measured characteristic response to one or more respective parameters of a brittle mode switching premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

20 34. The system of Claim 33, wherein the magnetic field generation system is operable to apply a time varying magnetic field to a security device.

35. The system of Claim 33 or Claim 34, wherein a light beam is used to interrogate said security device.

36. The system of any one of Claims 33 to 35, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

25 37. The system of any one of Claims 33 to 36, wherein said parameters represent one or more of coercivity and jitter values.

17-11-2004

GB0303938

38. The system of any one of Claims 35 to 37, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for detecting changes induced in said light beam by magnetic elements of said security device.
39. The system of Claim 38, wherein said magneto-optic Kerr effect detection
5 apparatus is configured to operate in transverse mode.
40. The system of any one of Claims 35 to 39, further operable to deflect said light beam across the surface of said security device.
41. The system of any one of Claims 33 to 40, further operable to read a unique identifier from said security device.
- 10 42. The system of Claim 41, wherein said unique identifier is identified by recognising a pattern of magnetic elements supported by said security device.
43. The system of Claim 41 or 42, wherein said unique identifier is identified by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.
- 15 44. The system of any one of Claims 33 to 43, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from said security device.
45. The system of any one of Claims 33 to 44, further operable to determine said one or more respective parameters of the premeasured characteristic response by
20 reading said one or more parameters from a database.
46. The system of Claim 45, wherein said database is remotely located from said detection system.
47. The system of any one of Claims 33 to 46, further operable to decrypt premeasured characteristic response information where it is read or provided in
25 encrypted form.
48. A method for reading a security device, comprising:

17.1.1-2004

GB0303938

applying a magnetic field to a security device;

measuring one or more parameters representative of a brittle mode switching measured characteristic response of said security device in response to said magnetic field; and

- 5 comparing said one or more parameters representative of a brittle mode switching measured characteristic response to one or more respective parameter(s) of a brittle mode switching premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.

49. The method of Claim 48, comprising applying a time varying magnetic field to a security device.

50. The method of Claim 48 or Claim 49, wherein measuring of one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field comprises measuring one or more of coercivity and jitter values.

51. The method of any one of Claims 48 to 50, comprising interrogating said security device using a light beam.

52. The method of any one of Claims 48 to 51, comprising operating a laser to produce a visible or near-infrared beam.

53. The method of Claim 51 or Claim 52, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.

54. The method of Claim 53, comprising using the magneto-optic Kerr effect transverse mode.

55. The method of any one of Claims 51 to 54, comprising deflecting said light beam across the surface of said security device.

56. The method of any one of Claims 48 to 55, comprising reading a unique identifier from said security device.

57. The method of Claim 56, comprising identifying said unique identifier by recognising a pattern of magnetic elements supported by said security device.

58. The method of Claim 56 or 57, comprising identifying said unique identifier by reading one or more of: an optically readable bar code; one or more optical indicia; a
5 magnetically encoded identifier; and an electronic identifier.

59. The method of any one of Claims 48 to 58, comprising determining said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

60. The method of any one of Claims 48 to 59, comprising determining said one or
10 more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

61. The method of Claim 60, comprising accessing a database remotely located from said detection system.

62. The method of any one of Claims 48 to 61, further comprising decrypting
15 premeasured characteristic response information where it is read or provided in encrypted form.

63. A product comprising the security device of any one of Claims 1 to 19.

64. The product of Claim 63, comprising one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging;
20 an item of clothing; an item of footwear; a smart-card; a credit or bank card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.

TRATADO DE COOPERACION DE PATENTES

De
LA AUTORIDAD INTERNACIONAL DE EXAMEN PRELIMINAR

PCT

Para:
HAINES, MILES JOHN ET AL
POTTER, JULIAN, MARK
D. YOUNG & CO.
21 New Fetter Lane
Londres EC4A 1DA
GRAN BRETAÑA

NOTIFICACIÓN DE LA TRANSMISIÓN
DEL INFORME DEL EXAMEN
PRELIMINAR INTERNACIONAL
(PCT Regla 71.1)

Fecha de Correo
(día/mes/año) 25/11/2004

Archivo de referencia del solicitante o
del agente

P018298WOP

NOTIFICACIÓN IMPORTANTE

Solicitud internacional No.

PCT/GB 03/03938

Fecha de presentación internacional
(día/mes/año)

10/09/2003

Fecha de prioridad (día/mes/año)

10/09/2002

Solicitante:

INGENIA HOLDINGS LIMITED et al.

- 1 Por el presente se notifica al solicitante, que la Autoridad del Examen Preliminar Internacional, transmite el informe del examen preliminar y sus anexos, en caso de que haya alguno, establecido en la solicitud internacional.
- 2 Será transmitida una copia del informe y de sus anexos, si hay alguno, a la Oficina Internacional para comunicar a todas las oficinas elegidas.
- 3 La Oficina Internacional preparará una traducción en Inglés del informe pero no de los anexos, y transmitirá dicha traducción a las oficinas elegidas que requieran de dicho informe.

4 RECORDATORIO

El solicitante debe entrar a la fase nacional ante cada oficina elegida llevando a cabo ciertos requerimientos (presentación de traducciones y pago de tasas nacionales) dentro de los 30 meses de la fecha de la prioridad (o más tarde en algunas oficinas)(Artículo 39 (1))(ver también el recordatorio enviado por la Oficina Internacional con el formato PCT/IB/301).

Donde se requiera presentar traducción de la solicitud internacional a una oficina elegida, dicha traducción debe contener la traducción de alguno de los anexos del informe del examen preliminar. Es responsabilidad del solicitante preparar y suministrar dicha traducción directamente a cada oficina elegida.

Para mayores detalles con relación a los límites de tiempo disponibles y requerimientos de las oficinas elegidas, ver Volumen II de la guía del solicitante del PCT.

Se llama la atención a los solicitante en cuanto al Artículo 33(5), que suministra el criterio de novedad, nivel inventivo y aplicación industrial descrito en el Artículo 33(2) al (4), solamente sirve para propósitos del Examen Preliminar Internacional y "cualquiera de los estados designados pueden aplicar criterios diferentes o adicionales para los propósitos de decidir si, en el Estado, la invención reivindicada es patentable o no" (ver también Artículo 27 (5). Tales criterios adicionales se pueden relacionar, por ejemplo, a excepciones de patentabilidad, requerimientos que permitan la revelación, claridad y sustentación de las reivindicaciones.

Nombre y dirección de correo del IPEA/
Oficina Europea de Patentes
D-80298 Munich

Tel. (+49-89) 2399-0, Tx: 523656 epmu d
Fax: (+49-89) 2399-4465

Funcionario autorizado

SPORTELLINI, E

Teléfono No. (+49-89) 2399 7647

TRATADO DE COOPERACION DE PATENTES

PCT

INFORME DEL EXAMEN PRELIMINAR INTERNACIONAL

(Artículo 36 y Regla 70 del PCT)

Archivo de referencia del solicitante o del agente P018298WOP	PARA ACCION POSTERIOR Ver Notificación de Transmisión del Informe del Examen Preliminar Internacional (Formato PCT/IPEA/416)	
Solicitud internacional No. PCT/GB03/03938	Fecha de presentación internacional (día/mes/año) 10/09/2003	Fecha de prioridad (día/mes/año) 10/09/2002
Clasificación Internacional de Patente (CIP) o Clasificación Nacional y CIP G06K 19/06		
Solicitante: INGENIA HOLDINGS LIMITED et al.		
1 Este informe de examen preliminar internacional ha sido preparado por esta Autoridad Examinadora Preliminar Internacional y se transmite al solicitante de acuerdo con el Artículo 36. 2 Este INFORME consiste en un total de <u>4</u> hojas, incluyendo esta carátula. ☒ Este informe también se acompaña de los ANEXOS, esto es, hojas de descripción, reivindicaciones y/o dibujos que han sido reformados y son la base de este informe y/o hojas que contienen rectificaciones hechas ante esta Autoridad (ver Regla 70.16 y Sección 607 de las Instrucciones Administrativas según el PCT) Estos anexos consisten en un total de <u>7</u> hojas.		
3 Este informe contiene indicaciones relacionadas con los siguientes ítems: I ☒ Base del informe II ☐ Prioridad III ☐ No establecimiento de opinión con respecto a la novedad, altura inventiva y aplicación industrial IV ☐ Carencia de unidad de la invención V ☒ Declaración razonada según artículo 35(2) con relación a la novedad, altura inventiva o aplicación industrial; citas y explicaciones que apoyan tal declaración VI ☐ Ciertos documentos citados VII ☐ Ciertos defectos en la solicitud internacional VIII ☐ Ciertas observaciones sobre la solicitud internacional		

Fecha de presentación de la demanda 08/04/2004	Fecha de completamiento de este informe 25/11/2004
Nombre y dirección de correo del IPEA/JP Oficina Europea de Patentes D-80298 Munich Tel.: +49 89 2399 - 0 Tx: 523656 epmu d Fax.: +49 89 2399 - 4465	Funcionario autorizado Schmidt, R Teléfono No. 49 89 2399 2491

INFORME DE EXAMEN PRELIMINAR INTERNACIONAL

Solicitud Internacional No.
PCT/GB 03/03938

I. Base del Informe

1 Con relación a los elementos de la solicitud Internacional (las páginas reemplazadas que han sido presentadas a la oficina receptora en respuesta a la invitación con respecto al Art. 14 están referidas en este informe "originalmente presentadas" y no se anexan a este informe ya que estas no contienen modificaciones (Reglas 70.16 y 70.17):

Descripción, páginas:

1 - 56 como se presentaron originalmente

Reivindicaciones Nos.:

1 - 64 como se recibieron en 17/11/2004 con carta de 15/11/2004

Dibujos, páginas:

1/23 - 23/23 como se presentaron originalmente

2 Con relación al idioma, todos los elementos antes marcados se pusieron a disposición y se suministraron a esta autoridad en el idioma en el que se presentó la solicitud internacional, a menos que se indique de otra forma en este punto.

Estos elementos se pusieron a disposición o se suministraron a esta autoridad en el siguiente idioma inglés, el cual es:

- ☐ el idioma de una traducción suministrada para fines de investigación internacional (según la Regla 23.1(b)).
- ☐ el idioma de publicación de la solicitud internacional (bajo la Regla 48.3(b)).
- ☐ el idioma de la traducción suministrada para fines de examen preliminar internacional (bajo la Regla 55.2 y/o 55.3)

3 Con relación a cualquier nucleótido y/o secuencia amino ácida descubierta en la solicitud internacional, el examen preliminar internacional se llevó a cabo con base en la lista de secuencia:

- ☐ contenida en la solicitud internacional en forma escrita
- ☐ presentado junto con la solicitud internacional en forma leíble en computador
- ☐ suministrado con posterioridad a esta autoridad en forma escrita
- ☐ suministrado luego a esta autoridad en forma leíble en computador
- ☐ la declaración que el listado de secuencia escrito suministrado posteriormente no va más allá del descubrimiento en la solicitud internacional que se presentó ha sido suministrada
- ☐ la declaración que la información grabada en forma leíble en computador es idéntica a la lista de secuencia escrita ha sido suministrada

4 Las reformas han dado como resultado la cancelación de:

- ☐ la descripción, páginas
- ☐ las reivindicaciones, Nos.
- ☐ los dibujos, hojas/fig.

INFORME DE EXAMEN PRELIMINAR INTERNACIONAL

Solicitud Internacional No.
PCT/GB 03/03938

5 ☐ Este informe ha sido establecido como si (parte de) las reformas no han sido hechas, ya que se consideran que han ido más allá del descubrimiento que fue presentado, como se indica en la casilla suplementaria (Regla 70.2 (c)).

(Cualquier reemplazo de hoja que contenga tales correcciones debe ser referido al ítem 1 y debe ser anexado a este informe)

6 Observaciones adicionales, si es necesario:

V. Declaración razonada bajo el artículo 35(2) con relación a la novedad, altura inventiva o aplicación industrial: citas y explicaciones que apoyan tal declaración.

1 Declaración

Novedad (N)	Reivindicaciones	1-64	Si
	Reivindicaciones		No
Altura inventiva (IS)	Reivindicaciones	1-64	Si
	Reivindicaciones		No
Aplicación industrial (IA)	Reivindicaciones	1-64	Si
	Reivindicaciones		No

2 Citas y explicaciones

Ver hoja separada

INFORME DEL EXAMEN PRELIMINAR INTERNACIONAL-HOJA ANEXA
Solicitud Internacional No. PCT/GB 03/03938

Numeral V.

1. Se hace referencia al siguiente documento:
D1: US-A-5 268 043

El documento D1 no fue citado en el informe de búsqueda internacional. Una copia de dicho documento fue ya suministrado al solicitante.

2. Con respecto al objeto de la reivindicación 1, el documento D1 revela un dispositivo de seguridad que comprende al menos un elemento magnético (12), donde dicho elemento magnético es sensible al campo magnético aplicado para suministrar una respuesta característica (ver columna 5, línea 45- columna 6, línea 18).

Teniendo en cuenta que los documentos disponibles no revelan ni sugieren fabricar dicho elemento magnético de un material que comprende defectos estructurales que cause una conmutación de modo sensible en el cual el crecimiento magnético de un campo magnético único, domina el cambio de magnetización de un elemento magnético respectivo, el contenido de la reivindicación 1 cumple con los requerimientos del artículo 33 (2) y (3) del PCT.

- 2.1 Lo mismo aplica para las reivindicaciones independientes 20, 33, y 48 ya que estas contienen características relacionadas con las características de conmutación de modo sensible.

REIVINDICACIONES

1. Un dispositivo de seguridad que comprende, por lo menos, un elemento magnético, en donde dicho elemento magnético es sensible ante un campo magnético aplicado para proporcionar una respuesta característica, caracterizado en que al menos dicho elemento magnético se hace de un material que contiene defectos estructurales que causa una conmutación de modo sensible en el cual el crecimiento magnético de un campo magnético único, domina el cambio de magnetización de un elemento magnético respectivo.
2. El dispositivo de seguridad de la Reivindicación 1, en donde por lo menos un elemento magnético está sostenido por un sustrato.
3. El dispositivo de seguridad de la Reivindicación 2, en donde por lo menos un elemento magnético está sostenido en dicho sustrato.
4. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético es sensible ante el campo magnético aplicado para cambiar la magnetización o la polarización magnética de por lo menos un elemento magnético.
5. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está hecho de un material magnéticamente suave.
6. El dispositivo de seguridad de la Reivindicación 5, en donde por lo menos un elemento magnético comprende un material magnéticamente suave seleccionado de uno o más de: níquel, hierro, cobalto y aleaciones de ellos entre sí o con silicio, como aleación níquel hierro, aleación cobalto hierro, aleación hierro silicio o aleación cobalto silicio.
7. El dispositivo de seguridad de las Reivindicaciones 5 ó 6, en donde el material magnéticamente suave es un permalloy.

8. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético tiene sustancialmente forma de alambre o alambre aplanado.
9. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está protegido con una capa que refleja la luz.
10. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde por lo menos un elemento magnético está cerca de una parte con reflectividad reducida a la luz del dispositivo de seguridad.
11. El dispositivo de seguridad de cualquier Reivindicación precedente que comprende varios elementos magnéticos.
12. El dispositivo de seguridad de la Reivindicación 11, en donde varios elementos magnéticos están distribuidos para proporcionar un patrón lineal.
13. El dispositivo de seguridad de la Reivindicación 11, en donde varios elementos magnéticos están distribuidos para proporcionar un patrón bidimensional.
14. El dispositivo de seguridad de la Reivindicación 12 o de la Reivindicación 13, en donde el patrón codifica un identificador.
15. El dispositivo de seguridad de cualquier Reivindicación precedente que comprende además un identificador único incorporado en él.
16. EL dispositivo de seguridad de la Reivindicación 15, en donde el identificador único se proporciona por medio de uno o más códigos de barras legibles ópticamente; uno o más indicios ópticos; un identificador codificado magnéticamente, y un identificador electrónico.
17. El dispositivo de seguridad de la Reivindicación 16, montado en una tarjeta inteligente, en donde el identificador electrónico está en un chip de tarjeta inteligente, que se encuentra en dicha tarjeta inteligente.

18. El dispositivo de seguridad de cualquier Reivindicación precedente, en donde la información de la respuesta característica premedida que representa uno o más parámetros medibles de dicha respuesta característica se almacena en el dispositivo de seguridad.

19. El dispositivo de seguridad de la Reivindicación 18, en donde la información de la respuesta característica premedida está en forma cifrada.

20. Un método de fabricación de un dispositivo de seguridad que comprende:

proporcionar por lo menos un elemento magnético que contiene defectos estructurales, en donde por lo menos un elemento magnético proporciona una conmutación de modo sensible, respuesta característica en respuesta a un campo magnético aplicado.

21. El método de la Reivindicación 19 que comprende proporcionar por lo menos un elemento magnético en un sustrato.

22. El método de la Reivindicación 20 o de la Reivindicación 21, que comprende formar por lo menos un elemento magnético usando un proceso de levantamiento o grabado en húmedo.

23. El método de la Reivindicación 20 o de la Reivindicación 21, que comprende formar por lo menos un elemento magnético usando un proceso de grabado con un haz de iones.

24. El método de cualquiera de las Reivindicaciones 20 a 23 que comprende medir la(s) magnitud(es) de uno o más parámetros magnéticos de por lo menos un elemento magnético.

25. El método de la Reivindicación 24, que comprende medir uno o más valores de coercitividad y fluctuación.

26. El método de la Reivindicación 24 o de la Reivindicación 25, que comprende usar la(s) magnitud(es) medida(s) de uno o más parámetros

magnéticos para representar la información de la respuesta característica premedida.

27. El método de la Reivindicación 26, que comprende cifrar la información de la respuesta característica premedida.

28. El método de la Reivindicación 26 o de la Reivindicación 27 que comprende almacenar la información de la respuesta característica premedida en forma cifrada o descifrada en un dispositivo de seguridad.

29. El método de la Reivindicación 26 o de la Reivindicación 27 que comprende almacenar la información de la respuesta característica premedida en forma cifrada o descifrada en un medio de almacenamiento remoto con respecto a dicho dispositivo de seguridad.

30. El método de la Reivindicación 29 que comprende almacenar dicha información de la respuesta característica premedida en forma cifrada o descifrada en una base de datos.

31. El método de cualquiera de las Reivindicaciones 20 a 30, que además comprende proporcionar dicho dispositivo de seguridad con un identificador único.

32. El método de la Reivindicación 31 cuando dependa de cualquiera de las Reivindicaciones 27 a 30 que comprenden almacenar una representación de dicho identificador único en asociación con información de la respuesta característica premedida.

33. Un sistema para leer un dispositivo de seguridad que comprende:

un sistema de generación de un campo magnético para aplicar un campo magnético a un dispositivo de seguridad; y

un sistema de detección para medir uno o más parámetros representativos de una respuesta característica medida de una conmutación de modo sensible de dicho dispositivo de seguridad en respuesta a un campo magnético,

en donde el sistema funciona para comparar uno o más parámetros representativos de una respuesta característica medida de una conmutación de modo sensible a uno o más parámetros respectivos de una respuesta característica premedida de una conmutación de modo sensible, para determinar si los parámetros medidos y premedidos respectivos son sustancialmente equivalentes.

34. El sistema de la Reivindicación 33, en donde el sistema de generación del campo magnético funciona para aplicar un campo magnético variable en el tiempo a un dispositivo de seguridad.

35. El sistema de la Reivindicación 33 o la Reivindicación 34, en donde el haz de luz se usa para interrogar un dispositivo de seguridad.

36. El sistema de cualquiera de las Reivindicaciones 33 a 35, en donde dicho haz de luz es un haz visible o cerca al infrarrojo producido por un diodo láser.

37. El sistema de cualquiera de las Reivindicaciones 33 a 36, en donde los parámetros representan uno o más valores de coercitividad y fluctuación.

38. El sistema de cualquiera de las Reivindicaciones 35 a 37, en donde el sistema de detección incorpora un dispositivo de detección del efecto magneto-óptico Kerr, para detectar cambios inducidos en el haz de luz por elementos magnéticos del dispositivo de seguridad.

39. El sistema de la Reivindicación 38, en donde el aparato de detección del efecto magneto-óptico Kerr está configurado para operar en modo transversal.

40. El sistema de cualquiera de las Reivindicaciones 35 a 39, que funciona además para desviar un haz de rayos de luz a través de la superficie del dispositivo de seguridad.

41. El sistema de cualquiera de las Reivindicaciones 33 a 40, que funciona además para leer un identificador único del dispositivo de seguridad.

42. El sistema de la Reivindicación 41, en donde el identificador único es identificado por el reconocimiento de un patrón de elementos magnéticos soportados por el dispositivo de seguridad.

43. El sistema de la Reivindicación 41 o de la Reivindicación 42, en donde el identificador único es identificado por leer uno o más de: un código de barras legible ópticamente, uno o más indicios ópticos, un identificador codificado magnéticamente y un identificador electrónico.

44. El sistema de cualquiera de las Reivindicaciones 33 a 43, que funciona además para determinar uno o más parámetros respectivos de la respuesta característica premedida, mediante la lectura de uno o más parámetros del dispositivo de seguridad.

45. El sistema de cualquiera de las Reivindicaciones 34 a 44, que funciona además para determinar uno o más parámetros de la respuesta característica premedida, mediante la lectura de uno o más parámetros de una base de datos.

46. El sistema de la Reivindicación 45, en donde la base de datos está localizada a distancia del sistema de detección.

47. El sistema de cualquiera de las Reivindicaciones 33 a 46 que funciona además para descifrar la información de la respuesta característica premedida cuando se lea o se suministre en una forma cifrada.

48. Un método para leer un dispositivo de seguridad, que comprende:

aplicar un campo magnético a un dispositivo de seguridad;

medir uno o más parámetros representativos de una respuesta característica medida de una conmutación de modo sensible de dicho dispositivo de seguridad en respuesta a dicho campo magnético; y

comparar uno o más de dichos parámetro(s) representativos de una respuesta característica medida de una conmutación de modo sensible a uno o más parámetro(s) respectivos de una respuesta característica premedida de una

conmutación de modo sensible para determinar si los parámetros medidos y premedidos respectivos son sustancialmente equivalentes.

49. El método de la Reivindicación 48 que comprende aplicar un campo magnético variable en el tiempo a un dispositivo de seguridad.

50. El método de la Reivindicación 48 o de la Reivindicación 49, en donde medir uno o más parámetros representativos de una respuesta característica medida del dicho dispositivo de seguridad en respuesta al campo magnético comprende medir uno o más valores de coercitividad y fluctuación.

51. El método de cualquiera de las Reivindicaciones 48 a 50 que comprende interrogar el dispositivo de seguridad usando un haz de luz.

52. El método de cualquiera de las Reivindicaciones 48 a 51 que comprende operar un láser para producir un haz visible o cerca al infrarrojo.

53. El método de la Reivindicación 51 o de la Reivindicación 52 que comprende detectar cambios inducidos en el haz de luz por medio de elementos magnéticos del dispositivo de seguridad, usando el efecto magneto-óptico Kerr.

54. El método de la Reivindicación 53 que comprende usar el modo transversal del efecto magneto-óptico Kerr.

55. El método de cualquiera de las Reivindicaciones 51 a 54 que comprende desviar el haz de luz a través de la superficie de dicho dispositivo de seguridad.

56. El método de cualquiera de las Reivindicaciones 48 a 55 que comprende leer un identificador único del dispositivo de seguridad.

57. El método de la Reivindicación 56 que comprende identificar el identificador único mediante el reconocimiento de un patrón de elementos magnéticos soportado por el dispositivo de seguridad.

58. El método de la Reivindicación 56 o de la Reivindicación 57 que comprende identificar el identificador único mediante la lectura de uno o más de: un código de

barras legible ópticamente, uno o más indicios ópticos, un identificador codificado magnéticamente y un identificador electrónico.

59. El método de cualquiera de las Reivindicaciones 48 a 58 que comprende determinar uno o más parámetros respectivos de la respuesta característica premedida mediante la lectura de uno o más parámetros desde el dispositivo de seguridad.

60. El método de cualquiera de las Reivindicaciones 48 a 59 que comprende determinar uno o más parámetros respectivos de la repuesta característica premedida, mediante la lectura de uno o más parámetros de una base de datos.

61. El método de la Reivindicación 60 que comprende acceder a una base de datos ubicada a distancia del sistema de detección.

62. El método de cualquiera de las Reivindicaciones 48 a 61 que además comprende descifrar la información de la respuesta característica premedida cuando se lee o proporciona en forma cifrada.

63. Un producto que comprende el dispositivo de seguridad de cualquiera de las Reivindicaciones 1 a 19.

64. El producto de la Reivindicación 63 que comprende uno o más de: un documento, un pasaporte, una tarjeta de identificación, un disco compacto, un disco versátil digital, un producto de software, empaque, una prenda de vestir, un artículo de calzado, una tarjeta inteligente, una tarjeta de crédito o bancaria, un producto cosmético, una pieza de ingeniería, un accesorio, y cualesquier otros bienes y /o artículos de comercio, sean fabricados o de otro modo.

235

SUPERINDUSTRIA Y COMERCIO
Radicacion : 05031640 00000000
Fecha (AMD): 2005-04-08 14:22:39
Tramite : 011 PCT-PATENT 379 FASE NACI 411 PRESENTA
Dependencia: 6020 DIVISION DE NUEVAS CREACIONES

Folios: 234

REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION DEL TRAMITE

	USUARIO	RADICADOR
PATENTE DE INVENCION ☒ MODELO DE UTILIDAD	()	()
Indicacion de que se solicita la concesion de una patente.	()	()
Datos de Identificacion del solicitante o de la persona que se presenta la solicitud.	()	()
Descripcion de la invencion.	()	()
Dibujos de ser estos pertinentes.	()	()
Comprobante de Pago de las tasas establecidas.	()	()
COMPLETA () INCOMPLETA ()	()	()
DISEÑO INDUSTRIAL ()		
Indicacion de que se solicita el registro de Diseño Industrial	()	()
Datos de Identificacion del solicitante o de la persona que presenta la solicitud.	()	()
Representacion grafica o fotografica del Diseño Industrial o muestra del Material que incorpora el diseño.	()	()
Comprobante de pago de las tasas establecidas	()	()
COMPLETA () INCOMPLETA ()	()	()
ESQUEMA DE TRAZADO ()		
Indicacion de que solicita el registro de un Esquema de trazado.	()	()
Datos de Identificacion del solicitante o de la persona que presenta La solicitud.	()	()
Representacion grafica del esquema de trazado	()	()
Comprobante de pago de las tasas establecidas.	()	()
COMPLETA () INCOMPLETA ()	()	()

Firma Responsable: *Claudia M Nave*

Fecha:

2020
Bogotá, D.C.,

Doctora:
MARGARITA CASTELLANOS A.
INGENIA HOLDINGS LIMITED & INGENIA TECHNOLOGY LIMITED
Solicitante

Oficio N° 13777

ASUNTO:	Radicación N°	05-31840
	Solicitud internacional	PCT/GB2003/003938
	Fecha limite inicio fase nacional	11/04/2005
	Trámite	011
	Evento	379
	Actuación	430
	Folios	001

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

- La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486).
- La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única N° 10 de 2001.



DORIS ELENA POLO CORDOBA
Jefe de la División de Nuevas Creaciones. (E)

El anterior requerimiento fue notificado por fijación en lista de fecha, 13 MAYO 2005.

202030