

G1



Industria y Comercio

SUPERINTENDENCIA

Delegatura de propiedad Industrial

División de Nuevas Creaciones

P.C.T

SOLICITUD

PATENTE DE INVENCION

— PCT ENTRADA EN FASE NACIONAL —.

21. EXPEDIENTE No.

05-31844

54. TÍTULO "DISPOSITIVO Y SISTEMA DE SEGURIDAD"

51. CLASIFICACIÓN INTERNACIONAL

71. SOLICITANTE INGENIA. HOLDINGS LIMITED E
INGENIA. TECHNOLOGY LIMITED.

DOMICILIO TORTOLA, ISLAS VIRGENES BRITANICAS Y
LONDRES, INGLATERRA, REINO UNIDO.

74. APODERADO DRA. MARGARITA CASTELLANOS ABONDANO.

22. BOGOTÁ, D. C., 08 ABR. 2005

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 6, 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 70,619

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/GB2003/003917

Fecha 10/09/2003

Publicación Internacional No. WO 2004/025548

Fecha 25/03/2004

⑥

Título (54)

"DISPOSITIVO Y SISTEMA DE SEGURIDAD"

⑦

Clasificación Internacional (51)

G08K 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.

05-17,043

Fecha

Marzo 07 de 2005

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

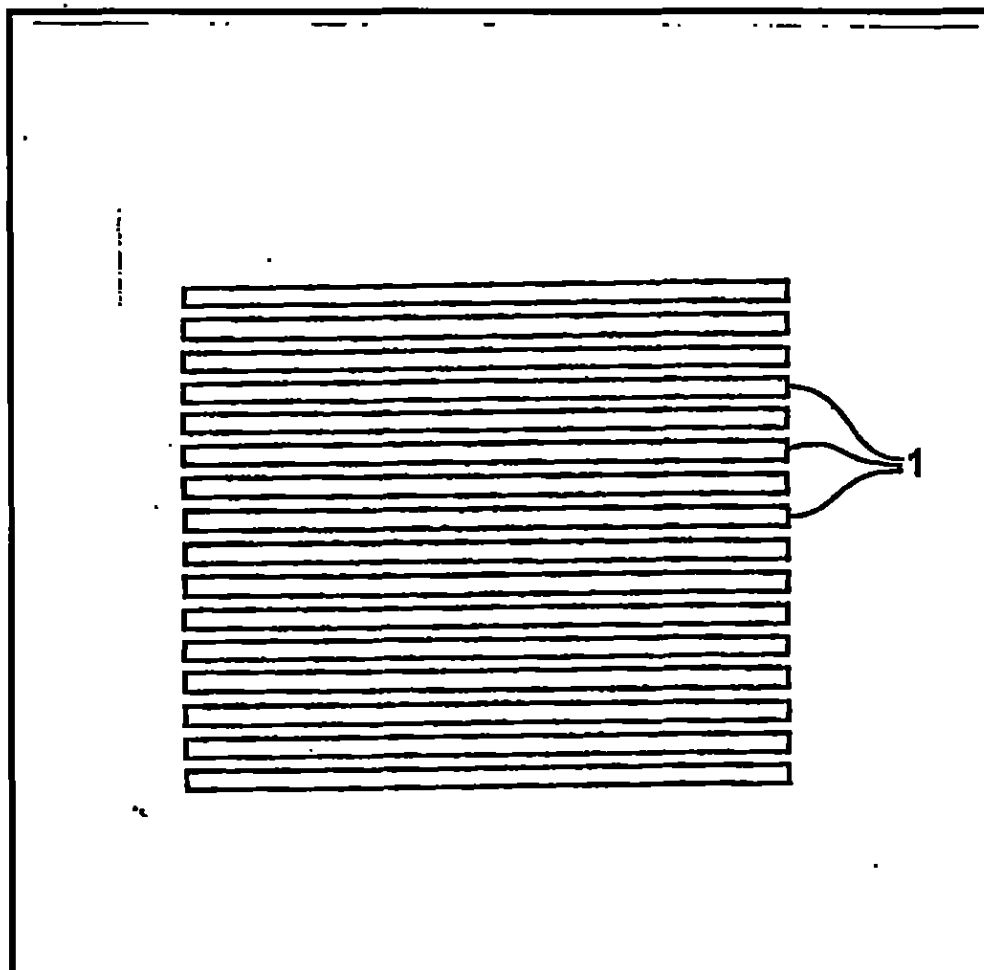
10

Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredita 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 con anexos y traducción del formato IPEA/416

11

FIGURA CARACTERISTICA:



12

Solicito la concesión de la patente,

08 ABR. 2005

NOMBRE: MARGARITA CASTELLANOS ABONDANO

FIRMA:

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

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

SUPERINDUSTRIA Y COMERCIO
Radicacion : 05031044 00000000
Fecha (HND): 2005-04-08 14:21:35
Tramite : 011 PCT-PATENT 379 FASE NACI 411 PRESENTAC
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES
Folios: 207

RECIBO OFICIAL DE CAJA : 05 - 17,043
FECHA : MARZO 7 DE 2005

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	Vr. PAGO
ALVARO CASTELLANOS	CONSIGNACION	BANCO POPULAR	050-00110-6	37803175	07/03/2005	6,772,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50003-01-01	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
Organisation
International Bureau



4977-FNrep 4

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

PCT

(10) International Publication Number
WO 2004/025548 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 3DA (GB).

(21) International Application Number:
PCT/GB2003/003917

(81) Designated States (national): AO, 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, GR, GM, HN, HU, ID, IL, IN, IS, JP, KE, KG, KH, 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

(30) Priority Data:
0330907.0 10 September 2003 (10.09.2003) GB

(84) Designated States (regional): ARIPO patent (OH, OM, KE, LS, MW, MZ, SD, SL, 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, NI, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

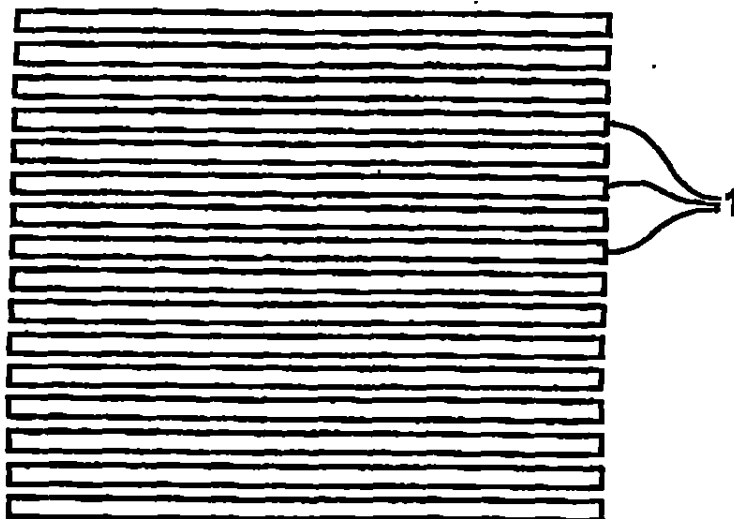
Declaration under Rule 4.17:
— of inventorship (Rule 4.17(iv)) for US only

(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 1TA (GB).

Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: SECURITY DEVICE AND SYSTEM



(57) Abstract: Disclosed is a security device (700) comprising two or more magnetic elements (702). The magnetic elements (702) are responsive to an applied magnetic field to provide a characteristic response that is difficult to reproduce. The security device (700) finds application in detecting forgeries.

WO 2004/025548 A1

WO 2004/025548 A1

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

SECURITY DEVICE AND SYSTEM

One aspect of the invention relates to a security device, for example to
5 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
10 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.

15

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:

- 20 • 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;
- 25 • 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

PIE298WO

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.

P18298WO

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.

5

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.

15

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

- That it be possible to measure the signature easily and without excessive cost;
- 20 • 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;
- 25 • 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 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
5 item which is inherently difficult to copy and thus limits counterfeiting.

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
10 authentication/ counterfeit prevention of high value items.

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

15 Various aspects of the invention are described herein and set out in the appended claims.

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
20 large 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
25 magnetic material, such as thin magnetic wires or strips, or dots. The magnetic material may be in the micro, macro or even nanoscale, and may include microwires or microdots, or even nanowires 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
P1234567890

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 comprising a part of an object adapted for use in its own
- 10 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.
- 20 Examples of suitable collections of magnetic elements are described in R.P.Cowburn, Journal of Physics D, 33, R1 (2000). The present invention may rely upon their singular effectiveness in creating a random signature for anti-forgery.
- 25 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 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
- P1628WO

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 similar a way as possible to each cycle of the time-varying applied magnetic field.

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.

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. 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

P18298WO

response can be decrypted and comparison can be made with a measured response.

In order to test the authenticity of an item protected by a random signature, it
5 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
10 baseline responses which can be compared to the predetermined, expected
baseline response to authenticate the device.

Authentication relies on the inherently random nature of the device.
Artificially fabricated magnetic elements make a very good practical random
15 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
20 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
25 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.

P11231WO

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
5 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,
10 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
15 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
20 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
25 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
5 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.

10 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.

15 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,
20 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,
25 for example being square or circular, or some other regular geometric shape, which may for example be formed into a two dimensional array.

As used herein reference made to magnetic wires, microwires or nanowires should be construed as being to such elements of elongated form, and in
PIA298WO

- 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 should be construed as being to such
- 5 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.
- 10 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.
- 15 The elements may be made from a magnetic material, which will by preference 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.
- 20 The elements may be coated with a protective overlayer to prevent oxidation or 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
- 25 conveniently transparent. Particular examples of protective overlayers include titanium dioxide, transparent epoxy resin, plastic or glass, transparent modified silicone resin conformal coating and transparent acrylic conformal coating.

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
5 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
10 include silicon, glass, plastic or some other material with a smooth surface.

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
15 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,
20 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.

25 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
F1A298WO

information about the article, pricing information, stock control information etc.

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.

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.

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.

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.

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

P12397WO

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.

5

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

10 fields.

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

15 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.

20

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

25 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 μ m wide wire; the next would be 2.53 μ m, the next 2.56 μ m etc, until 56 wires later the width has risen to 5 μ m. The total wire width is 200 μ m in this example. An alternative ensemble might start with a 1 μ m wide wire; the next would be 1.01 μ m, the next 1.02 μ m etc, until 450 wires later the width has risen to 5 μ m. 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. In the foregoing examples such a single wide wire could be 1 mm long and 150 μ m 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 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 embodiments of the invention. It will however be understood that it is not necessary that such a predetermined base line magnetic signature response is

PLEASEWO

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, 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-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.

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 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 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 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, 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 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 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).

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.

PLEASEWO

In the third embodiment referred to above, the prerecorded/premeasured 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 identification systems with multiple points of access etc.

10

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 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 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.

25

For different applications, suitable systems may comprise a plurality of such 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
5 network.

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-
10 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
15 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
20 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
25 incorporates or is in data communication with a store of predetermined responses.

In all cases, the device reader preferably makes a comparison between the measured and predetermined baseline magnetic signature responses, for
FIGURE TWO

19

example against a predetermined tolerance limit, and actuates a response mechanism depending upon whether signatures are identical, for example within those tolerance limits.

- 5 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
10 an item of restricted equipment, access to a particular service or the like.

- 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
15 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
20 have a transparent protective overlayer. In various embodiments the magnetic material remains optically reflective.

- 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
25 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
- P11239WO

applied. Optionally, the device incorporates or is provided with a magnetic field generator to generate such a field.

In various embodiments, the transverse magneto-optical Kerr effect is used to
5 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
10 apply the same.

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
15 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
20 polariser may be included, for example in the in-coming beam path in conventional manner, where this is desirable or necessary.

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
25 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.

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,
P1234567

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 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 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 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.

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.

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
5 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
10 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 $0.5\ \mu\text{m}$ with a centre-to-centre spacing of $1.5\ \mu\text{m}$. If the photoresist is left in place, then the structures comprise a set of $0.5\ \mu\text{m}$ wires attached to the substrate, and an
15 equal number (minus 1) of $1\ \mu\text{m}$ wires attached to the top of the substrate.

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
20 as hereinbefore described therewith.

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
25 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.

The invention will now be described by way of example only with reference to Figures 1 to 16 of the accompanying drawings in which:

Figure 1 is an illustration of a first collection of magnetic elements used for a random magnetic signature in accordance with the invention;

5 Figure 2 is an illustration of a second collection of magnetic elements for such use;

Figure 3 is an illustration of a third collection of magnetic elements for such use;

10 Figure 4 is an illustration of a device for measuring the magnetic response of a small area of thin magnetic film, such as the signatures in Figures 1 to 3;

Figure 5 is an illustration of an embodiment of the invention in a smart card;

Figure 6 is an illustration of an embodiment of the invention in an electronic key;

15 Figure 7 is an illustration of an embodiment of the invention in an identity tag for attachment to an item to be protected;

Figure 8 is an illustration of an embodiment of the invention incorporated into a CD for authentication purposes;

Figure 9 is an illustration of an embodiment of the invention incorporated onto a certificate for authentication purposes;

20 Figures 10a to 10h illustrate a manufacturing technique for producing various embodiments of security devices according to the present invention;

Figure 11 shows a reading arrangement according to the present invention;

Figure 12 shows a component of reading arrangement according to the present invention;

25 Figure 13 shows a coil driving signal;

Figure 14 shows a synchronisation signal;

Figure 15 shows a coil driving signal; and

Figure 16 shows a unipolar detector signal.

Referring first to Figures 1 to 3, illustrations of three example structures of magnetic elements are provided in plan view.

5 In the first, a collection of regular rectangular magnetic elements (1) is shown schematically and not to scale. The material of the elements is $\text{Ni}_{40}\text{Fe}_{60}$. 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.

10

Moreover, any representation that the elements are of equal widths is schematic only. An array of 1 μm 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
15 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.

Figure 2 shows a generally similar structure having generally similar
20 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
25 from the principles of the invention.

On Figure 3 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
FIG 3

- microdot is 100 μm 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.

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

- Figure 4 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 1 to 3.
- 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
- 5 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 $0^\circ - 60^\circ$. Additional magnetic field coils can be present to apply an additional field transversely to the long-axis of the wire.
- 10 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
- 15 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
- 20 recorded signal. These are then passed to other electronics (not shown) which acquire and if necessary decipher 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
- 25 baseline response, and a comparison is made.

Figure 5 illustrates the application of the present invention to a smart shipped 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

FIGURE 5

a credit card or 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
5 for backward compatibility with magnetic stripe only systems.

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,
10 it sits within the foot print of the smart chip itself as illustrated by the broken line (28). For many 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
15 chip. However, such placement is purely for convenience, and the magnetic elements (26) could be placed elsewhere on the card.

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
20 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 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
25 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 incorporating a signature device reader such as that illustrated in Figure 4. The device reader may be incorporated into an existing smart card reader. For example, with the embodiment shown, the reading device for the magnetic
5 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 difficulty. In this way, cards and readers remain backwards compatible to conventional card/reader technology not having the identification and authentication system herein described.

10

The reader measures an actual response from the card. An expected baseline 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
15 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 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.

20

The smart card in accordance with various embodiments of the invention will 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.
25 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.

The system represented by the embodiment in Figure 5 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
5 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 5 as part of a financial services system, for example as a credit card, a system can be
10 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
15 will also readily suggest themselves.

In Figure 6 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
20 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 6.

25

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 4.

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 6 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 6 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.

20

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.

25

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
5 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
10 way.

A further embodiment of the invention is illustrated in Figure 7. In Figure 7, 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
15 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
20 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.

25

The embodiment of Figure 7 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,
P18298WO

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
5 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 7 will
10 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
15 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.

20 Figure 8 illustrates a data storage disk such as a CD, DVD or the like to which 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
25 elsewhere on the disc.

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
P1238WO

and destination of genuine originals, and to identify unauthorised importation and the like.

In a more advanced mode of operation, disc readers can be manufactured
5 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 arrangement.

10

Figure 9 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, an identity or authorisation certification intended to
15 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 example a photograph, written information (63), and a bar code (64). It might
20 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
25 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.

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, paper money and the like, important legal documents, and other such documentation.

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 10a to 10h. The process starts in Figure 10a 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.

Figure 10c illustrates the device of Figure 10b 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 P123rwo

system with a LaserWriter add-on 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.

Figure 10d shows the device of Figure 10c 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 10e, magnetic elements 702 formed of a 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 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 10f. The capping layer 718 is designed to protect the permalloy layer from oxidation and also 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 10g. 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.

PIA296WO

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 10h.

10 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.

5

Where embodiments of the invention use the magnetic switching properties of the material to produce a signature, baseline or characteristic response, magnetically soft materials are useful. Magnetically soft materials are ferromagnetic materials in which the magnetism can be easily reversed. These materials generally have narrow square-shaped hysteresis loops. Thus, the magnetisation of a magnetic element made from 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 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.

20

A measurement of jitter may be used to provide a parameter relating to a signature, baseline or characteristic response. A jitter measurement may be made by repeating measurements on the magnetic elements and determining how much the coercivity varies between sets of measurements. These sets of measurements can be repeated many times for the magnetic elements of the security device. In one example, coercivity may be measured one hundred times for the magnetic elements at room temperature. The measured coercivity values are then fitted to a Gaussian bell-curve, and the mean

25

coercivity and jitter (as indicated by the mean and standard deviation Δ of the fitted Gaussian curve, respectively) calculated.

5 Magnetic elements may be tested to determine whether or not they operate in a repeatable manner. A Kerr magnetometer, as described in Applied Physics Letters, Vol. 73, p. 3947, 1998, is used to measure the coercivity of the magnetic elements.

10 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.

15 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
20 between the two sets to compensate for different temperatures.

However, if desired or required for various other embodiments, coercivity and/or jitter measurements may be made at several temperatures, including temperatures outside a normal operating temperature range. For example, sets
25 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 various embodiments, security devices may have their baseline or premeasured characteristic response defined by a mean coercivity value and/or a jitter value Δ determined as indicated above. Various other embodiments use, for example, either a mean coercivity value or a jitter value to represent a baseline or premeasured characteristic response. In use, the baseline or premeasured characteristic response of a security device is compared to its measured characteristic response to determine if that security device is a forgery.
- 10 The baseline or 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 herein) the digitised values of mean coercivity and/or jitter value Δ representing a baseline or 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 signature or characteristic response has been measured is a forgery.

- 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 signature or characteristic response of a particular security device in order that it may be compared to a baseline or premeasured characteristic response. Any differences between the measured and premeasured response, outside of any allowable limits, indicate that the security device that has been read is a forgery.

P18295W0

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.

5

Various embodiments of systems for reading security devices, both hand-held or otherwise are envisaged. Various such embodiments are described herein in connection with Figures 11 to 16 of the drawings.

- 10 Figure 11 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 and/or intensity of light reflected from the magnetic elements
15 using the magneto-optic Kerr effect (MOKE).

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 aluminium block 934 is typically 2 cm x 2 cm x 1
20 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 to 1550 nm. One embodiment uses a laser diode operating at 670 nm. The laser beam 944 passes through a first beam
25 path channel 938, before it leaves the aluminium block 934 and is incident upon a mirror 950.

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
P1829FWO

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.

- 5 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
10 parallel to the axis of the magnetic elements 902.

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
15 second an orthogonal polarity. Light of the first polarity is reflected from magnetic elements 902 and gives rise to an aggregate signal that measures the mean polarisation/reflectivity state (sometimes known as the aggregate response) of the magnetic elements illuminated by the beam 947.

- 20 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
25 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 focusing 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
 5 signal proportional to the magnetisation of any magnetic elements 902 illuminated by the plane polarised laser beam 947.

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

The field generation system 935 comprises components for producing a time varying applied magnetic field 932 for applying to a security device 900. The
 15 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
 20 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).

The field generation system 935 additionally comprises a cross-over detector
 25 968 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 14. The synchronisation signal 981 is composed 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.

- 5 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
- 10 (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.
- 15 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
- 20 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 signature/characteristic response of the security device
- 25 900 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.

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.

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 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 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).

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 signature or 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).

5

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.

10
15

Various ways exist for determining the baseline or 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 baseline/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.

20
25

In various other embodiments, a smart card carries a security device and unique identifier and encrypted baseline or premeasured characteristic response information are stored in the smart card. The smart card is read in a

conventional manner and a measured signature or characteristic response is measured as herein described.

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 baseline or 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
10 operable to determine a unique identifier for each security device and to retrieve baseline or premeasured characteristic response information corresponding to the unique identifier determined by the security device reading system. The baseline or premeasured characteristic response information can then be decrypted as necessary by a respective security device
15 reader.

In embodiments of the security device reading system, once the information regarding the measured signature or characteristic signal response has been extracted it is compared by the microprocessor to the baseline or premeasured
20 characteristic response, possibly decrypted using a private asymmetric data key, to determine whether or not the security device 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.

25 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 signature or 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.

20

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.

25

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.

- 5 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
- 10 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 from a remote source
- 15 embodied in a carrier medium such as an electronic signal, including radio frequency carrier wave or optical carrier wave.

- The foregoing examples are merely illustrative of the possible uses of a device in accordance with various aspects of the invention. It will be appreciated that
- 20 a signature device in accordance with various embodiments of the invention could have a huge range of applications, in particular being applicable to any situation where significant commercial or security issues arise from the misuse of counterfeit copies of original items.

- 25 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 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
- P1829FWO

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 be varied programmably, for example, under the control of a microprocessor, possibly in dependence upon
5 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 irrespective of whether or not it relates to the claimed invention or
10 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 dependent claims,
15 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.

20

CLAIMS

- 5 1. A security device comprising two or more magnetic elements, wherein said magnetic elements are responsive to an applied magnetic field to provide a characteristic response.
2. The security device of Claim 1, wherein said characteristic response is
10 provided in combination with a premeasured characteristic response.
3. The security device of Claim 1 or Claim 2, wherein said characteristic response represents an aggregate response of said magnetic elements to said applied magnetic field.
- 15 4. The security device of any preceding Claim, wherein said magnetic elements are supported by a substrate.
5. The security device of Claim 4, wherein said magnetic elements are
20 supported on said substrate.
6. The security device of any preceding Claim, wherein the magnetic elements comprise thin layer magnetic material.
- 25 7. The security device of Claim 6, wherein the thin layers of magnetic material are less than 1 μm thick.
8. The security device of Claim 7, wherein the thin layers of magnetic material between 10 nm and 100 nm thick.

9. The security device of any preceding Claim, wherein said magnetic elements are responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of at least one of the magnetic elements.
- 5 10. The security device of any preceding Claim, wherein at least one of the magnetic elements is made from a magnetically soft material.
11. The security device of Claim 10, wherein at least one of the magnetic elements 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.
- 10 12. The security device of Claim 10 or 11, wherein said magnetically soft material is a permalloy material.
- 15 13. The security device of any preceding Claim, wherein at least one of the magnetic elements is substantially wire-shaped or flattened wire shaped.
- 20 14. The security device of any preceding Claim, wherein the device comprises a generally parallel array of elongate rectangular magnetic elements.
- 25 15. The security device of Claim 14, wherein the magnetic elements comprise an array of generally parallel magnetic nanowires.
16. The security device of any preceding Claim, wherein the magnetic elements have generally the same size and/or shape.

17. The security device of any preceding Claim, wherein several discrete groups of differently sized and/or shaped magnetic elements, the magnetic elements being generally similarly sized and/or shaped within each group, are provided so that several different switching fields can be identified.
- 5
18. The security device of Claim 17, comprising an ensemble of rectangular magnetic elements in parallel array including several discrete groups of magnetic elements of different widths.
- 10
19. The security device of any preceding Claim, wherein differently sized and/or shaped magnetic elements are provided in a continuously varying array, so that variations in sized and/or shape between a magnetic element and its neighbours are minimised to avoid large discontinuities.
- 15
20. The security device of Claim 19, comprising an ensemble of rectangular magnetic elements in parallel array of width varying continuously across the array.
21. The security device of any preceding Claim, further comprising a single
- 20
- relatively large area magnetic element for use as a reference element.
22. The security device of any preceding Claim, wherein at least one of the magnetic elements is backed by a light reflective layer.
- 25
23. The security device of any preceding Claim, wherein at least one of the magnetic elements is provided proximal a reduced light reflectivity portion of said security device.

24. The security device of any preceding Claim, wherein the magnetic elements are arranged to provide a linear pattern.
25. The security device of any preceding Claim, wherein said magnetic elements are arranged to provide a two-dimensional pattern.
26. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.
27. The security device of claim 26, 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.
28. The security device of claim 27, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.
29. 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.
30. The security device of Claim 29, wherein said premeasured characteristic response information is in encrypted form.
31. The security device of Claim 30, wherein said premeasured characteristic response information 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 security device.

32. The security device of Claim 2 or any one of Claims 3 to 31 when
5 dependent on Claim 2, wherein the premeasured characteristic response is stored in physical proximity to the security device in machine-readable form.

33. A method of manufacturing a security device, comprising:
providing two or more magnetic elements, wherein said magnetic
10 elements provide a characteristic response in response to an applied magnetic field.

34. The method of Claim 33, comprising providing said magnetic elements
on a substrate.

15 35. The method of Claim 33 or Claim 34, comprising forming at least one of the magnetic elements using a lift off or wet etching process.

36. The method of Claim 33 or Claim 34, comprising forming at least one
20 of the magnetic elements using an ion beam etching process.

37. The method of any one of Claims 33 to 36, comprising measuring the magnitude(s) of one or more magnetic parameters of said magnetic elements.

25 38. The method of Claim 37, comprising measuring one or more of coercivity and jitter values.

39. The method of Claim 37 or Claim 38, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.

5 40. The method of Claim 39, comprising encrypting said premeasured characteristic response information.

41. The method of Claim 39 or Claim 40, comprising storing said premeasured characteristic response information in encrypted or unencrypted
10 form on said security device.

42. The method of Claim 39 or Claim 40, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.
15

43. The method of Claim 42, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.

20 44. The method of any one of Claims 33 to 43, further comprising providing said security device with a unique identifier.

45. The method of Claim 44 when dependant upon any one of Claims 39 to 43, comprising storing a representation of said unique identifier in association
25 with said premeasured characteristic response information.

46. A system for reading a security device, comprising:

a magnetic field generation system for applying a magnetic field to a security device comprising two or more magnetic elements; and

P18298WO

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
5 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.

10 47. The system of Claim 46, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

48. The system of Claim 46 or Claim 47, wherein the magnetic field
15 generation system is operable to apply a time varying magnetic field to a security device.

49. The system of any one of Claims 46 to 48, wherein a light beam is used
to interrogate said security device.

20

50. The system of Claim 49, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

51. The system of any one of Claims 46 to 50, wherein said parameters
25 represent one or more of coercivity and jitter values.

52. The system of any one of Claims 49 to 51, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for

57

detecting changes induced in said light beam by magnetic elements of said security device.

53. The system of Claim 52, wherein said magneto-optic Kerr effect
5 detection apparatus is configured to operate in transverse mode.

54. The system of any one of Claims 36 to 40, further operable to deflect
said light beam across the surface of said security device.

10 55. The system of any one of Claims 46 to 54, further operable to read a
unique identifier from said security device.

56. The system of Claim 55, wherein said unique identifier is identified by
reading one or more of: an optically readable bar code; one or more optical
15 indicia; a magnetically encoded identifier; and an electronic identifier.

57. The system of any one of Claims 46 to 56, further operable to
determine said one or more respective parameters of the premeasured
characteristic response by reading said one or more parameters from said
20 security device.

58. The system of any one of Claims 46 to 57, further operable to
determine said one or more respective parameters of the premeasured
characteristic response by reading said one or more parameters from a
25 database.

59. The system of Claim 58, wherein said database is remotely located
from said detection system.

P1829FWO

60. The system of any one of Claims 46 to 59, further operable to decrypt premeasured characteristic response information where it is read or provided in encrypted form.

5 61. A method for reading a security device, comprising:

applying a magnetic field to a security device comprising two or more magnetic elements;

measuring one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field; and

10 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.

15

62. The system of Claim 61, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

20 63. The method of Claim 61 or Claim 62, comprising applying a time varying magnetic field to a security device.

64. The method of any one of Claims 61 to 63, 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.

25 65. The method of any one of Claims 61 to 64, comprising interrogating said security device using a light beam.

P15295WO

66. The method of any one of Claims 61 to 65, comprising operating a laser to produce a visible or near-infrared beam.
- 5 67. The method of Claim 65 or Claim 66, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.
68. The method of Claim 67, comprising using the magneto-optic Kerr
10 effect transverse mode.
69. The method of any one of Claims 61 to 68, comprising reading a unique identifier from said security device.
- 15 70. The method of Claim 69, 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.
71. The method of any one of Claims 61 to 70, comprising determining
20 said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.
72. The method of any one of Claims 61 to 71, comprising determining
25 said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.
73. The method of Claim 72, comprising accessing a database remotely located from said detection system.

74. The method of any one of Claims 61 to 73, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.

5 75. A product comprising the security device of any one of Claims 1 to 32.

76. The product of Claim 75, 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
10 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.

1/13

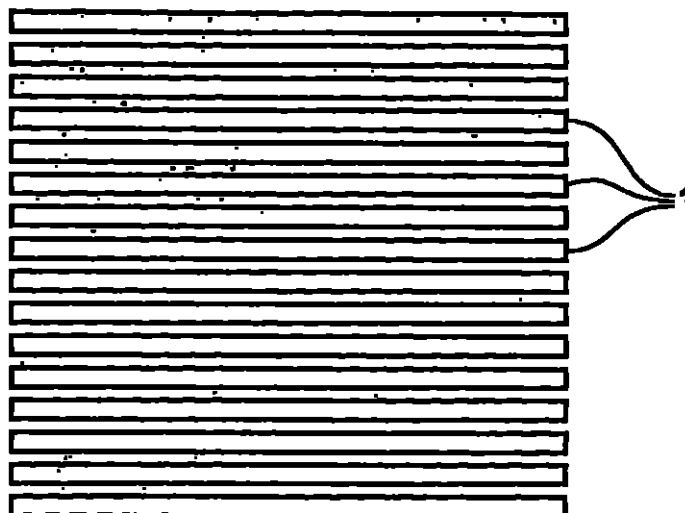


Fig. 1

SUBSTITUTE SHEET (RULE 26)

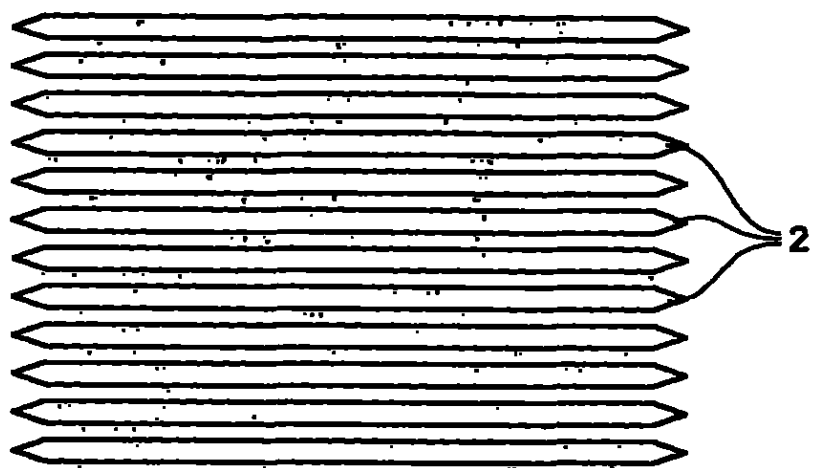


Fig. 2

3/13

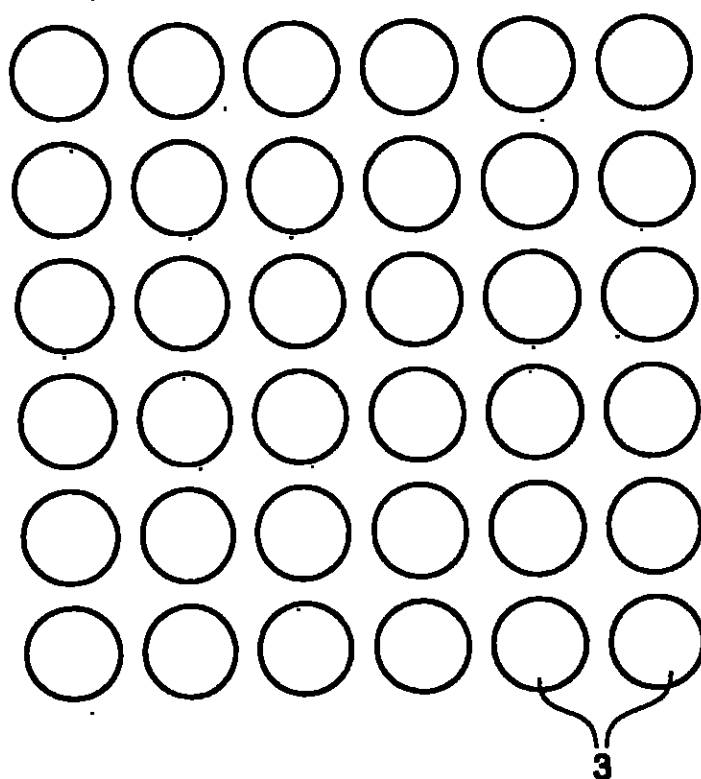


Fig. 3

4/13

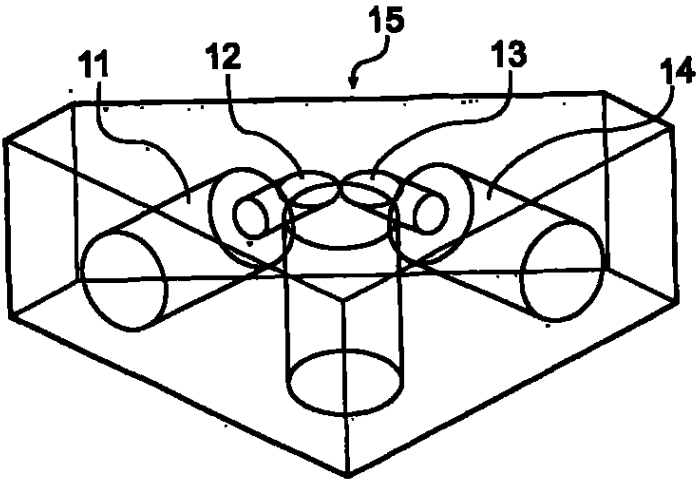


Fig. 4a

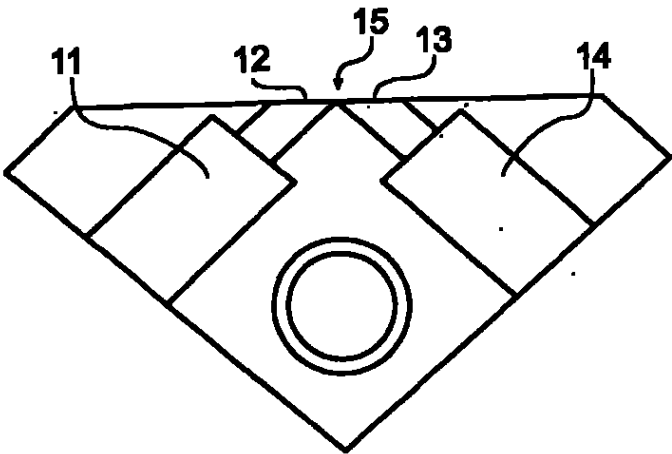


Fig. 4b

5/13

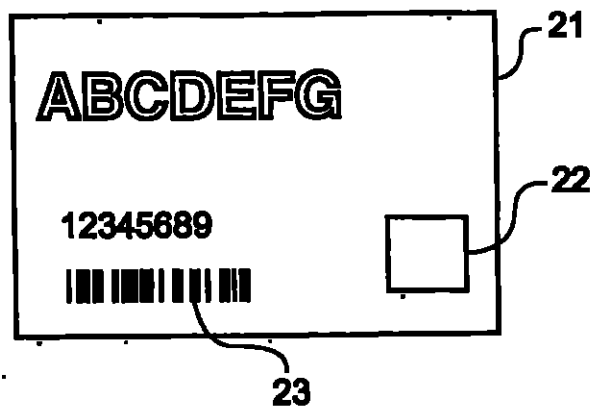


Fig. 5a

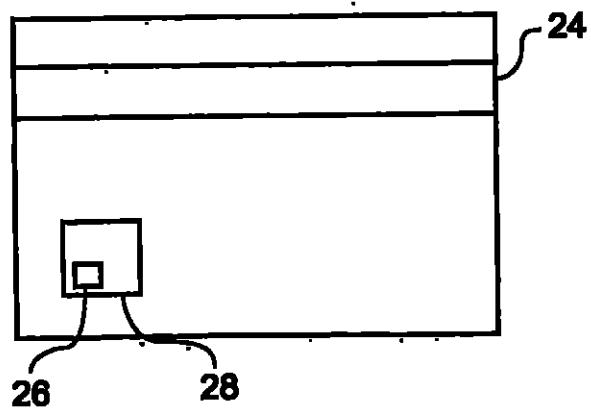


Fig. 5b

6/13

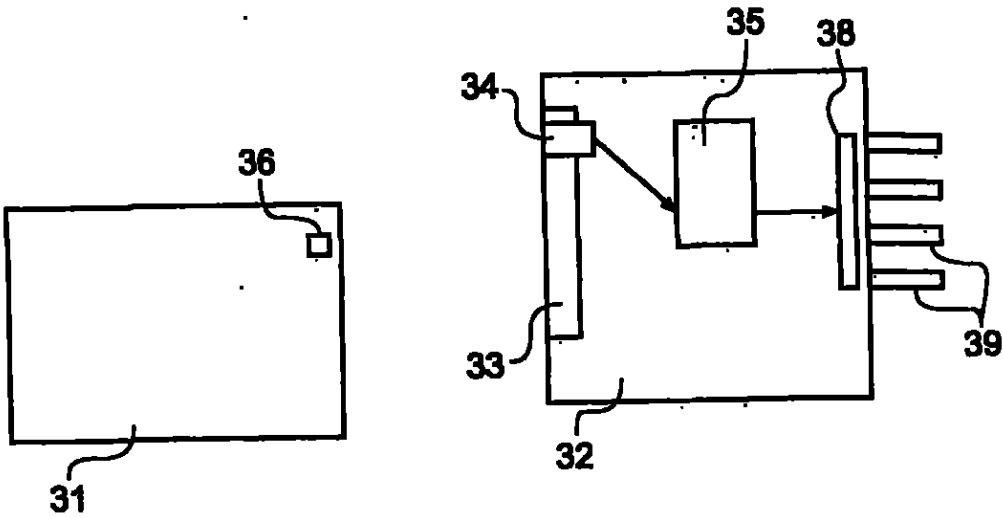


Fig. 6

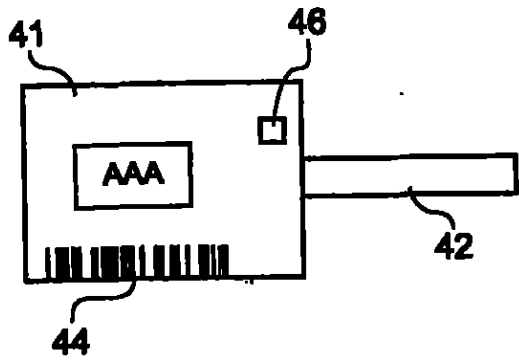


Fig. 7

7/13

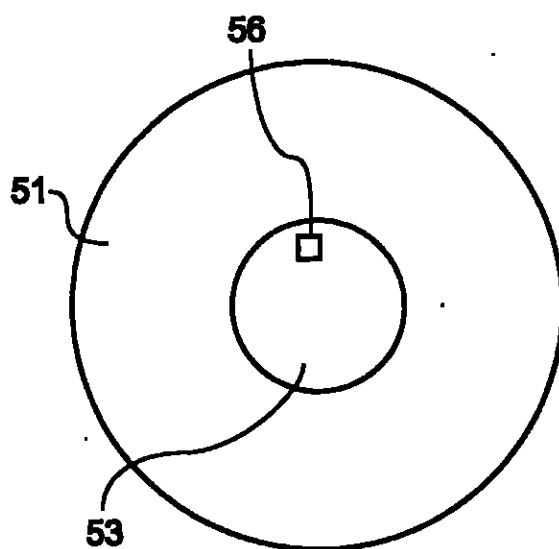


Fig. 8

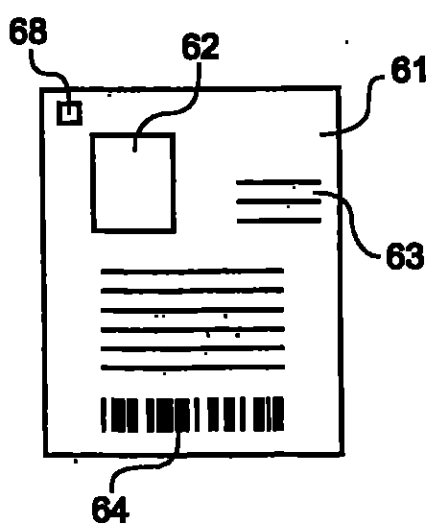


Fig. 9

8/13

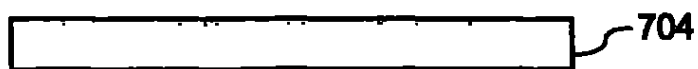


Fig. 10a

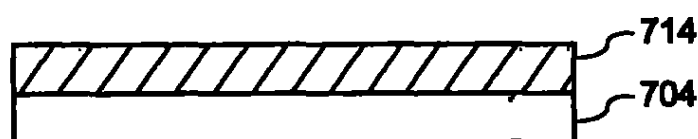


Fig. 10b

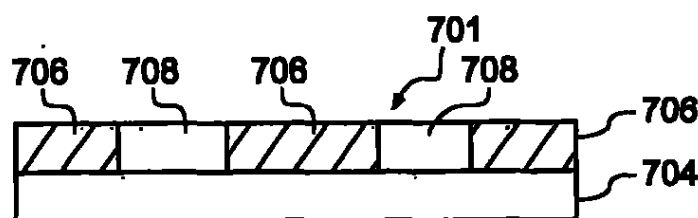


Fig. 10c

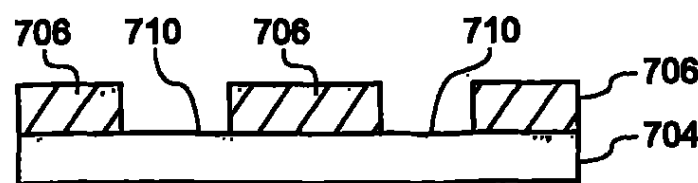


Fig. 10d

SUBSTITUTE SHEET (RULE 26)

9/13

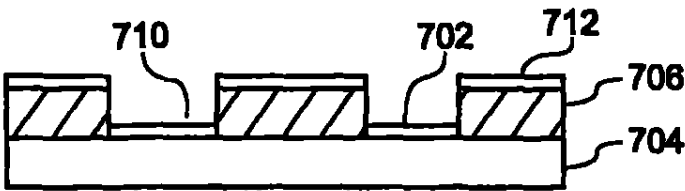


Fig. 10e

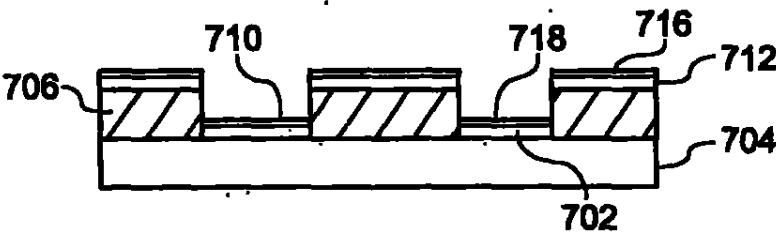


Fig. 10f

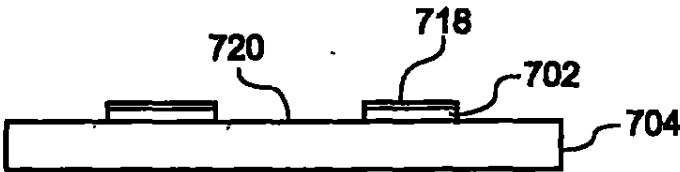


Fig. 10g

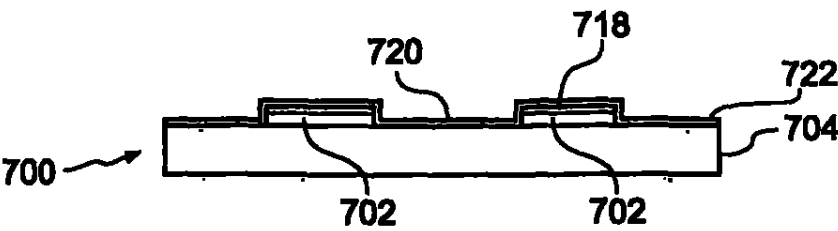


Fig. 10h

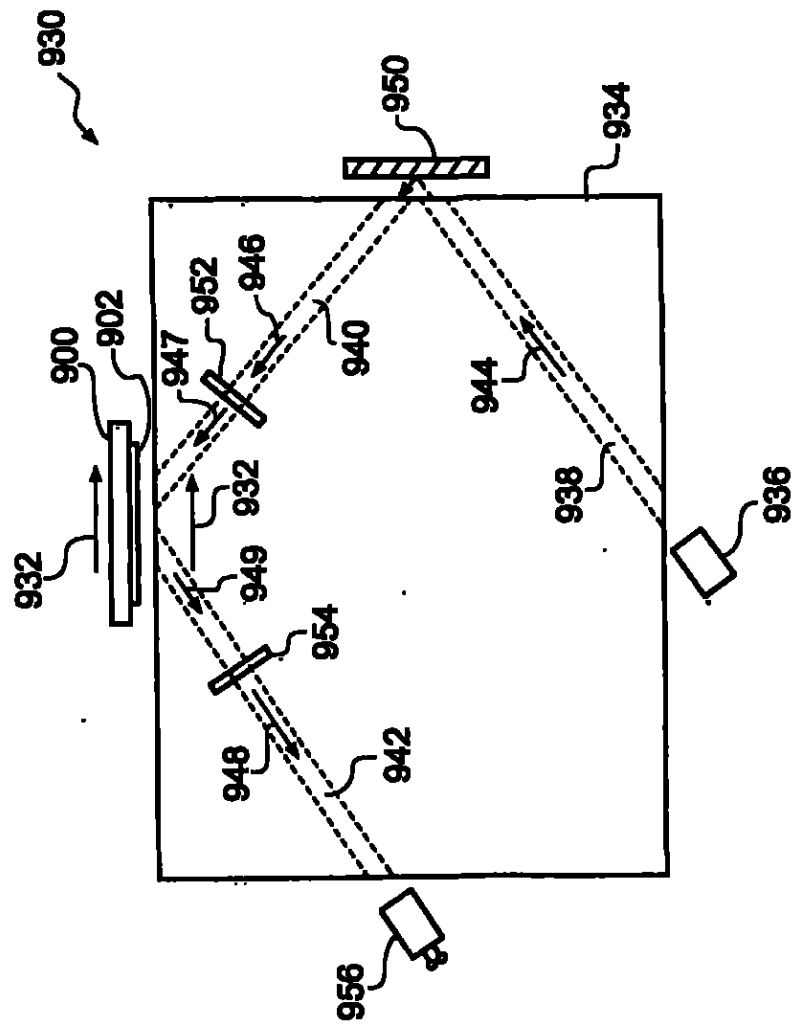


Fig. 11

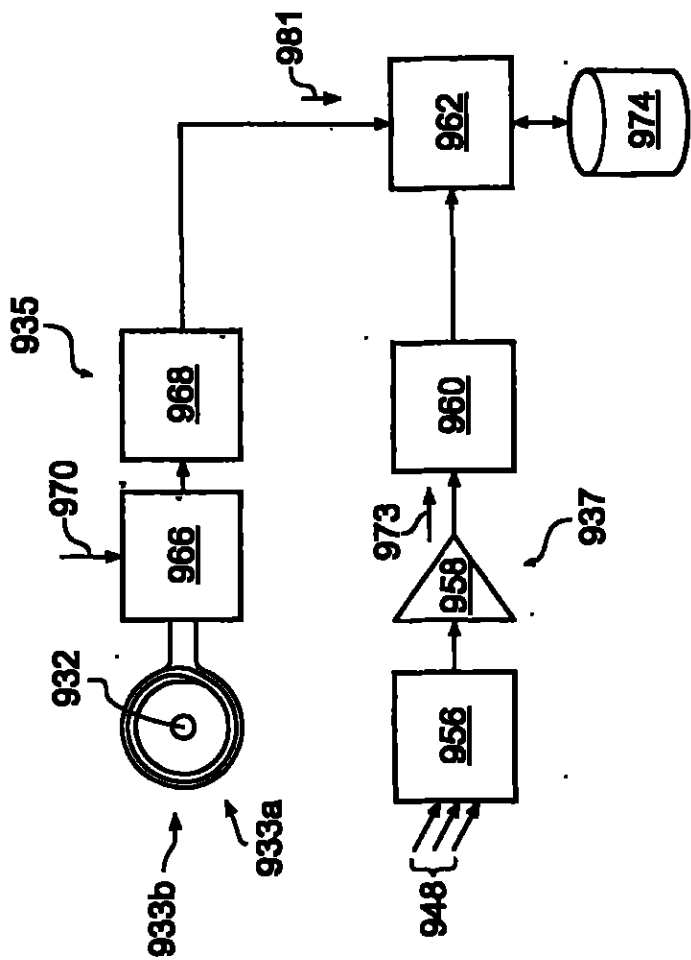


Fig. 12

12/13

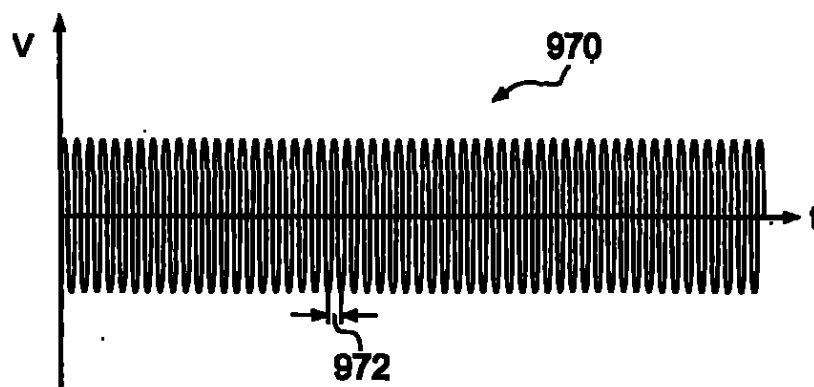


Fig. 13

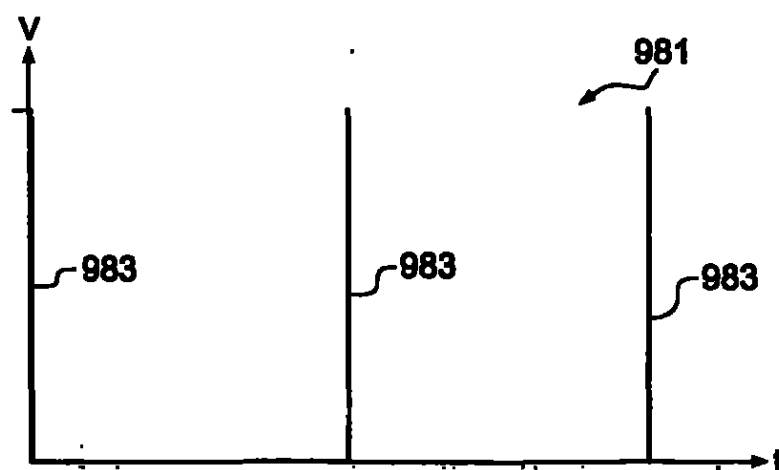


Fig. 14

13/13

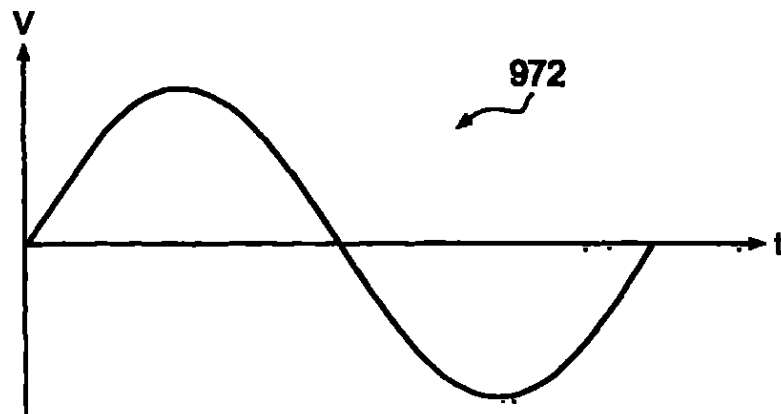


Fig. 15

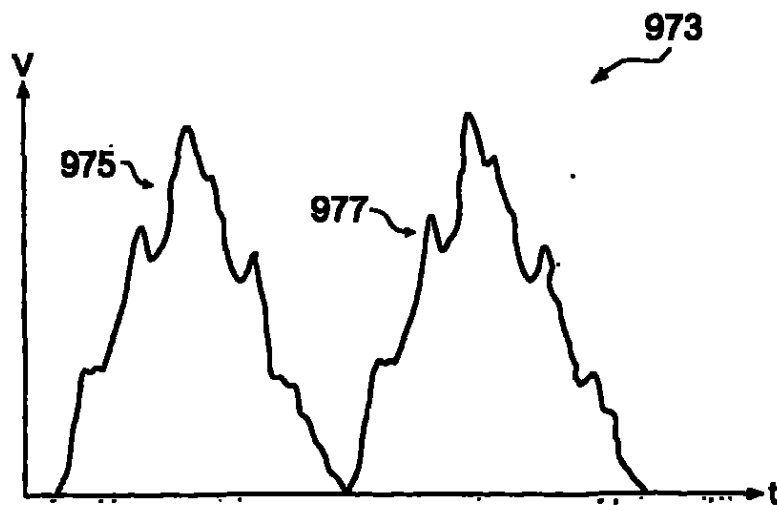


Fig. 16

DISPOSITIVO Y SISTEMA DE SEGURIDAD

Un aspecto de la invención se refiere a un dispositivo de seguridad, por ejemplo a un dispositivo que comprende una identificación y/o una autenticación para usar solo o en asociación con, incorporado dentro de o sobre, o unido a otro artículo. El dispositivo de seguridad proporciona una respuesta característica o rúbrica para la identificación y/o autenticación de una manera que limita o hace difícil la copia del dispositivo, y en consecuencia la copia o falsificación de cualquier ítem utilizado en asociación con él. Otro aspecto de la invención se refiere a un lector de datos particularmente adaptado para leer tal respuesta / rúbrica característica, un método para producir / medir tal respuesta / rúbrica característica en un sistema de seguridad que incluye el dispositivo y el lector, y/o un método de identificación o autenticación que utiliza tal dispositivo y/o sistema.

Una pérdida mayor de ingresos para algunos negocios y una fuente sustancial de la actividad criminal proviene de la falsificación ilegal o copia de ítems.

Los ejemplos incluyen, pero no se limitan a:

- Copiar tarjetas y dispositivos similares utilizados para transacciones con documentación financiera tales como tarjetas de crédito y tarjetas bancarias para permitir transacciones no autorizadas y retiros de ATMs;
- Falsificar y copiar ítems utilizados para identificación, tales como pasaportes, visas, licencias de conducción, tarjetas de identificación personal y similares;

- Copiar material que esta sobre un medio de almacenamiento de datos, tal como discos CD y DVD;
- Falsificar y copiar documentos oficiales tales como certificados;
- Duplicar tarjetas inteligentes utilizadas con propósitos de identidad / acceso, por ejemplo para controlar el acceso a áreas como parte de un sistema de seguridad, para controlar el acceso a servicios tales como TV paga, para controlar o registrar el acceso al uso de hardware tal como computadores u otros equipos de oficina en un ambiente de multi-usuario;
- Copiar etiquetas de seguridad o autenticidad como parte de la falsificación de la fabricación de bienes, para hacer copias no autorizadas o inferiores al valor más alto de calidad del sello de marca de los bienes, bienes con alta especificación crítica de seguridad y similares.

15

Este es un problema identificado particularmente en relación con las tarjetas y dispositivos similares utilizados para transacciones con documentación financiera y para propósitos de identificación, y esta área a conducido al desarrollo de sistemas de seguridad, los cuales probablemente nunca son aplicables generalmente a la mayoría o a todas las áreas en donde la copia es un problema.

20

Como la documentación comercial y sistemas de seguridad en general han llegado a ser más sofisticados, con mayor automatización unida con un incremento en la capacidad de información almacenada sobre el ítem, se han creado grandes oportunidades para el fraude financiero y de identidad mediante la copia de tales documentos. Ha aumentado la

25

concentración de la riqueza y / o la información a la que se puede acceder a través de tarjetas de crédito y bancarias y los documentos de identidad. Esto ha desarrollado una necesidad creciente en la verificación e identificación exacta de tales ítems y/o en la prevención efectiva de la copia.

En las tarjetas y los sistemas documentarios en particular se han adoptado medidas que mejoran la seguridad haciendo difícil o incomoda la falsificación . Esta aproximación se ha concentrado en particular en la incorporación de dispositivos encajados sobre o dentro de la tarjeta u otro documento, lo que hace que sean difíciles de copiar efectivamente. Los ejemplos incluyen imágenes holográficas, retículos de difracción, sustancias especiales (tintas, materiales etc), estructuras repujadas, estructuras dentro del material de la tarjeta, etc.

Aunque finalmente estas marcas pueden ser copiadas por los falsificadores sofisticados, esto ocurrirá si las recompensas son suficientes. Existe un deseo general por una marca de seguridad que prácticamente no pueda ser falsificada.

Una estrategia efectiva contra la copia no autorizada de ítems, existe si una señal al azar o respuesta característica se puede asociar con el ítem o con un dispositivo que este unido al ítem. La rúbrica / respuesta característica al azar, podría venir de algunos procesos de fabricación no controlables que nunca se puedan duplicar precisamente. Por lo tanto siempre existe alguna pequeña diferencia entre el ítem original y su copia; si esta diferencia se puede detectar y comparar con una

respuesta medida previamente (e.g., una respuesta de línea base en la cual se registran separadamente, las respuestas de elementos magnéticos individuales o se registra la repuesta promedio de una colección de tales elementos magnéticos) tomados a partir del ítem original, se puede identificar la falsificación .

Hay 4 requerimientos primarios preferidos de una rúbrica práctica al azar;

- Que sea posible medir la rúbrica fácilmente y sin costo excesivo;
- 10 • Que sea posible representar fácilmente la rúbrica de la línea base, preferiblemente mediante una pequeña lista de números dígitos;
- Que tenga un grado alto de azar inherente en la producción de la rúbrica, tal que toda rúbrica sea ligeramente diferente;
- 15 • Que no sea posible controlar la producción de la rúbrica puesto que su azar podría ser separado o suprimido y se haría una copia idéntica de una rúbrica existente.

Las dificultades para alcanzar todos estos requerimientos han limitado a la fecha la aplicabilidad práctica del concepto en una amplia escala de sistemas cotidianos.

Visto desde una primera perspectiva la invención proporciona un dispositivo de seguridad para un ítem el cual es inherentemente difícil de copiar y por lo tanto limita la falsificación.

Visto desde otra perspectiva la invención proporciona un dispositivo de seguridad para un ítem basado en una rúbrica al azar la cual es fácilmente producida y medida sobre una escala y a un costo apropiado para usar todos los días en la autenticación y la prevención de la falsificación de ítems de valor alto.

Además visto desde otra perspectiva la invención proporciona un lector de datos particularmente adaptado para leer la rúbrica de tal dispositivo.

10 Varios aspectos de la invención se describen aquí y en el conjunto de reivindicaciones anexas.

Así, de acuerdo con la invención en un primer aspecto se proporciona un dispositivo de seguridad que comprende por lo menos uno y preferiblemente una pluralidad, y más preferiblemente una gran pluralidad de elementos magnéticos ordenados sobre un sustrato adecuado y que tiene una máquina capaz de leer la respuesta de la rúbrica magnética, proporcionada en combinación con una lectura predeterminada de la rúbrica de respuesta magnética de la línea base.

20

En varias incorporaciones, los elementos magnéticos pueden comprender un material magnético en capa delgada, tal como hilos magnéticos delgados, o bandas o puntos. El material magnético puede estar en la escala micro, macro, o aun en nano-escala, y puede incluir micro-hilos o micro-puntos, o aun nano-hilos o nano-puntos, puestos en una forma adecuada sobre un sustrato adecuado para dar una marca magnética capaz de ser leída por una máquina, con una señal de

rúbrica de línea base que se puede medir, altamente dependiente de la estructura inherente precisa. La respuesta rúbrica de línea base predeterminada da una figura comparativa, una respuesta "esperada" que se puede usar en conexión con una respuesta medida para autenticar el dispositivo.

Como aquí se usa, "dispositivo" en lo mas amplio comprende el (los) elemento(s) magnético(s) según se describieron aquí anteriormente, a ser colocados sobre el sustrato adecuado, tal como, por ejemplo, la superficie de un ítem para el cual va a ser aplicado un dispositivo de seguridad. Ejemplos de la aplicación de tal dispositivo incluyen sin limitación, tal dispositivo que constituye o que comprende una parte de un objeto adaptado para uso por si mismo como una identificación, autenticación, clave o cualquier otra aplicación; un dispositivo que constituye o que comprende parte de tal objeto proporcionado para uso con un segundo objeto, en particular por ejemplo como un accesorio adicional a este, para autenticación, identificación u otro etiquetado, relacionado con la seguridad u otros propósitos; una porción del dispositivo incorporado dentro de o sobre un segundo ítem para tal identificación, autenticación o propósitos relacionados con la seguridad u otros propósitos. En particular, el dispositivo se proporciona para autenticar e impedir / prevenir la falsificación no autorizada por copiado o clonación de un artículo del cual forma parte, o con el cual esta asociado.

25

Ejemplos de colecciones adecuadas de elementos magnéticos se describen en R.P. Cowburn, Journal of Physics D, 33, R1 (2000). La

actual invención puede contar con sus efectividades singulares en la creación de una rúbrica al azar para anti-falsificación.

Los elementos magnéticos son tales que cuando se aplica a los
5 elementos un campo magnético que varía en el tiempo, sus respuestas magnéticas son una función no lineal e histerética del campo aplicado. Esta no linealidad se puede caracterizar por saltos discretos en la magnetización a ciertos valores del campo aplicado. Los elementos son tales que pequeñas diferencias en la fabricación, las cuales deben
10 existir naturalmente de un elemento a otro, causarán que la respuesta magnética varíe ligeramente de elemento a elemento. Además para varias incorporaciones, los elementos son tales que un elemento dado responde en tanto como es posible en la misma forma a cada ciclo del campo magnético que varía en el tiempo.

15

Con el propósito de determinar la respuesta rúbrica de la línea base de una colección de elementos magnéticos, se aplica un campo magnético que varía en el tiempo a los elementos y se registra la respuesta magnética de los elementos. La respuesta se puede medir utilizando el
20 dispositivo aquí descrito, o por algunos otros medios.

La respuesta de línea base se puede condensar mediante la identificación de características específicas tales como saltos súbitos , o la media y la desviación estándar de los campos de interrupción.
25 Alternativamente, la respuesta de línea base se puede convertir de una secuencia de dominio de tiempo de las medidas de magnetización a

una lista de dominio de frecuencia de las medidas. Alternativamente, la respuesta de línea base puede no procesarse.

Medir la respuesta de línea base predeterminada es análogo a un
5 procedimiento de calibración. Se anticipa que la respuesta de línea
base predeterminada se medirá solamente una vez, al momento de la
fabricación y que entonces el dispositivo será suministrado al usuario
con la respuesta de línea base predeterminada almacenada en forma
accesible para el usuario, por ejemplo remotamente del dispositivo, o en
10 asociación con el dispositivo en una forma que no sea accesible sin
autorización. En particular, es deseable que la respuesta de línea base
predeterminada este encriptada seguramente, especialmente si está
sostenida sobre o con el dispositivo. Preferiblemente, la respuesta
rúbrica de línea base predeterminada se encripta utilizando un algoritmo
15 de encriptación asimétrico con la clave privada utilizada para cifrar que se
mantiene secreta y la clave pública utilizada para descifrar que se hace
disponible para cualquier lector del dispositivo tal que la respuesta de la
rúbrica de línea base predeterminada esperada pueda ser decriptada y
se pueda hacer la comparación con una respuesta medida.

20

Con el propósito de probar la autenticidad de un ítem protegido por una
rúbrica al azar, es necesario en varias incorporaciones aplicar un campo
magnético que varía en el tiempo a los elementos magnéticos y
registrar la respuesta rúbrica magnética medida de los elementos a los
25 que se aplicó el campo. El mismo procedimiento se utiliza primero para
determinar la respuesta de línea base esperada predeterminada que
entonces se almacena como antes, y luego mediante el uso de un lector

adecuado obtener respuestas de línea base medidas subsiguientemente que se pueden comparar con la respuesta de línea base esperada predeterminada para autenticar el dispositivo.

- 5 La autenticación depende de la naturaleza al azar inherente al dispositivo. Los elementos magnéticos fabricados artificialmente hacen una muy buena rúbrica práctica al azar porque el campo de interrupción magnética de cada elemento depende críticamente de la estructura física de los terminados de los elementos. Variaciones estructurales en
- 10 el tamaño de solamente unos cuantos nanómetros pueden causar cambios significativos al campo de interrupción (K. J. Kirk, J. N. Chapman, and C. D. W. Wilkinson, J. Appl. Phys. 85, 5237 (1999)). Por lo tanto, con el propósito de replicar la rúbrica al azar, es necesario replicar la forma precisa de los elementos con precisión cercana a la
- 15 atómica. Esto es irrealizable utilizando la tecnología actual y probablemente permanezca así por muchas décadas. Mientras que se requiere manipulación a nivel cercano al atómico para copiar el dispositivo descrito en esta invención, es suficiente una medida macroscópica para chequear la autenticidad, ya que cuando la
- 20 estructura se somete a interrupción magnética, la estructura total interrumpe junta, haciendo la respuesta magnética muy fácil de medir. Por lo tanto la rúbrica al azar de acuerdo con esta invención requiere bajo costo, proceso simple para interrogarla, pero ingeniería de difícil falsificación para copiarla. Esto es ideal para una rúbrica práctica al
- 25 azar.

Si la respuesta magnética de una colección de elementos se registra junta como una medida conjunta, se debe apreciar que las fluctuaciones estáticas sobre las cuales se basa esta invención estarán atenuadas. El factor de atenuación será $1/\sqrt{N}$, en donde N es el número de elementos nominalmente idénticos en el conjunto. Así, si una colección de elementos individuales tiene un campo de interrupción con una desviación estándar de 10 Oe, entonces una colección de conjuntos de 100 elementos tendrá solamente una desviación de 1 Oe. La medida de la respuesta magnética por lo tanto deberá hacerse más cuidadosamente. De otro lado, el volumen total del material magnético se habrá incrementado por un factor N , lo cual hace que la medida se haga más fácilmente.

En varias incorporaciones, la autenticación depende de una correspondencia entre la respuesta de línea base medida del dispositivo, y una respuesta de línea base predeterminada seguramente almacenada, en particular en forma encriptada. Será extremadamente improbable que un falsificador que intente falsificar un dispositivo que incorpora una respuesta de línea base pre-registrada en forma encriptada produzca una falsificación perfecta que tenga una respuesta rúbrica magnética medible que corresponda con la original pre-registrada encriptada. En el dispositivo genuino, la respuesta de línea base predeterminada se registra en una encriptación conocida solamente por la compañía fabricante o por aquellos autorizados para esto. Si el presunto falsificador meramente intenta copiar ambos, el dispositivo de rúbrica y el derivado encripto de él, la falsificación fallará, porque aun si se copia exactamente el encripto la respuesta rúbrica magnética del

dispositivo copiado será diferente de la original. Por lo tanto, en la falsificación, no corresponderá la respuesta medida y la respuesta rúbrica registrada y predeterminada. Si el falsificador crea una copia del dispositivo de rúbrica, el podría fácilmente medir en su lugar la
5 respuesta de línea base del dispositivo copiado. Sin embargo, el no podría crear un encripto válido adecuado que corresponda a la repuesta de línea base falsificada porque el no conoce la encriptación. Por lo tanto, fallan ambas posibles estrategias de copia.

- 10 En consecuencia de acuerdo con varios aspectos de la invención, se describe un método práctico de generar y leer una rúbrica al azar utilizando materiales magnéticos estructurados artificialmente, el cual para propósitos prácticos es cercanamente imposible de copiar, y el cual ofrece así un dispositivo de seguridad que puede autenticar
15 originales y prevenir la falsificación por copiado de tales originales.

Los elementos magnéticos de varias incorporaciones comprenden capas delgadas de material magnético, preferiblemente menores de 1 μm de ancho, y más preferiblemente menores de 100 nm de ancho.

- 20 Ellos pueden ser de 10 nm o menos, pero por preferencia serán generalmente de alrededor de 40 nm de ancho.

- Todos lo elementos pueden ser nominalmente idénticos en forma y de disposición distribuida regularmente, o pueden haber sido introducidas
25 intencionalmente diferencias entre ellos y/o patrones irregulares de disposición. Se debe enfatizar que la naturaleza al azar de la respuesta magnética es una consecuencia inherente al material de fabricación, no

depende de la forma, configuración y distribución del patrón de los elementos.

Generalmente los elementos pueden estar en forma rectangular, en particular rectangular elongada, por ejemplo que comprenden un orden de elementos generalmente rectangular elongado magnético paralelo, o puede comprender áreas de material magnético, por ejemplo que son cuadradas o circulares, o algunas otras formas geométricas regulares, las cuales por ejemplo se pueden formar en un arreglo de dos dimensiones.

Como aquí se usa, la referencia hecha a hilos magnéticos, micro-hilos o nano-hilos, deberá ser entendida que es como de tales elementos de forma elongada, y en particular elementos rectangulares elongados y/o elementos elongados en un arreglo generalmente paralelo, pero no restringido a los ejemplos rectangulares paralelos aquí dados con propósitos de ilustración. Como aquí se usa, la referencia hecha a puntos magnéticos, micro-puntos y nano-puntos, debe ser entendida que es como que tales elementos comprenden áreas de material magnético de menos elongación, más en forma agazapada, y en particular de forma geométrica regular, y/o formadas en un arreglo de dos dimensiones, pero no restringidas a la geometría circular de los ejemplos que aquí se dan con propósitos de ilustración.

Los elementos pueden ser discretos, sin material magnético que los conecte, o pueden estar parcialmente conectados mediante material magnético dentro de un número de redes de trabajo, o pueden estar

completamente conectados mediante material magnético dentro de una única red de trabajo.

Los elementos pueden estar hechos de material magnético, el cual será
5 de preferencia suave magnéticamente, por ejemplo a base de níquel, hierro, cobalto y aleaciones de cada uno de ellos con el otro o con silicio, tal como la aleación níquel – hierro, la aleación cobalto – hierro, la aleación hierro – silicio o la aleación cobalto – silicio.

- 10 Los elementos pueden estar cubiertos con una sobre-capa protectora para prevenir la oxidación o el daño mecánico, dicha sobre-capa protectora comprende una capa delgada de un material no magnético que tiene propiedades adecuadas de resistencia mecánica y/o ambiental, y/o tratamientos de superficie, y/o recubrimientos, que
15 comprenden por ejemplo una capa de un material de cerámica, de vidrio o plástico. Tales sobre-capas son convenientemente transparentes. Ejemplos particulares de sobre-capas protectoras incluyen dióxido de titanio, resina epóxica transparente, plástico o vidrio, recubrimiento conformacional de resina de silicona modificada
20 transparente y recubrimiento conformacional acrílico transparente.

Los elementos se ponen sobre un sustrato adecuado. Existe una sub-capa entre los elementos y el sustrato. El dispositivo se puede incorporar directamente dentro de, o sobre el ítem que va a ser
25 protegido, en cuyo caso el sustrato puede ser el ítem que va ser protegido contra la falsificación del mismo o se pone sobre algún material sustrato adecuado o se incorpora adentro para el propósito.

Alternativamente, el dispositivo se puede incorporar dentro de una unidad separada tal como un marbete, etiqueta, certificación etc, que se puede unir a, o de otro lado se puede utilizar en conjunción con un ítem a ser protegido, la unidad que se puede unir comprende o incorpora algunos materiales sustrato adecuados. Los materiales sustrato adecuados incluyen silicio, vidrio, plástico o algún otro material con superficie lisa.

En el caso de elementos magnéticos que se forman sobre la unidad que se puede unir, la unidad que se puede unir puede estar unida directamente al ítem a ser protegido, o puede formar parte de un certificado u otra documentación asociada con el ítem a ser protegido. Se pueden proporcionar medios en asociación con una unidad que se puede unir, para efectos de la unión entre la unidad que comprende un dispositivo de identificación de acuerdo con la invención y el ítem a ser protegido. Tales medios pueden proporcionar enganches que se pueden liberar o remover de la unidad, que se puede unir al ítem protegido, o enganches permanentes sobre él. En el caso anterior, los medios pueden comprender además medios de cerradura para asegurar que solamente las personas autorizadas puedan remover la unidad. En cualquiera de los casos, los medios de unión pueden comprender además protección contra la manipulación y/o mecanismos que indican la manipulación por personas no autorizadas.

Los usos adecuados para tales unidades que se pueden unir incluyen, sin limitación, etiquetas para ítems de valor, de importancia de seguridad, o de otra importancia crítica, por ejemplo para permitir la identificación de un artículo como genuino, la verificación de la

procedencia del artículo y los similares y/o etiquetar el artículo de una manera segura y controlada, por ejemplo con información acerca de precio, información de control y almacenamiento, etc.

- 5 También se pueden contemplar usos similares en el caso de elementos magnéticos que sean formados directamente sobre un ítem a ser protegido . Sin embargo tal incorporación directa del dispositivo sobre el ítem a ser protegido será efectiva singularmente para prevenir la reproducción no autorizada, dado el azar y por lo tanto la naturaleza
- 10 inherente de reproducibilidad no controlable del dispositivo de rúbrica, y por lo tanto será particularmente útil en asociación con ítems que pueden ser susceptibles para la producción de copias falsificadas, ya que el dispositivo proporcionará la identificación rápida de un ítem como original.

15

Los elementos se pueden formar por litografía óptica, por ejemplo, utilizando el método aquí descrito, aunque se puede utilizar el repujado o alguna otra forma de impresión por contacto .

- 20 La pluralidad de elementos que constituyen el dispositivo generalmente puede ser del mismo tamaño y forma, o puede tener un tamaño y forma que difieren continuamente o discontinuamente a través del dispositivo. Preferiblemente, estará presente en un conjunto un número de tamaños diferentes del elemento.

25

En una incorporación, varios grupos discretos de elementos de tamaño y/o de forma diferente, se proporcionan a los elementos que están

generalmente de tamaño y de forma similar dentro de cada grupo, de tal manera que se pueden identificar algunas diferencias en los campos de interrupción. Por ejemplo, un conjunto de elementos rectangulares en orden paralelo puede contener algunos grupos discretos de
5 diferentes anchos.

Un ejemplo adecuado comprende 100 elementos rectangulares, cada uno de 1 mm de largo; 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
10 ancho. La respuesta magnética de tal conjunto, mostrará cuatro grupos distintos de campos de interrupción, cada uno de los cuales exhibirá una variación estática de un marbete al próximo, lo cual se puede utilizar para formar una rúbrica al azar.

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

20

En los ejemplos, el número de elementos en cada grupo es tal que cada grupo generalmente debe cubrir la misma área. La fuerza de la señal detectada a partir del lector usualmente depende del área total de cobertura, por lo que cada uno de los cuatro o cinco grupos de campos
25 de interrupción registrará la misma fuerza en el lector. Esta es una característica preferida para muchas aplicaciones, pero se puede contemplar que para otras aplicaciones varios grupos discretos de

elementos de diferente tamaño o de diferente forma se puedan proporcionar en donde diferentes grupos ocupan diferentes áreas del dispositivo.

- 5 En una incorporación alternativa, se proporcionan elementos de diferente tamaño o de diferente forma en un orden que varia continuamente, ya que las variaciones en tamaño y/o forma entre un elemento y su vecino se minimizan para evitar grandes discontinuidades. Por ejemplo el área de un elemento debe variar de la
- 10 de su vecino en no más de 5% y en particular en cerca de 1%. Como resultado se produce una colección de campos de interrupción que varia suavemente. La variación puede ser armonizada de acuerdo con la forma funcional adecuada que puede ser lineal o no lineal.
- 15 Por ejemplo en un dispositivo análogo como el descrito antes con elementos rectangulares en orden paralelo el ancho de los elementos varia como una función uniforme a través de ordenamiento. Un conjunto puede iniciar con un hilo de 2.5 μm de ancho, el próximo sería de 2.53 μm , el próximo de 2.56 μm etc, hasta que 56 hilos después el ancho ha
- 20 alcanzado 5 μm . El ancho total del hilo es de 200 μm en este ejemplo. Un conjunto alternativo puede iniciar con un hilo de 1 μm de ancho; el próximo sería 1.01 μm , el próximo de 1.02 μm , etc, hasta que 450 hilos después el ancho ha alcanzado 5 μm . Se pueden utilizar formas funcionales diferentes, e.g., lineal, cuadrática, etc, para determinar la
- 25 progresión de los anchos a través del conjunto. A diferencia del ejemplo previo, este no daría distintos grupos de campos de interrupción, sino mas bien una colección plana de campos de interrupción.

En una incorporación, el dispositivo, en adición al orden de la rúbrica que comprende una gran pluralidad de elementos rúbrica, comprende un área única relativamente grande de elemento magnético para utilizar como elemento referencia, por ejemplo un nano-hilo magnético relativamente ancho. En los ejemplos precedentes tal hilo único ancho podría ser de 1 mm de largo y 150 μm de ancho. Para un hilo de tal ancho, la propiedad magnética es casi idéntica a la del material en masa, que usualmente esta completamente definida. Así, en adición a 5 bloques los cuales tienen campos de interrupción erráticos se proporciona un campo de interrupción bien definido, que se puede utilizar para calibrar el lector. Esta calibración podría incluir el hacer ajustes basados en el ambiente, tales como sustraer la influencia del campo magnético de la tierra, por ejemplo, o compensar los cambios de temperatura.

15

Es necesario que se proporcione una respuesta rúbrica magnética de línea base predeterminada en combinación con un dispositivo de seguridad de acuerdo con varias de las incorporaciones de la invención. Sin embargo se entenderá que no es necesario, que tal respuesta rúbrica magnética de línea base predeterminada se proporcione en 20 asociación física con el dispositivo de seguridad, sino meramente que este disponible para el usuario autorizado del dispositivo para propósitos de comparación para dar una respuesta "esperada" a ser comparada con una respuesta real cuando el dispositivo se lee por 25 medios adecuados, tales como los medios aquí descritos que leen la rúbrica magnética.

Se pueden proporcionar varias incorporaciones. En una primera, la línea base pre-registrada se puede proporcionar en asociación física con el dispositivo o ítem protegido. En una segunda, la línea base pre-registrada se puede almacenar en un dispositivo lector. En una tercera, la línea base pre-registrada se puede almacenar remotamente en ambos, en el dispositivo y el dispositivo lector en una manera accesible a una persona autorizada, de tal manera que la comparación necesaria entre la lectura esperada (i.e., pre-registrada) y la real (medida) se pueda hacer para propósitos de autenticación.

10

En la primera incorporación antes mencionada, la respuesta de línea base pre-registrada se proporciona en asociación física cerrada con el dispositivo o ítem protegido. En una alternativa, la línea base pre-registrada se almacena en proximidad física al dispositivo en forma que una máquina pueda leer. Por ejemplo, la línea base pre-registrada se almacena como una parte del dispositivo; o se almacena adyacente o debajo del dispositivo sobre un sustrato común; o se almacena en la vecindad del dispositivo como parte de una unidad que incorpora el dispositivo de seguridad de la invención; opcionalmente con otras características de seguridad o información, tales como una tarjeta inteligente, un documento de identificación, una tarjeta llave, una falsa llave o similares, o una etiqueta para un artículo a ser protegido; o se almacena sobre o con un artículo a ser protegido, dicho artículo a ser protegido también a sido proporcionado con un dispositivo de acuerdo con la invención; o se almacena como parte de un certificado u otro documento asociado con un ítem a ser protegido, dicho certificado u

20

25

otra documentación también puede incorporar tal dispositivo de acuerdo con las varias incorporaciones de la invención.

En esta incorporación, la línea base pre-registrada, se debe almacenar
5 en forma que se pueda leer pero encriptada. Por ejemplo, la respuesta de línea base condensada o no procesada se señala digitalmente utilizando un algoritmo de encriptación asimétrico tal como RSA. La clave privada, que se usa para cifrar, solamente es conocida por la compañía fabricante; la clave pública que es utilizada para descifrar, está
10 contenida sobre todo terminal lector que pueda ser utilizado para leer el dispositivo.

La respuesta de línea base señalada digitalmente y encriptada se almacena sobre el ítem, preferiblemente con los elementos magnéticos
15 por ejemplo, los elementos en los que se ha impreso por debajo o a lo largo, o alternativamente registrándola sobre una banda magnética de datos, o registrándola sobre un código óptico de barras, o registrándola sobre un chip de tarjeta inteligente, o sobre otros medios. También se puede encriptar otra información, tal como, pero no limitada al nombre
20 del propietario, o un código de identidad único, o una suma de referencia, dentro de la misma corriente de datos y rúbrica digital para prevenir que los elementos magnéticos sean transferidos a otro ítem o información importante sobre un documento o certificado que sea modificado.

25

En la segunda incorporación referida antes, la respuesta de línea base pre-registrada / premedida se almacena sobre, por, o en asociación

cercana con un dispositivo lector. Tal incorporación ayuda por si misma en particular a los sistemas tipo "cerradura y llave", en donde el dispositivo actúa como una llave y se utiliza en asociación con un lector que actúa como una cerradura para limitar el acceso a áreas
5 particulares, la operación de ítems particulares o el uso de servicios particulares para el (los) contenedor (es) de la llave especificada.

En esta incorporación, no es necesario que se almacenen los datos de rúbrica de línea base pre-registrada sobre o en asociación cerrada con
10 el dispositivo en si mismo o ítem protegido. Sin embargo opcionalmente, los datos todavía se pueden almacenar en una forma encriptada para seguridad, por ejemplo de la manera descrita antes, o bien pueden ser protegidos seguramente.

15 En la tercera incorporación referida antes, los datos de rúbrica de línea base pre-registrados / premedidos se almacenan remotamente del dispositivo y del ítem protegido y del dispositivo lector. Tal modo de operación ayuda por si mismo en particular a, pero no se limita a, sistemas en donde se contempla una red de trabajo que comprende un
20 gran número de lectores cada uno esperando interrogar un gran número de dispositivos, por ejemplo como puede ser el caso con tarjetas de crédito y similares con múltiples puntos de venta, los sistemas de seguridad e identificación con múltiples puntos de acceso, etc.

25

De acuerdo con esta incorporación los datos de rúbrica pre-registrados acerca del dispositivo, y en particular acerca de una pluralidad de

dispositivos diferentes, preferiblemente se almacenan en una central de almacenamiento de datos, por ejemplo conectada a una pluralidad de lectores sobre una red de trabajo distribuida. En tal red de trabajo se pueden contemplar dos modos alternativos de operación. En el primero, 5 se adapta un lector para leer un dispositivo, interrogar a la central de almacenamiento de datos por los datos rúbrica pre-registrados, y hacer la comparación. En el segundo, el dispositivo lector se adapta para leer el dispositivo y pasar los datos de rúbrica real a tal central de almacenamiento de datos para propósitos de verificación. Los principios 10 esenciales permanecen iguales.

En otro aspecto de la invención se proporciona un sistema de seguridad que incluye por lo menos un dispositivo como el aquí descrito antes y por lo menos un dispositivo lector, dicho dispositivo lector comprende 15 medios para leer la respuesta magnética del dispositivo. En particular, el dispositivo lector comprende o se proporciona en asociación con un generador de campo magnético para aplicar a los elementos un campo magnético que varía en el tiempo, y tiene un registrador de la respuesta magnética para registrar la respuesta de los elementos magnéticos a 20 los que se les aplicó el campo magnético. Aquí se describe una incorporación de un dispositivo lector.

Para aplicaciones diferentes, los sistemas adecuados pueden comprender una pluralidad de tales lectores y/o una pluralidad de tales 25 dispositivos. Se puede arreglar un sistema que comprende una pluralidad de tales lectores, de tal forma que cada lector funcione

independientemente en aislamiento, o que algunos o todos de tales lectores estén unidos sobre una red de trabajo distribuida.

Los lectores proporcionados para un sistema operado de acuerdo con
5 el primer modo de operación reseñado antes, además preferiblemente
comprende medios para leer la respuesta rúbrica de línea base pre-
registrada predeterminada, en particular la respuesta rúbrica pre-
registrada y encriptada, almacenada sobre, con, o en asociación con un
dispositivo o un artículo protegido; y preferiblemente además
10 comprende medios comparadores para comparar las respuestas rúbrica
de línea base pre-registradas y medidas. Los lectores adaptados a un
sistema para uso de acuerdo con el segundo modo de operación
descrito antes, preferiblemente además comprenden medios de
almacenamiento para almacenar la(s) respuesta(s) rúbrica de línea
15 base predeterminada del dispositivo(s) dirigido a usar con el, y
preferiblemente además comprende medios comparadores para hacer
una comparación entre la respuesta de línea base almacenada y la
medida. Los lectores dirigidos para uso de acuerdo con el tercer modo
de operación descrito antes, preferiblemente comprenden medios para
20 recibir datos concernientes a una respuesta rúbrica de línea base
predeterminada almacenada remotamente, por ejemplo vía directa de
entrada de datos por un usuario, o vía interrogación de una base de
datos remota sobre una red de trabajo distribuida, junto con medios
comparadores para comparar la respuesta predeterminada con la
25 respuesta medida; o en una alternativa, medios para transmitir la
respuesta medida a un comparador remoto, dicho comparador

incorpora o está en comunicación de datos con un almacenamiento de respuestas predeterminadas.

En todos los casos, el dispositivo lector preferiblemente hace una
5 comparación entre las respuestas de rúbrica magnética de línea base medida y predeterminada, por ejemplo contra un límite de tolerancia predeterminado, y pone en acción un mecanismo de respuesta que depende de si las rúbricas son idénticas, por ejemplo dentro de aquellos límites de tolerancia.

10

El mecanismo de respuesta puede comprender medios sencillos de mostrar si el dispositivo se autentica, de cualquier forma adecuada, que incluyen indicadores visuales, de audio, alfanuméricos y similares. Adicionalmente o alternativamente, se pueden proporcionar otras
15 respuestas. Por ejemplo, la autenticación puede servir para liberar un seguro real o virtual, que permite el acceso a un área restringida, la operación de un ítem de equipo restringido, el acceso a un servicio particular, o similares.

20 De acuerdo con otro aspecto de la invención, se describe un dispositivo simple que puede medir la respuesta magnética de un área pequeña de un material magnético de película fina. El dispositivo se adapta bien, pero no se limita, para medir la rúbrica magnética al azar de un dispositivo tal como el descrito antes. La pequeña área será por
25 preferencia de un tamaño de 0.2 mm por 0.2 mm o mayor; el material magnético tendrá un espesor que oscila entre 1 nm y 500 nm y por preferencia estará en el intervalo entre 1 nm y 50 nm. El material

magnético puede ser una película continua o puede ser una colección de elementos magnéticos. El material magnético puede tener una sobre-capa protectora transparente. En varias incorporaciones el material magnético se mantiene reflectivo ópticamente.

5

En varias incorporaciones de acuerdo con este aspecto de la invención un dispositivo para medir la respuesta magnética de tal área de material magnético cuando se aplica un campo magnético que varía en el tiempo al material magnético, comprende una fuente de iluminación, y
10 en particular una fuente de iluminación infra-roja; un colimador para enfocar la iluminación sobre la superficie del material magnético; y un colector para coleccionar la iluminación reflejada, y un monitor de respuesta variable de esta reflexión en el tiempo cuando se aplica el campo magnético que varía en el tiempo. Opcionalmente, el dispositivo
15 incorpora o es proporcionado con un generador de campo magnético para generar tal campo.

En varias incorporaciones el efecto Kerr magneto-óptico transversal, se utiliza para medir la respuesta magnética del área del material
20 magnético cuando se aplica un campo magnético que varía en el tiempo al material magnético. Este efecto es bien conocido en la literatura. La respuesta que el dispositivo mide puede incorporar medios adicionales para aplicar tal campo magnético que varía en el tiempo al área de material magnético bajo investigación, o se puede utilizar un
25 dispositivo separado para aplicar el mismo.

En varias incorporaciones el dispositivo opera sin luz polarizada. Convencionalmente, el efecto Kerr transversal requiere que la luz que llega sea un plano polarizado. Usualmente esto se alcanza insertando una hoja de Polaroid o algún otro elemento óptico polarizante en el camino del rayo que llega. Se ha encontrado sorprendentemente que en la aplicación de esta invención, se puede quitar el polarizador para reducir el costo de fabricación y para reducir el tamaño del dispositivo. En una incorporación preferida del presente dispositivo el polarizador está ausente. Esto es adecuado para muchas aplicaciones. Nunca se entenderá que se puede incluir un polarizador, por ejemplo en el camino del rayo que llega de una manera convencional, en donde este es deseable o necesario.

Preferiblemente, el colimador comprende un agujero. Se encontró que en la escala de operación del dispositivo, este enfoca efectivamente la luz sin la necesidad de usar un lente. Esto reduce de nuevo el costo de fabricación y reduce el tamaño del dispositivo. Convenientemente, el agujero tiene un diámetro de un tamaño que oscila entre 0.2 mm y 5 mm.

20

La luz entonces se refleja desde la superficie de la película magnética delgada. Preferiblemente se proporciona un segundo agujero, con un diámetro de un tamaño que oscila entre 0.2 mm y 5 mm para enfocar la luz reflejada. Se prefiere que el segundo agujero tenga el mismo diámetro que el primer agujero. La luz se pasa a un colector que comprende un dispositivo sensible a la luz, el cual es por preferencia un

25

fototransistor o un fotodiodo sensible a la radiación producida por la fuente de luz.

En varias incorporaciones, la fuente de luz comprende un diodo que emite luz. Esto está en contraste con el arte previo en donde la gran escala de dispositivos para medir el efecto Kerr magneto-óptico usa un láser, o una lámpara de descarga o una lámpara de incandescencia. El presente dispositivo es más pequeño, más económico y elimina los riesgos asociados con un producto que contiene un láser.

10

Se prefiere el diodo que emite luz infra-roja (DEL) sobre un DEL de espectro visible por dos razones: se pueden alcanzar intensidades ópticas altas en el infra-rojo debido a las corrientes altas que se pueden sostener con DELs infra-rojos; el receptor óptico puede volverse insensible a la luz visible, reduciendo así la interferencia de la luz ambiental.

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

En otro aspecto de la invención, un método de fabricación de un dispositivo de seguridad comprende la formación de por lo menos uno, y preferiblemente una gran pluralidad de elementos magnéticos como los descritos antes; la obtención de una respuesta magnética rúbrica de línea base para los elementos; el almacenamiento de la respuesta de línea base como una respuesta de línea base predeterminada en una

forma accesible al usuario del dispositivo, opcionalmente por encriptación y almacenamiento en asociación física con el dispositivo en cualquier forma que se pueda leer.

- 5 En varias incorporaciones los elementos se formarán por litografía óptica.

En varias implementaciones de acuerdo con este aspecto de la invención se puede hacer un ahorro en el costo en el proceso de
10 litografía en el caso de los elementos magnéticos que comprenden un ordenamiento generalmente de estructuras rectangulares. La fotorresistencia se aplica al sustrato en la forma usual y se moldea por una exposición óptica seguida de desarrollo. El material magnético entonces se deposita sobre el moldeado fotorresistente. Usualmente, el
15 fotorresistente entonces, se desarrollaría en un solvente (proceso de despegue "lift off"). Sin embargo, el fotorresistente se puede dejar en el lugar, porque el material magnético depositado por encima de él forma un segundo conjunto de elementos magnéticos rectangulares. Por ejemplo, suponiendo que el resistente ha sido moldeado dentro de
20 estructuras rectangulares de 0.5 μm de ancho con un espaciamiento entre centro y centro de 1.5 μm . Si el fotorresistente se deja en el lugar, entonces las estructuras comprenden un conjunto de hilos de 0.5 μm unidos al sustrato, e igual número (menos 1) de hilos de 1 μm unidos a la parte superior del sustrato.

25

La invención en otro aspecto comprende un método de marcación de un ítem para seguridad, para propósitos de identificación o

autenticación mediante el uso del dispositivo anterior y/o el sistema y/o el método y en particular mediante asociación con un dispositivo como el descrito aquí anteriormente.

- 5 La invención en otro aspecto comprende un método de identificación o autenticación de un ítem mediante el uso del dispositivo anterior y/o el sistema y/o el método y en particular mediante asociación con un dispositivo como el descrito aquí anteriormente, la aplicación de un campo magnético que varía en el tiempo a los elementos de él para
10 obtener una respuesta rúbrica magnética de línea base medida, por ejemplo utilizando el lector descrito aquí anteriormente, y la comparación de la respuesta medida con una respuesta rúbrica magnética de línea base registrada.

- 15 La invención ahora se describirá mediante ejemplos solamente con referencia a las Figuras 1 a 16 de los dibujos acompañantes, en las cuales:

La Figura 1 es una ilustración de una primera colección de elementos
20 magnéticos utilizados para una rúbrica magnética al azar de acuerdo con la invención;

La Figura 2 es una ilustración de una segunda colección de elementos magnéticos para tal uso;

La Figura 3 es una ilustración de una tercera colección de elementos
25 magnéticos para tal uso;

La Figura 4 es una ilustración de un dispositivo para medir la respuesta magnética de un área pequeña de una película magnética tal como las rúbricas en las Figuras 1 a 3;

La Figura 5 es una ilustración de una incorporación de la invención en una tarjeta inteligente;

La Figura 6 es una ilustración de una incorporación de la invención en una llave electrónica;

La Figura 7 es una ilustración de una incorporación de la invención en un marbete de identidad para unir a un ítem a ser protegido;

La Figura 8 es una ilustración de una incorporación de la invención incorporada dentro de un CD para propósitos de autenticación;

La Figura 9 es una ilustración de una incorporación de la invención incorporada sobre un certificado para propósitos de autenticación;

La Figuras 10a a 10h ilustran una técnica de fabricación para producir varias incorporaciones de dispositivos de seguridad de acuerdo con la presente invención;

La Figura 11 muestra un arreglo de lectura de acuerdo con la presente invención;

La Figura 12 muestra un componente del arreglo de lectura de acuerdo con la presente invención;

La Figura 13 muestra una señal de conducción en espiral;

La Figura 14 muestra una señal de sincronización;

La Figura 15 muestra una señal de conducción en espiral; y

La Figura 16 muestra un detector unipolar de señal.

25

Primero en referencia a las Figuras 1 a 3, se proporcionan ilustraciones de 3 estructuras ejemplo de elementos magnéticos en vista de plano.

En la primera, se muestra una colección de elementos magnéticos rectangulares regulares (1) esquemáticamente y no a escala. El material de los elementos es $\text{Ni}_{80}\text{Fe}_{20}$. El material se pone con un espesor de 40 nm. El área sobre toda la porción de rúbrica es de 1 mm por 1 mm. La ilustración es solamente esquemática y no a escala. En particular se debe apreciar que cada área de 1 mm por 1 mm comprenderá una muy grande pluralidad de elementos con ancho de micro-escala.

10

Más aún, cualquier representación en la que los elementos sean de anchuras iguales solamente es esquemática. Para algunas aplicaciones puede ser adecuado un ordenamiento de hilos de 1 μm de ancho. Sin embargo, como se señaló antes, a menudo se preferirá cualquier ordenamiento de grupos discretos de hilos de diferente ancho que den varios campos de interrupción discretos (por ejemplo como se describió antes), o un ordenamiento que varía continuamente con el ancho que varía de manera lineal u otra manera funcional (por ejemplo como se describió antes).

20

La Figura 2 muestra una estructura similar generalmente que tiene dimensiones similares generalmente. De nuevo aplican las advertencias antes mencionadas acerca de la naturaleza esquemática de los anchos ilustrados. Sin embargo, en este ejemplo, las porciones rectangulares (2) no tienen los extremos cuadrados, sino que se proporciona con extremos en punta. Los extremos con diferentes formas pueden afectar el campo de interrupción y por lo tanto se prefieren para ciertas

25

aplicaciones. Cualquier extremo de forma adecuada se puede usar sin que se aparte de los principios de la invención.

En la Figura 3 se muestra aun otra alternativa, la porción rúbrica
5 comprende generalmente un cuadrado de 1 mm por 1 mm de micro-
puntos magnéticos circulares (3). En este ejemplo el espesor del
material es de cerca de 100 nm. Cada micro-punto es de 100 μ m de
diámetro. De nuevo esta solamente es ilustrativa. Se pueden considerar
formas alternativas, y de nuevo elementos que varían discretamente o
10 continuamente en tamaño y/o forma, proporcionado el requerimiento
básico para un dispositivo de acuerdo con la invención es decir que se
pueda obtener y reunir una respuesta rúbrica de línea base que se
pueda medir de manera reproducible.

15 La película se coloca por cualquier método adecuado, en particular por
litografía óptica tal como la que utiliza el método aquí descrito.

La Figura 4 ilustra un dibujo mecánico de un ejemplo de un dispositivo
pequeño adecuado para medir la respuesta magnética de un área
20 pequeña de una película delgada magnética, tal como una película
magnética que comprende una rúbrica magnética de acuerdo con la
invención, por ejemplo las rúbricas ilustradas en las Figuras 1 a 3.

El dispositivo que mide la respuesta magnética comprende una fuente
25 de luz de alta intensidad, en este caso un diodo que emite luz infra-roja
dentro de la cubierta (11). La luz se colima por un agujero único (12) de
diámetro que oscila en el intervalo entre 0.2 mm – 5 mm. Entonces la

luz se refleja a distancia de la superficie de la película delgada magnética colocada en la posición (15), contra ésta y pasa a través de un segundo agujero (13), que tiene un diámetro que oscila en el intervalo entre 0.2 mm –5 mm, y preferiblemente del mismo diámetro
5 que el del primer agujero.

La luz reflejada se pasa entonces dentro de un dispositivo sensible a la luz en la cubierta (14), el cual es por preferencia un fototransistor o fotodiodo sensible a la radiación infra-roja. En esta incorporación
10 ilustrada el dispositivo sensible a la luz se selecciona de tal manera que tenga una sensibilidad baja a la luz visible, lo que permite que el dispositivo se use sin pantalla óptica. El dispositivo también puede estar pintado de negro para reducir las reflexiones de luz desviada.

15 Las espirales del campo magnético (no mostradas) se unen al dispositivo para aplicar campos magnéticos en el intervalo que oscila entre 0 – 500 Oe al material magnético bajo ensayo. En el caso que el material magnético bajo ensayo comprenda un arreglo de elementos elongados, tales como rectángulos, por preferencia las espirales del
20 campo magnético se orientan para aplicar un campo en el plano de la película bien sea a lo largo del eje longitudinal de las estructuras elongadas o en un ángulo que oscila entre 0° - 60° a lo largo del eje longitudinal. Pueden estar presentes espirales de campo magnético adicionales para aplicar un campo adicional transversalmente al eje
25 longitudinal del hilo.

El fototransistor u otro dispositivo que recibe luz se conecta a electrónicos adecuados (no mostrados) que registran la intensidad reflejada a partir del material magnético mientras que se pasa una corriente alterna a través de las espirales que genera el campo magnético aplicado. Los electrónicos procesan la señal utilizando un chip Procesador de Señal Digital o un chip Microcontrolador que registran las respuestas medidas en un número de ciclos del campo magnético aplicado y las suman juntas coherentemente para reducir el ruido. El número de ciclos registrados será tal que el tiempo total de adquisición no exceda 10 segundos, y por conveniencia no excederá 5 segundos. Los electrónicos que procesan la señal entonces identifican el campo de interrupción medio para cada una de las transiciones de interrupción principales en la señal registrada. Entonces éstas se pasan a otros electrónicos (no mostrados) que adquieren y si es necesario descifran la respuesta de línea base pre-registrada a partir de la banda magnética, tarjeta inteligente, código óptico de barras, o a partir de una fuente textual remota o de un almacenamiento electrónico de datos u otros medios, o alternativamente transmite la respuesta medida a un comparador de datos remoto que tiene acceso a la respuesta de línea base pre-registrada, y se hace una comparación.

La Figura 5 ilustra la aplicación de la presente invención a una tarjeta que tiene un chip inteligente de otra forma de diseño generalmente convencional. La tarjeta (21) de tamaño y forma típicamente como el de una tarjeta de crédito o similar y que verdaderamente se puede usar como una tarjeta de crédito o similar, se ilustra en vista de plano desde arriba (A) y desde abajo (B). La tarjeta lleva alguna información

alfanumérica, pero su principal sistema de almacenamiento de información es el chip inteligente (22). Esta se apoya por un código de barras opcional (23), y una banda magnética (24) la cual típicamente se proporciona para compatibilidad retráda con sistemas de banda
5 magnética solamente.

Sobre la parte trasera de la tarjeta inteligente se aplica un dispositivo de rúbrica magnética (26) que comprende un ordenamiento de elementos magnéticos de diseño apropiado de 1 mm por 1 mm de acuerdo con la
10 invención. Por conveniencia, en el ejemplo mostrado, este se sienta dentro del pie de impresión del chip inteligente en si mismo como se ilustra por la línea interrumpida (28). Para muchas aplicaciones puede ser conveniente sentar el elemento magnético (26) dentro de este pie de impresión. Una aproximación alternativa para alcanzar el mismo
15 efecto puede ser incorporar el dispositivo de rúbrica magnética relativamente pequeño de hilos de 1 mm dentro de un espacio agrandado especialmente entre los contactos sobre el chip inteligente. Sin embargo, tal ubicación es puramente por conveniencia, y los elementos magnéticos (26) podrían ser colocados sobre cualquier otra
20 parte de la tarjeta.

Al momento de la fabricación de la tarjeta se toma una lectura inicial de la rúbrica de línea base. Una forma para hacer esto es usar un magnetómetro de exploración. En la incorporación ilustrada de una
25 tarjeta inteligente, la respuesta de línea base se almacena sobre la tarjeta, que primero tiene que ser señalada digitalmente utilizando un algoritmo de encriptación asimétrico tal como RSA. La llave pública puede

hacerse disponible para un usuario y/o ser almacenada sobre un terminal lector o aun sobre la tarjeta en si misma sin que comprometa la seguridad. La rúbrica entonces se puede utilizar para verificar que la tarjeta es un producto genuino del fabricante, y para eliminar la amenaza de abuso fraudulento de copias clonadas de la tarjeta lo cual constituye una fuente que incrementa tanto el fraude en transacciones financieras y el fraude en identidad.

En uso la tarjeta se lee por un lector de tarjeta adecuado, en particular por un lector de tarjeta que incorpora un dispositivo lector de rúbrica tal como el que se ilustra en la Figura (4). El dispositivo lector se puede incorporar dentro de un lector de tarjeta inteligente existente. Por ejemplo, con la incorporación mostrada, el dispositivo para leer el elemento magnético necesita leer el lado opuesto de la tarjeta al que se lee por el lector de tarjeta inteligente, y por lo tanto se puede incorporar dentro de un lector convencional de tarjeta inteligente con una dificultad de ingeniería relativamente pequeña. De esta manera, las tarjetas y los lectores mantienen retralidos compatibles con tecnología convencional de tarjeta/lector que no tiene el sistema de identificación y autenticación aquí descrito.

El lector mide una respuesta real a partir de la tarjeta. También se almacena sobre la tarjeta una respuesta de línea base esperada. Esta se puede almacenar en cualquier forma que se pueda leer pero se incorpora convenientemente dentro de la tarjeta en uno de los dispositivos de almacenamiento de datos existente. Por ejemplo la rúbrica de línea base se puede registrar en su forma encriptada sobre el

chip inteligente (22), el código de barras (23) o la banda magnética (24).
Por lo tanto el lector es capaz de leer tanto la rúbrica magnética real
como la predeterminada y la rúbrica magnética esperada pre-registrada.
El lector se adapta para compararlas, dentro de ciertos límites de
5 tolerancia, e indica como resultado de esa comparación si la tarjeta se
auténtica o no.

La tarjeta inteligente de acuerdo con varias incorporaciones de la
invención será aplicable en todas las circunstancias en donde este
10 siendo utilizada la tecnología convencional de tarjeta inteligente,
incluyendo sin limitación tarjetas bancarias y de crédito, tarjetas de
almacenamiento seguro de información, tarjetas de identificación y
autenticación y similares. Se proporciona un medio que autentica la
tarjeta como genuina, y por lo tanto proporciona un obstáculo
15 significativo para el abuso fraudulento de copias falsificadas de tarjetas
originales.

El sistema representado por la incorporación de la Figura (5) es un
sistema simple, en el cual un dispositivo de acuerdo con varias
20 incorporaciones de la invención sirve meramente para autenticar la
tarjeta como un producto de fabricación genuino y por lo tanto para
detectar copias falsificadas, y en consecuencia la respuesta de línea
base predeterminada se almacena convenientemente sobre la tarjeta.
Se entenderá fácilmente que tal sistema es solamente un ejemplo del
25 modo de operación. En una alternativa, la rúbrica "esperada" original se
podría almacenar en cualquier parte. Por ejemplo en relación con el uso
de una tarjeta como se ilustra en la Figura (5) como parte de un sistema

de servicios financieros, por ejemplo como una tarjeta de crédito, se puede contemplar un sistema en donde una pluralidad de tarjetas están en distribución, donde una pluralidad de lectores están en uso, y donde los lectores comprenden una red de trabajo distribuida con un
5 almacenamiento central de datos tal que ya contendrá detalles del cliente, que además está adaptada para procesar información rúbrica con propósitos de verificación de acuerdo con los principios aquí descritos. También se sugerirán fácilmente otros modos de operación en sí mismos.

10

La Figura (6) proporciona una ilustración del uso de una incorporación de la presente invención en un arreglo de cerradura y llave. La tarjeta llave (31) de un material fuerte adecuado por ejemplo de un material plástico adecuado se proporciona con un dispositivo (36) que
15 comprende un ordenamiento de elementos magnéticos de 1 mm por 1 mm como se describió previamente.

La tarjeta llave se proporciona en asociación con un arreglo lector / cerradura ilustrado esquemáticamente por el resto de la Figura (6).

20

La cerradura (32) incorpora una ranura (33) dentro de la cual se puede recibir el extremo de la tarjeta llave (31). Cuando se posiciona apropiadamente en ella, el dispositivo (36) se sienta adyacente al lector (34) del diseño general ilustrado en la Figura (4).

25

El lector (34) obtiene una lectura de la respuesta magnética a partir del dispositivo (36) de la manera pre-descrita, y pasa esta respuesta a una

unidad de control (35). La unidad de control (35) almacena o de otra manera tiene acceso a la respuesta esperada predeterminada, por ejemplo almacenando ésta con la cerradura, opcionalmente en forma encriptada. Esta efectúa la comparación y en el evento que se encuentre una pareja dentro de las tolerancias predeterminadas, pasa una instrucción a los medios de control (38) para poner en acción las palancas de la cerradura (39) y abrir la cerradura.

Aunque el ejemplo ilustrado en la Figura (6) es una cerradura electromecánica se entenderá por su puesto que los principios de la presente invención son igualmente aplicables a todas las circunstancias en donde se pueda considerar un medio físico o virtual de cerradura u otros medios de control de acceso. Por ejemplo sin limitación, se podría usar un dispositivo a lo largo de las líneas de la incorporación ilustrada en la Figura (6) en conjunción con una cerradura electrónica para una puerta u otro cierre, en conjunción con una ignición electrónica para un vehículo, en conjunción con un inmovilizador electrónico para un vehículo, como un medio para controlar el acceso a una pieza de un equipo electrónico, por ejemplo mediante el requerimiento de la inserción antes de operar el equipo, como un medio para restringir el acceso a un servicio particular, etc.

En la incorporación ilustrada se ilustra una tarjeta única en asociación con la cerradura. En la práctica aun para cerraduras simples de usuario único es probable que sea necesario proporcionar varias llaves. Está en la naturaleza de la presente invención que estas tendrán dispositivos de rúbrica inherentemente diferentes. En consecuencia, la cerradura

necesitaría almacenar y responder a rúbricas de línea base para cada uno de estos dispositivos. También se pueden contemplar modos mas complejos de operación en donde una cerradura proporciona el acceso a una pluralidad de usuarios, o en donde en realidad una pluralidad de
5 cerraduras se proporcionan en asociación con una pluralidad de usuarios.

En un primer ejemplo de tal operación, una pluralidad de cerraduras y una pluralidad de llaves se proporcionan en asociación con un sistema
10 de entrada de múltiple usuario dentro de un área segura. En un segundo ejemplo de tal modo de operación una pluralidad de tarjetas de operador se proporciona para el control de operación de equipo de oficina de múltiple usuario. En estos ejemplos todas la rúbricas de línea base autorizadas se pueden almacenar sobre cada cerradura, o
15 alternativamente las cerraduras pueden estar juntas, unidas sobre una red de trabajo distribuida a una base de datos central que almacena los detalles de las tarjetas de todos los usuarios autorizados. Tal sistema permite no solamente buena seguridad debido a la dificultad de producir tarjetas falsificadas, sino que también permite el control y el monitoreo
20 del acceso en una forma activa.

Otra incorporación de la invención se ilustra en la Figura (7). En la Figura (7) un dispositivo de rúbrica de acuerdo con la invención (46) se incorpora sobre un etiqueta que se puede unir a un ítem a ser
25 identificado / protegido. La etiqueta comprende una proyección plástica (41) la cual opcionalmente incorpora 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 ítem a ser etiquetado. La proyección (41) se une al ítem a ser etiquetado mediante la tira de unión (42). En la incorporación ilustrada la tira de unión (42) es una unión de lazo simple. La unión
5 puede ser liberable o permanente. Cuando la seguridad y la permanencia de la unión de la etiqueta son de particular importancia fácilmente se contemplaría una unión más compleja, la cual puede por ejemplo incluir mecanismos de cerradura, mecanismos de prevención de intromisión, mecanismos de indicación de intromisión y similares.

10

La incorporación de la Figura 7 permite el etiquetado de ítems bien sea de manera temporal o permanente en donde no es práctico o deseable incorporar directamente un dispositivo de acuerdo con la invención sobre el ítem en sí mismo. Ejemplos de modos de uso incluyen sin
15 limitación, etiquetas mejoradas de seguridad para equipaje en aerolíneas, etiquetas de autenticidad para ítems de alto valor de calidad, en particular prendas de vestir y similares, etiquetas de origen e identidad para los mismos, para propósitos de control de existencias, y por ejemplo para identificación original y por lo tanto controlar la
20 importación no autorizada de artículos de calidad genuina encaminados a otros mercados, marcación de ítems con propósitos de control de existencias; marcación de precio de los ítems, etiquetas que se utilizan de tal manera que hacen difícil para un comprador transferirlas a una etiqueta de precio (más bajo) a partir de otro ítem para obtener
25 ganancias con un precio bajo fraudulento.

El modo normal de operación de una etiqueta del tipo ilustrado en la Figura 7 será de autenticación. En consecuencia, la información de la rúbrica pre-registrada usualmente estará sobre la proyección (41). La información pre-registrada se almacenará en cualquier forma adecuada
5 capaz de ser leída por una máquina. En el ejemplo dado estaría en el código de barras. Se proporcionará un lector adaptado para leer tanto la rúbrica magnética del dispositivo (46), como la rúbrica esperada encriptada, y efectuar una comparación para autenticar la etiqueta. La efectividad de la seguridad de la etiqueta radica en que es muy difícil de
10 copiar, puesto que la naturaleza al azar de la rúbrica significa que una etiqueta copiada será identificable inmediatamente como tal.

La Figura 8 ilustra un disco de almacenamiento de datos tal como un CD, DVD o los similares, en los que ha sido aplicado un dispositivo de
15 acuerdo con la invención. El disco (51) incorpora una proyección de rúbrica magnética (56) que comprende elementos magnéticos como los descritos antes, preferiblemente en el área muerta (53) que no lleva otros datos. Sobre cualquier otra parte del disco se proporciona una lectura predeterminada encriptada de la rúbrica (56).

20

En lo más simple, en un primer modo de operación, el sistema permite al fabricante autenticar los CDs / DVDs originales, para identificar copias falsificadas, y en asociación con un sistema adecuado de control de existencias rastrear el origen y destino de los originales genuinos, e
25 identificar la importación no autorizada y similares.

En un modo de operación mas avanzado, se pueden fabricar los lectores de disco tal que incorporen dispositivos lectores para leer el dispositivo (56) y autenticar el disco y los cuales estarán inhabilitados para que lean copias no autorizadas. También es posible contemplar un sistema con el cual tales lectores modificados se pueden utilizar en conjunción con el sistema de identificación / autenticación de la invención como parte de un arreglo de licencia para el usuario final.

La Figura 9 es un ejemplo del uso de la invención sobre un documento de identificación formal. Tal documento puede ser un documento de identificación o autenticación, tal como un pasaporte, una licencia para conducir, un certificado de autorización o calificación, o similares, una identidad, autorización o certificación encaminada a acompañar, verificar o identificar de otra manera un artículo, o cualquier otro documento en donde las copias falsificadas pueden ser un problema.

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

Un dispositivo que comprende elementos magnéticos como el anterior (66) se incorpora en el documento. Este dispositivo se puede leer de la manera descrita antes. En un modo de operación, el dispositivo (66) sirve con un propósito de simple autenticación, y una lectura encriptada pre-registrada de su respuesta magnética esperada también se incorpora en el documento. Convenientemente en el ejemplo dado esta

podría ser incorporada en el código de barras, o almacenada de otra manera en una forma que se pueda leer. Sin embargo se apreciará que en sistemas más sofisticados sería posible almacenar remotamente la rúbrica magnética esperada, opcionalmente con otra identificación y/o

5 otros detalles de seguridad.

El dispositivo de acuerdo con la invención aplicado de esta manera a la documentación, sirve primariamente como una forma de protección de copia. Por lo tanto este sirve como un dispositivo de autenticación

10 económico y conveniente en todas las circunstancias en donde hay una vulnerabilidad elevada de fraude a partir de la falsificación de originales genuinos, por ejemplo en relación con documentos de identificación, certificados formales, documentos financieros tales como cheques, papel moneda y similares, documentos de importancia legal, y otros de

15 tal documentación.

Se pueden proporcionar varias incorporaciones de un dispositivo de seguridad que incorpora elementos magnéticos . Ahora se describirá, a manera de ejemplo, un proceso de fabricación de varios de tales

20 dispositivos de seguridad sobre un sustrato de silicona utilizando litografía óptica.

El proceso de fabricación se ilustra en las Figuras 10a a 10h. El proceso inicia en la Figura 10a con un limpiado y pulido de un sello de silicona

25 704. En varias incorporaciones, el sustrato de silicona es de aproximadamente 0.5 mm de espesor con el objeto de facilitar la manipulación y proporcionar un dispositivo de seguridad áspero. Sobre

el sello se torne a una capa fotorresistente 714 para proporcionar un recubrimiento suave como se muestra en la Figura 9b. El sello y la capa fotorresistente 714 entonces se hornean para formar la capa fotorresistente 714.

5

La Figura 10c ilustra el dispositivo de la Figura 10b post-expuesto a radiación UV o radiación cercana a la UV (e.g., a 405 nm). Las regiones 708 representan regiones expuestas. Las regiones expuestas 708 se escriben directamente sobre la superficie superior 701 de la capa fotorresistente 714 utilizando un sistema de litografía óptica de escritura directa por tamizado, tal como por ejemplo, un sistema NanoMOKE2 con un Escritor Láser sobre adición, suministrado por Durham Magneto Optics Ltd. De este modo se puede escribir un patrón unidimensional o bidimensional en la capa fotorresistente 714 para cada dispositivo de seguridad que se fabrique. Este patrón puede definir una pluralidad de formas de alambre, tales como, por ejemplo, aquellos ilustrados en la Figura 1.

La Figura 10d muestra el dispositivo de la Figura 10c después que ha sido desarrollada la remoción de la fotorresistente expuesta 708. La remoción de la fotorresistente expuesta 708, expone las porciones 710 del sustrato de silicona subyacente 704.

Subsiguientemente, como se muestra en la Figura 10e, los elementos magnéticos 702 formados de un material de permalloy, tal como, por ejemplo, $\text{Ni}_{80}\text{Fe}_{20}$ (ver, por ejemplo, Bozorth, Ferromagnetism, ISBN 0-7803-1032-2, para más información) se deposita en las porciones

expuestas 710 mediante un proceso de deposición por salpicadura o evaporación, típicamente con un espesor en el intervalo que oscila entre cerca de 10 a cerca de 100 nm, e.g., cerca de 40 nm. También se forman otras capas 712 de material de permalloy sobre la
5 fotorresistente 706 no expuesta restante durante el proceso de deposición por salpicadura.

Posteriormente, se forma el metal que corona las capas 716 y 718 de oro o aluminio sobre las capas de permalloy 712 y los elementos
10 magnéticos 702, como se ilustra en la Figura 10f. La capa de corona 718 se diseña para proteger la capa de permalloy de la oxidación y también proporciona una reflectividad óptica mejorada.

Utilizando un solvente adecuado, e.g., acetona se remueven las capas
15 fotorresistentes no expuestas 706 a lo largo de las capas subyacentes de permalloy 712 y las capas de corona 716, para dejar la estructura ilustrada en la Figura 10g. La estructura resultante comprende los elementos magnéticos 702 formados sobre el sustrato de silicona 704 separado por las regiones sustrato de silicona expuestas 720. Las
20 superficies superiores de los elementos magnéticos 702 se coronan por capas de corona 718.

La estructura resultante antes mencionada se coloca dentro de una cámara de deposición de vapor químico de plasma mejorado (PECVD)
25 en donde se deposita una capa de dióxido de silicio (SiO_2) 722 sobre la superficie superior expuesta de las regiones sustrato de silicona 720 y las capas de corona 718. La capa de dióxido de silicio 722 forma una

capa transparente ópticamente (que incluye, *Inter-alia*, una capa que es sustancialmente transparente a la radiación electromagnética infra-roja).

El dispositivo de seguridad resultante 700 se muestra en la Figura 10h.

Se fabrican varios dispositivos de seguridad 700 sobre un sustrato
5 único de silicona 704, el sustrato de silicona 704 subsiguientemente se puede pasar dentro de una pluralidad de dispositivos de seguridad individuales 700.

Los solicitantes han producido varios dispositivos de seguridad prototipo
10 utilizando el proceso de fabricación aquí descrito antes. Durante la producción de estos dispositivos de seguridad prototipo, los parámetros utilizados en el proceso de deposición por salpicadura fueron como sigue: montaje de potencia de 250 W; presión base 5×10^{-7} mbar; gas Argón; presión del gas 1 a 2 mTorr; flujo de 5 cc/minuto; tasa de
15 rotación del sustrato 10 rpm; tasa de deposición 1 a 1.5 Angstroms por segundo; y una temperatura de sustrato de 22 a 27°C. También es posible aplicar un campo magnético a lo largo del plano del dispositivo durante el proceso de fabricación.

20 Los solicitantes señalan a partir de un análisis de sus dispositivos de seguridad prototipo, que un ajuste fino de la tasa de crecimiento y/o la presión de salpicadura para los elementos magnéticos puede proporcionar mejoras en las características de interrupción magnética del modo de interrupción de la forma. Los solicitantes también han
25 señalado que a partir de un análisis de sus dispositivos de seguridad prototipo, los materiales suaves magnéticamente tienden a dar origen a propiedades de interrupción magnética deseables .

Una vez ha sido fabricado un dispositivo de seguridad este se prueba, bien sea sólo o como parte de un lote de tales dispositivos de seguridad, para determinar su respuesta característica. La respuesta
5 característica se mide para asegurar que esta proporcione la identificación adecuada del dispositivo de seguridad particular.

Cuando las incorporaciones de la invención usan las propiedades de interrupción magnética del material para producir una rúbrica, línea
10 base o respuesta característica, son útiles materiales suaves magnéticamente. Los materiales suaves magnéticamente son materiales ferromagnéticos en los cuales el magnetismo puede ser invertido fácilmente. Estos materiales generalmente tienen lazos ("loops") de histéresis de forma cercana al cuadrado. Por lo tanto, la
15 magnetización de un elemento magnético hecho de tal material interrumpe su dirección en respuesta a un campo aplicado relativamente agudo. La coercitividad de tales materiales (i.e., el campo inverso necesitado para llevar la magnetización de un elemento magnético hecho de tal material a cero después que esta saturado)
20 tiende a ser relativamente baja, asegurando por lo tanto que magnetos de fuerza de campo relativamente baja se puedan utilizar para producir un interruptor en la dirección de magnetización del elemento magnético. Tales magnetos de fuerza de campo relativamente baja pueden ser totalmente económicos, generalmente compactos y fácilmente
25 manejados para producir un campo magnético controlado de buena uniformidad.

Se puede usar una medida de la fluctuación para proporcionar un parámetro relacionado con una rúbrica, línea base o respuesta característica, una medida de la fluctuación se puede hacer por repetición de medidas sobre los elementos magnéticos y determinando
5 cuanto varía la coercitividad entre conjuntos de medidas. Estos conjuntos de medidas se pueden repetir varias veces para los elementos magnéticos del dispositivo de seguridad. En un ejemplo, la coercitividad se puede medir cien veces para los elementos magnéticos a temperatura ambiente. Los valores de coercitividad medidos entonces
10 se ajustan a una curva de campana Gaussiana, y se calculan la coercitividad media y la fluctuación (indicadas por la media y la desviación estándar Δ de la curva Gaussiana ajustada, respectivamente).

15 Los elementos magnéticos pueden ser probados para determinar si ellos operan o no de una manera reproducible. Para medir la coercitividad de los elementos magnéticos se usa un magnetómetro Kerr, como se describe en Applied Physics Letters, Vol. 73, p 3947, 1998.

20

Los solicitantes han encontrado que para varias incorporaciones, sobre una temperatura de operación probablemente típica (por ejemplo, de -20°C a 50°C cuando se proporcionan medidas anti-niebla en un lector), la fluctuación exhibe solamente una débil dependencia de la
25 temperatura.

En varias incorporaciones, hay una dependencia que se puede medir de la coercitividad media con la temperatura. Sin embargo, a menos que la coercitividad media de una pluralidad de elementos magnéticos varié en la misma forma con la temperatura, las diferencias de coercitividad entre los elementos magnéticos permanece casi constante. Así, cuando se compara la coercitividad media medida contra la respuesta característica premedida, se puede hacer una tolerancia para una compensación constante entre los dos conjuntos para compensar por temperaturas diferentes.

10

Sin embargo, si se desea o se requiere para otras varias incorporaciones, las medidas de coercitividad y fluctuación se pueden hacer a varias temperaturas, que incluyen temperaturas fuera del intervalo normal de temperaturas de operación. Por ejemplo, se pueden hacer conjuntos de medidas sobre elemento magnético a -50°C , 0°C y 65°C para un dispositivo de seguridad tasado para operación desde cerca de -20°C a cerca de 50°C .

En varias incorporaciones, los dispositivos de seguridad pueden tener sus líneas base o respuesta característica premedida definida por el valor de coercitividad media y/o el valor de fluctuación Δ determinados como se indicó antes. Otras varias incorporaciones usan, por ejemplo, su valor de coercitividad media o su valor de fluctuación para representar una línea base o respuesta característica premedida. En uso, la línea base o 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 línea base o respuesta característica premedida puede estar
5 codificada, por ejemplo, mediante la digitalización de los valores de la
coercitividad media y/o el valor de fluctuación Δ . En varias
incorporaciones, estos valores se almacenan en forma encriptada sobre
el dispositivo de seguridad correspondiente, bien sea con o sin un
identificador que puede ser único. En otras varias incorporaciones,
10 estos valores se almacenan separadamente del dispositivo de
seguridad. En varias incorporaciones, durante una operación de lectura
(como la aquí descrita), los valores digitalizados de la coercitividad
media y/o valor Δ de fluctuación que representan una línea base o
respuesta característica premedida se pueden recuperar / recobrar para
15 un dispositivo de seguridad particular y comparar con los valores
medidos de coercitividad media y/o valor Δ de fluctuación para un
dispositivo de seguridad que da a entender que es el mismo dispositivo,
por lo tanto para determinar si el dispositivo de seguridad para el que
se ha medido la rúbrica o respuesta característica es o no una
20 falsificación.

Los dispositivos de seguridad pueden estar unidos a artículos con el
objetivo de ayudar en la identificación de esos artículos como genuinos
o no fraudulentos. En uso es necesario leer la rúbrica o respuesta
25 característica de un dispositivo de seguridad particular con el propósito
que ésta se pueda comparar con la línea base o respuesta
característica premedida. Cualquier diferencia entre las respuestas

medida y premedida, fuera de cualquier límite permisible, indica que ese dispositivo que ha sido leído es una falsificación. Puesto que la producción de centros de nucleación magnética esta más allá del control del fabricante, cualquier copia del dispositivo resultará casi
5 invariablemente en una respuesta característica diferente, tal como, por ejemplo, los valores de coercitividad media y fluctuación.

Se contemplan varias incorporaciones de sistemas para lectura de dispositivos de seguridad manuales o de otra forma. Varias de tales incorporaciones se describen aquí en conexión con las Figuras 11 a 16
10 de los dibujos.

La Figura 11 muestra un arreglo de lectura 930, que forma un componente de un sistema de lectura de un dispositivo de seguridad para obtener una respuesta característica medida de un dispositivo de
15 seguridad 900 mientras que el dispositivo de seguridad 900 esta sometido a un campo magnético aplicado 932. El arreglo de lectura 930 puede detectar cambios en la polarización y/o intensidad de la luz reflejada desde los elementos magnéticos utilizando el efecto magneto-óptico Kerr (MOKE).

20

El arreglo de lectura 930 comprende un bloque de aluminio 934 cuyas superficies interna y externa se ennegrecen utilizando una pintura negro mate anti-reflexión. El tamaño del bloque de aluminio 934 es típicamente de 2 cm x 2 cm x 1 cm. El bloque de aluminio 934
25 comprende canales de paso del rayo 938, 940, 942. Un diodo láser 936 del infra-rojo cercano o visible, que se proporciona con ópticos de colimación (no mostrados), se puede operar para producir un rayo láser

colimado 944 a una longitud de onda de, por ejemplo, 600 a 1550 nm. Una incorporación usa un diodo láser que opera a 670 nm. El rayo láser 944 pasa a través de un primer canal de paso del rayo 938, antes de dejar el bloque de aluminio 934 e incide sobre un espejo 950.

5

El rayo láser 944 se refleja desde el espejo 950 en un segundo canal de paso del rayo 940 formado en el bloque de aluminio 934. Un polarizador 952 colocado en el segundo canal del paso del rayo 940 convierte el rayo láser 944 en un plano de rayo láser polarizado 947. El plano de rayo láser polarizado 947 entonces deja el segundo canal de paso del rayo 940.

10

El bloque de aluminio 934 también comprende un tercer canal de paso del rayo 942. El tercer canal de paso 942 se orienta para coleccionar la luz reflejada 949 que se refleja desde un dispositivo de seguridad 900 cuando está siendo leído. Típicamente, si un dispositivo de seguridad 900 tiene elementos magnéticos en forma de hilo o en forma de hilos aplanados 902, el campo aplicado 932 se aplica en una dirección sustancialmente paralela al eje de los elementos magnéticos 902.

15

20

Un analizador 954, usado en varias incorporaciones, incorpora una placa opcional de cuarto de onda y se coloca en el tercer canal de paso del rayo 942 un polarizador. El analizador 954 pasa la luz de una primera polaridad y los bloques de luz de una segunda polaridad ortogonal. La luz de la primera polaridad se refleja desde los elementos magnéticos 902 y dan origen a una señal agregada que mide el estado de polarización media / reflectividad (algunas veces conocida como

25

respuesta agregada) de los elementos magnéticos iluminados por el rayo 947.

El polarizador 952 y el analizador 954 se arreglan para medir la señal longitudinal del efecto magneto-óptico Kerr producida cuando el plano del rayo láser polarizado 947 incide sobre los elementos magnéticos 902. También se pueden utilizar otros arreglos del efecto magneto-óptico Kerr, por ejemplo, que incluyen arreglos sin un polarizador y/o un analizador y/o que utilizan un arreglo transversal o polar. Sin embargo, un beneficio de utilizar un arreglo longitudinal magneto-óptico Kerr es que éste generalmente proporciona una señal mejorada cuando se compara con los arreglos transversal o polar.

Alineada con el tercer canal de paso del rayo 942 está una unidad detectora 956, la cual en esta incorporación incorpora un lente de enfoque y un circuito de fotodiodo o un circuito de foto transistor sensibles a la radiación que los ilumina. El circuito de fotodiodo responde a la luz transmitida a través del analizador 954 para dar una señal proporcional a la magnetización de cualquiera de los elementos magnéticos 902 iluminados por el plano del rayo láser polarizado 947.

La Figura 12 muestra un sistema de generación de campo 935, un sistema de detección 937, y un sistema de control y procesamiento 939 que forman, en conjunción con el arreglo de lectura 930 antes descrito, otra parte de una incorporación de un sistema de lectura de un dispositivo de seguridad.

El sistema de generación de campo 935 comprende componentes para producir un campo magnético aplicado que varía en el tiempo 932 para aplicar a un dispositivo de seguridad 900. El sistema de generación de campo 935 comprende un circuito conductor 966 que opera para

5 conducir las espirales de generación de campo 933a, 933b, en respuesta a una señal que conduce la espiral 970. La señal que conduce la espiral 970 es una señal sinusoidal periódica compuesta de una pluralidad de formas de ondas sinusoidales individuales 972 que oscilan en una frecuencia de 100 Hz (ver Figuras 13 y 15), que

10 conducen las espirales de generación de campo 933a, 933b para producir un campo magnético que oscila sinusoidalmente a 100 Hz. En esta incorporación la forma de onda sinusoidal de 100 Hz se produce por un circuito oscilador electrónico convencional (no mostrado).

15 El sistema de generación de campo 935 adicionalmente comprende un detector que pasa de un lado a otro 968 para detectar los cambios de polaridad en la señal que conduce la espiral 970. El detector que pasa de un lado a otro 968 produce una señal de sincronización 981 en respuesta a que es conducida por el circuito conductor 966, como se

20 muestra en la Figura 14. La señal de sincronización 981 se compone de una secuencia de espigas 983 cada una producida en el momento que cambia la polaridad de la señal que conduce la espiral 970. En otras varias incorporaciones, el mismo microcontrolador que registra el acceso de la señal Kerr se utiliza para generar la secuencia del campo

25 aplicado (vía un convertidor Digital a Análogo), por lo tanto el microcontrolador puede controlar la sincronización 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 se une a un amplificador 958. Las señales producidas por la unidad detectora 956 son amplificadas por el amplificador 958 para dar una señal unipolar del detector 973 (ver Figura 16). La señal unipolar del detector 973 se alimenta entonces en un convertidor análogo a digital (ADC) 960 para digitalización. El ADC 960 es un dispositivo de 10 bit que opera en una frecuencia de muestreo de 10 kHz; por lo cual da 1024 niveles posibles de datos discretos para cada una de las 100 muestras tomadas en el tiempo tomado para un ciclo de 100 Hz de ciclo completo.

En una incorporación, el ADC 960 opera a 10 kHz y adquiere alrededor de 100 puntos de datos por ciclo de campo magnético aplicado. El campo aplicado se adapta a una frecuencia de alrededor de 10 kHz / 100 = 100 Hz. Los datos se promedian alrededor de 0.5 segundos, i.e., hay 50 conjuntos de datos promediados para un elemento magnético único. A partir de esta se miden la coercitividad media y la fluctuación. Entonces el proceso se repite para otro elemento magnético. En total alrededor de 8 elementos magnéticos se analizan de esta manera.

El sistema de control y procesamiento 939 se usa para adquirir datos medidos representativos de la respuesta rubrica / característica del dispositivo de seguridad 900 a partir del sistema de detección 937, analiza el dato medido y lo compara con una respuesta característica premedida para determinar si el dispositivo de seguridad es genuino.

El sistema de control y procesamiento 939 comprende una unidad de procesamiento 962 que tiene un almacenamiento de datos asociado 974. En varias incorporaciones, la unidad de procesamiento 962 comprende un microprocesador o un microcontrolador y memoria asociada (no se muestra), que incluye un amortiguador de anillo al que se alimentan constantemente muestras de datos desde el ADC 960, cuando el amortiguador de anillo es habilitado por el microprocesador.

Cuando se inicia el sistema de lectura del dispositivo de seguridad, el amortiguador de anillo está inhabilitado por el microprocesador. Con el propósito de comenzar la acumulación de datos dentro del amortiguador de anillo una primera espiga 983 es recibida por el microprocesador. Esto dispara el microprocesador para empezar un conteo del número de espigas de sincronización 983 que son recibidas y simultáneamente habilita el amortiguador de anillo. Por lo tanto, los datos comienzan a acumularse dentro del amortiguador de anillo en sincronización con una transición de polaridad que ocurre en el campo magnético aplicado 932. Cuando el microprocesador detecta la espiga N^a 983 (e.g., la 100^a), una señal se envía para inhibir otra acumulación de datos en el amortiguador de anillo. El amortiguador de anillo en éste momento contendrá N conjuntos de datos cada uno acumulado durante medio ciclo del campo magnético aplicado 972, con cada conjunto de datos representando una porción respectiva digitalizada 975, 977 de la señal unipolar del detector 973 en un momento respectivo durante el tiempo de duración t ($t = N \times \text{frecuencia del campo magnético aplicado} / 2$) de la acumulación de datos, (e.g., t = 0.5 segundos de duración para

100 ciclos a 100 Hz con $N = 100$, y 5000 medidas individuales hechas con un ADC de conjunto de tasa a 10 kHz).

Como se indicó antes, los conjuntos de datos se pueden acumular en una variedad de formas. Una vez adquiridos, los datos se pueden procesar para extraer una variedad de información relativa a la rúbrica medida o respuesta de señal característica. Se pueden aplicar algoritmos estándar a los conjuntos de datos para calcular la coercitividad media medida y/o la fluctuación como dadas por una medida de la desviación estándar de medidas de coercitividad. Ejemplos de tales algoritmos se pueden encontrar, por ejemplo, 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).

15

El ajuste de datos puede ser hecho bien sea por el mismo microprocesador / microcontrolador que determina la respuesta señal característica medida, o por un sistema de computador conectado. Por ejemplo, cuando una base de datos remota almacena la respuesta característica premedida, los datos de respuesta de señal característica medido originalmente se pueden transmitir a un procesador remoto para realizar el ajuste Gaussiano. Similarmente, cuando se usa como parte de un sistema de detección de fraude, un lector puede estar conectado a un computador manual "Palm-top" que almacena los datos de la respuesta característica premedidos descargándolos de la Internet, y comparándolos con la respuesta señal característica medida. En varias incorporaciones, los computadores "Palm-top" se pueden utilizar como

un despliegue interactivo del lector y también como un medio de acceso a bases de datos remotas, e.g., mediante la utilización de teléfonos GSM.

- 5 Existen varias formas para determinar la línea base o respuesta característica premedida de un dispositivo de seguridad. Estas formas varían de acuerdo con el tipo de dispositivo de seguridad y dependen de, por ejemplo, si la respuesta característica premedida está o no almacenada / codificada sobre el dispositivo de seguridad; de si la línea
- 10 base / respuesta característica premedida esta o no encriptada; y de si se proporciona o no un identificador único en asociación con el dispositivo de seguridad. Todas estas posibilidades proporcionan incorporaciones realizables.
- 15 En otras varias incorporaciones, una tarjeta inteligente lleva un dispositivo de seguridad y un identificador único y se almacena en la tarjeta inteligente la línea base encriptada o la información de la respuesta característica premedida. La tarjeta inteligente se lee de una manera convencional y la rúbrica medida o respuesta característica se
- 20 mide como se describió aquí.

En una incorporación de un sistema de lectura de un dispositivo de seguridad, la información de la respuesta característica premedida se almacena en una base de datos, para que una o más unidades de

25 procesamiento tengan acceso. Preferiblemente, la línea base o la información de la respuesta característica premedida esta encriptada. Tal sistema puede estar distribuido y comprende un servidor remoto

unido a través de una red de trabajo a uno o más lectores del dispositivo de seguridad. Un sistema de acuerdo con esta incorporación se puede operar para determinar un identificador único para cada dispositivo de seguridad y recuperar la línea base o la información de la
5 respuesta característica premedida correspondiente al identificador único determinado para el sistema de lectura del dispositivo de seguridad. La línea base o la información de la respuesta característica premedida entonces puede ser decriptada cuando sea necesario para un lector del dispositivo de seguridad respectivo.

10

En incorporaciones del sistema de lectura del dispositivo de seguridad, una vez ha sido extraída la información relativa a la rúbrica medida o respuesta señal característica, esta es comparada por el microprocesador con la línea base o respuesta característica
15 premedida, posiblemente decriptada usando una llave asimétrica de datos, para determinar si el dispositivo de seguridad puede ser o no clasificado como no falsificado. Tal comparación se hace con un margen de error permitido para variaciones que son introducidas, por ejemplo, por fluctuaciones de temperatura.

20

Aun cuando ciertos de los materiales ejemplos aquí descritos son ferromagnéticos, aquellos versados en el arte entenderán que se pueden utilizar otros tipos de elementos magnéticos y/o no magnéticos, proporcionados para dar origen a una respuesta característica
25 adecuada que se pueda medir. Por ejemplo, se pueden usar elementos no magnéticos cuando tales elementos producen una respuesta que se

puede medir en un campo magnético, cuando tal respuesta puede ser medida para proporcionar una rúbrica o respuesta característica.

Aquellos ordinariamente versados en el arte serán conocedores de
5 varias técnicas que se pueden usar para fabricar y caracterizar
elementos magnéticos adecuados para dispositivos de seguridad. Un
ejemplo de una de tales técnicas de fabricación y uno de tales procesos
de caracterización se puede encontrar en "Optimised process for the
10 fabrication of mesoscopic magnetic structures" Adeyeye et al, Journal of
Applied Physics, Vol. 682, No. 1, pp. 469-473, 1 Julio de 1997, el cual
investigó el efecto del tamaño del elemento magnético sobre las
propiedades magnéticas de él.

Las incorporaciones producidas de acuerdo con la invención pueden
15 incorporar medidas mejoradas de reflectividad / contraste bien sea solas
o en cualquier combinación. Materiales tales como el oro, aluminio,
cromo y /o tantalio se pueden poner por debajo y/o por encima de los
elementos magnéticos para mejorar su reflectividad y/o la señal Kerr
que los elementos magnéticos proporcionan. Las áreas de un
20 dispositivo de seguridad se pueden tratar para reducir sus
reflectividades con el objetivo de mejorar la reflectividad / contraste
entre los elementos magnéticos y sus áreas circundantes.

En varias incorporaciones, se proporcionan elementos magnéticos en la
25 forma de hilos o hilos aplanados. La forma terminada de tales hilos se
puede controlar durante la fabricación de un dispositivo de seguridad.
Se puede proporcionar un terminado angulado, por ejemplo, desde

L4

cerca de 60° a cerca de 90°. En otras varias incorporaciones se pueden proporcionar terminados aplanados y/o terminados semicirculares, para influenciar la nucleación magnética. La forma de los terminados se puede escoger para proporcionar características de interrupción magnética mejoradas.

Aunque la invención ha sido descrita en relación con incorporaciones particulares, se apreciará que la invención no se limita a estas, y que son posibles muchas variaciones que caen dentro del alcance de la invención.

Se apreciará que ciertas de las varias incorporaciones de la invención antes descritas se pueden implementar y/o configurar, por lo menos en parte, utilizando un aparato de procesamiento de datos, tal como, por ejemplo, hardware, firmware y/o un computador configurado con un programa de computador. El programa de computador se puede almacenar sobre un medio vehículo de forma que se pueda usar un aparato de procesamiento de datos. El medio vehículo puede ser, por ejemplo, memoria en estado sólido, memoria óptica o memoria magneto-óptica tal como un disco que se puede leer y/o escribir, por ejemplo, un disco compacto y un disco digital versátil, o memoria magnética tal como un disco o una cinta, y los aparatos que procesan datos pueden utilizar el programa para configurarlo para operación. El programa de computador puede ser suministrado desde una fuente remota incorporada en un medio vehículo tal como una señal electrónica, que incluye onda vehículo de radiofrecuencia u onda vehículo óptica.

Los ejemplos anteriores son meramente ilustrativos de los posibles usos del un dispositivo de acuerdo con varios aspectos de la invención. Se apreciará que un dispositivo de rúbrica de acuerdo con las varias incorporaciones de la invención podría tener un enorme intervalo de aplicaciones, en particular que son aplicables a cualquier situación en donde el abuso de copias falsificadas de ítems originales o de las ediciones de seguridad eleva la significancia comercial.

10 Aquellos ordinariamente versados en el arte serán conocedores que la descripción aquí hecha , se refiere meramente a ejemplos ilustrativos de cómo la invención puede ponerse en práctica, y que se pueden contemplar muchas incorporaciones que incorporan uno o más componentes, e.g., de otras incorporaciones, a lo largo con otras

15 incorporaciones no explícitamente descritas aquí. Por ejemplo, tasas de adquisición de datos, tasas de muestra, el número y tamaño de los niveles de cuantización, las tasas de ciclización del campo magnético aplicado, el número de conjuntos de datos acumulados, etc., todos se pueden variar / seleccionar como se desee. Tales parámetros se

20 pueden variar de manera programada, por ejemplo, bajo el control de un microprocesador, posiblemente en dependencia con varias condiciones medidas, tales como, por ejemplo, la temperatura.

El alcance de la presente divulgación incluye cualquier característica

25 novedosa o combinación de características aquí divulgadas explícitamente o implícitamente o cualquier generalización de ellas, independientemente de si se refieren o no la invención reivindicada o

mitiga cualquiera o todos los problemas direccionados por la presente invención. Por lo tanto el solicitante notifica que se pueden formular reivindicaciones nuevas tal que las características durante la prosecución de esta solicitud o de cualquier otra solicitud derivada de ésta. En particular, con referencia a las reivindicaciones anexas, cláusulas, aspectos y párrafos, características dependientes a partir de las reivindicaciones, cláusulas, aspectos y/o párrafos que se pueden combinar con aquellos de las reivindicaciones independientes, cláusulas, aspectos y/o párrafos y características de las reivindicaciones independientes respectivas, cláusulas, aspectos y/o párrafos se pueden combinar en cualquier manera apropiada y no meramente en las combinaciones específicas enumeradas.

15

20

25

REIVINDICACIONES

1. Un dispositivo de seguridad que comprende dos o más
elementos magnéticos, en donde dichos elementos magnéticos
5 son sensibles a un campo magnético aplicado para proporcionar
una respuesta característica.
2. El dispositivo de seguridad de la reivindicación 1, en donde dicha
respuesta característica se proporciona en combinación con una
10 respuesta característica premedida.
3. El dispositivo de seguridad de la reivindicación 1 o la
reivindicación 2, en donde dicha respuesta característica
representa una respuesta agregada de dichos elementos
15 magnéticos a dicho campo magnético aplicado.
4. El dispositivo de seguridad de cualquier reivindicación
precedente, en donde dichos elementos magnéticos están
sostenidos por un sustrato.
20
5. El dispositivo de seguridad de la reivindicación 4, en donde
dichos elementos magnéticos están sostenidos sobre dicho
sustrato.
- 25 6. El dispositivo de seguridad de cualquier reivindicación
precedente, en donde los elementos magnéticos comprenden
una capa delgada de material magnético.

7. El dispositivo de seguridad de la reivindicación 6, en donde las capas delgadas del material magnético son de menos de 1 μm de espesor.
- 5 8. El dispositivo de seguridad de la reivindicación 7, en donde las capas delgadas de material magnético tienen entre 10 nm y 100 nm de espesor.
- 10 9. El dispositivo de seguridad de cualquier reivindicación precedente, en donde dichos elementos magnéticos son sensibles a dicho campo magnético aplicado para interrumpir la magnetización o polarización magnética de por lo menos uno de los elementos magnéticos.
- 15 10. El dispositivo de seguridad de cualquier reivindicación precedente, en donde por lo menos uno de los elementos magnéticos está hecho de un material suave magnéticamente.
- 20 11. El dispositivo de seguridad de la reivindicación 10, en donde por lo menos uno de los elementos magnéticos comprende un material suave magnéticamente seleccionado de uno o más de : níquel, hierro, cobalto, y aleaciones de ellos con cada uno de los otros o con silicio, tal como aleación níquel hierro, aleación cobalto hierro, aleación hierro silicio o aleación cobalto silicio.

25

12. El dispositivo de seguridad de la reivindicación 10 o 11, en donde dicho material suave magnéticamente es un material de permalloy.
- 5 13. El dispositivo de seguridad de cualquier reivindicación precedente, en donde por lo menos uno de los elementos magnéticos sustancialmente es en forma de hilo o en forma de hilo aplanado.
- 10 14. El dispositivo de seguridad de cualquier reivindicación precedente, en donde el dispositivo comprende un ordenamiento generalmente paralelo de elementos magnéticos rectangulares.
- 15 15. El dispositivo de seguridad de la reivindicación 14, en donde los elementos magnéticos comprenden un ordenamiento de nanohilos magnéticos generalmente paralelos.
- 20 16. El dispositivo de seguridad de cualquier reivindicación precedente, en donde los elementos magnéticos generalmente tienen el mismo tamaño y/o forma.
- 25 17. El dispositivo de seguridad de cualquier reivindicación precedente, en donde varios grupos discretos de elementos magnéticos de diferente tamaño y/o forma, siendo los elementos magnéticos generalmente similares en tamaño y forma dentro de cada grupo, se proporcionan tal que se puedan identificar varios campos de interrupción diferentes.

18.El dispositivo de seguridad de la reivindicación 17, que
comprende un ensamble de elementos magnéticos rectangulares
en ordenamiento paralelo que incluye varios grupos discretos de
5 elementos magnéticos de diferentes anchos.

19.El dispositivo de seguridad de cualquier reivindicación
precedente, en donde se proporcionan elementos magnéticos de
10 diferente tamaño y/o forma en un ordenamiento que varía
continuamente, tal que las variaciones en tamaño y/o forma entre
un elemento magnético y su vecino estén minimizadas para
evitar grandes discontinuidades.

15 20.El dispositivo de seguridad de la reivindicación 19, que
comprende un ensamble de elementos magnéticos rectangulares
en ordenamiento paralelo de espesor que varía continuamente a
través del ordenamiento.

20 21.El dispositivo de seguridad de cualquier reivindicación
precedente, que comprende además un elemento magnético
único de área relativamente grande que se usa como un
elemento de referencia.

25

22.El dispositivo de seguridad de cualquier reivindicación precedente, en donde por lo menos uno de los elementos magnéticos está recubierto por una capa reflectiva de luz.

5 23.El dispositivo de seguridad de cualquier reivindicación precedente, en donde por lo menos uno de los elementos magnéticos se proporciona próximo a una porción de reflectividad reducida de luz de dicho dispositivo de seguridad.

10 24.El dispositivo de seguridad de cualquier reivindicación precedente, en donde los elementos magnéticos se arreglan para proporcionar un patrón lineal.

25.El dispositivo de seguridad de cualquier reivindicación
15 precedente, en donde dichos elementos magnéticos se arreglan para proporcionar un patrón bidimensional.

26.El dispositivo de seguridad de cualquier reivindicación
20 precedente, que además comprende un identificador único incorporado con él.

27.El dispositivo de seguridad de la reivindicación 26, en donde
dicho identificador único se proporciona por medio de uno o más
de: un código de barras que se puede leer ópticamente; uno o
25 más indicios ópticos; un identificador codificado magnéticamente;
y un identificador electrónico.

28.El dispositivo de seguridad de la reivindicación 27, montado sobre una tarjeta inteligente, en donde dicho identificador electrónico es proporcionado por un chip de tarjeta inteligente proporcionado sobre dicha tarjeta inteligente.

5

29.El dispositivo de seguridad de cualquier reivindicación precedente, en donde la información de respuesta característica premedida que representa uno o más parámetros que se pueden medir de dicha respuesta característica se almacena sobre dicho dispositivo de seguridad.

10

30.El dispositivo de seguridad de la reivindicación 29, en donde dicha información de respuesta característica premedida está en forma encriptada.

15

31.El dispositivo de seguridad de la reivindicación 30, en donde dicha información de respuesta característica premedida se encripta utilizando un algoritmo de encriptación asimétrico con la llave privada usada para cifrar que es mantenida en secreto y la llave pública usada para decifrar que se hace disponible para cualquier lector del dispositivo de seguridad.

20

32.El dispositivo de seguridad de la reivindicación 2 o de cualquiera de las reivindicaciones 3 a 31 cuando dependen de la reivindicación 2, en donde la respuesta característica premedida

25

se almacena en proximidad física al dispositivo de seguridad en forma que pueda ser leída por una máquina.

33. Un método de fabricación de un dispositivo de seguridad, que
5 comprende: proporcionar dos o más elementos magnéticos, en donde dichos elementos magnéticos proporcionan una respuesta característica en respuesta a un campo magnético aplicado.

34. El método de la reivindicación 33, que comprende proporcionar
10 dichos elementos magnéticos sobre un sustrato.

35. El método de la reivindicación 33 o la reivindicación 34, que comprende formar por lo menos uno de los elementos magnéticos utilizando un proceso de despegue "lift off" o proceso
15 de grabado en húmedo.

36. El método de la reivindicación 33 o la reivindicación 34, que comprende formar por lo menos uno de los elementos magnéticos utilizando un proceso de grabado por rayo de iones.
20

37. El método de cualquiera de las reivindicaciones 33 a 36, que comprende medir la (s) magnitud (es) de uno o más parámetros magnéticos de dichos elementos magnéticos.

25 38. El método de la reivindicación 37, que comprende medir uno o más de los valores de coercitividad y fluctuación.

39.El método de la reivindicación 37 o la reivindicación 38, que comprende utilizar la magnitud (es) medida (s) de dichos uno o más parámetros magnéticos para representar la información de respuesta característica premedida.

5

40.El método de la reivindicación 39, que comprende encriptar dicha información de respuesta característica premedida.

41.El método de la reivindicación 39 o la reivindicación 40, que
10 comprende almacenar dicha información de respuesta característica premedida en forma encriptada o no encriptada sobre dicho dispositivo de seguridad.

42.El método de la reivindicación 39 o la reivindicación 40, que
15 comprende almacenar dicha información de respuesta característica premedida en forma encriptada o no encriptada en un medio de almacenamiento remoto a dicho dispositivo de seguridad.

20 43.El método de la reivindicación 42, que comprende almacenar dicha información de respuesta característica premedida en forma encriptada o no encriptada en una base de datos.

44.El método de cualquiera de las reivindicaciones 33 a 43, que
25 además comprende proporcionar dicho dispositivo de seguridad con un identificador único.

45. El método de la reivindicación 44 cuando dependa de cualquiera de las reivindicaciones 39 a 43, que comprende almacenar una representación de dicho identificador único en asociación con dicha información de respuesta característica premedida.

5

46. Un sistema para leer un dispositivo de seguridad, que comprende: un sistema de generación de campo magnético para aplicar un campo magnético a un dispositivo de seguridad que comprende dos o más elementos magnéticos; y un sistema de
10 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 se puede operar para comparar dichos uno o más parámetros representativos de una respuesta característica
15 medida con uno o más parámetros respectivos de una respuesta característica premedida para determinar si los parámetros respectivos medidos y premedidos son sustancialmente equivalentes.

20 47. El sistema de la reivindicación 46 en donde dicha respuesta característica medida y dicha respuesta característica premedida son representativas de una respuesta agregada producida por dichos dos o más elementos magnéticos.

25 48. El sistema de la reivindicación 46 o la reivindicación 47, en donde el sistema de generación de campo magnético se puede operar

para aplicar un campo magnético que varia en el tiempo a un dispositivo de seguridad.

49.El sistema de cualquiera de las reivindicaciones 46 a 48, en
5 donde se utiliza un rayo de luz para interrogar dicho dispositivo de seguridad.

50.El sistema de la reivindicación 49, en donde dicho rayo de luz es
un rayo del visible o del infra-rojo cercano producido por un diodo
10 láser.

51.El sistema de cualquiera de las reivindicaciones 46 a 50, en
donde dichos parámetros representan uno o más valores de
cohercitividad y fluctuación.

15 52.El sistema de cualquiera de las reivindicaciones 49 a 51, en
donde dicho sistema de detección incorpora aparatos de
detección del efecto magnéto – óptico kerr para detectar cambios
inducidos en dicho rayo de luz por los elementos magnéticos de
20 dicho dispositivo de seguridad.

53.El sistema de la reivindicación 52, en donde dicho aparato de
detección del efecto magnéto – óptico kerr está configurado para
operar en modo transverso.

25

54.El sistema de cualquiera de las reivindicaciones 36 a 40 que además se puede operar para deflectar dicho rayo de luz a través de la superficie de dicho dispositivo de seguridad.

5 55.El sistema de cualquiera de las reivindicaciones 46 a 54, que además se puede operar para leer un identificador único desde dicho dispositivo de seguridad.

56.El sistema de la reivindicación 55, en donde dicho identificador
10 único se identifica leyendo uno o más de: un código de barras que se puede leer ópticamente; uno o más indicios ópticos; un identificador codificado magnéticamente; y un identificador electrónico.

15 57.El sistema de cualquiera de las reivindicaciones 46 a 56, que además puede operar para determinar dichos uno o más parámetros respectivos de la respuesta característica premedida leyendo dichos uno o más parámetros desde dicho dispositivo de seguridad.

20 58.El sistema de cualquiera de las reivindicaciones 46 a 57, que además puede operar para determinar dichos uno o más parámetros respectivos de la respuesta característica premedida leyendo dichos uno o más parámetros desde una base de datos.

25 59.El sistema de la reivindicación 58 en donde dicha base de datos está localizada remotamente de dicho sistema de detección.

60. El sistema de cualquiera de las reivindicaciones 46 a 59, que además puede operar para descryptar la información de respuesta característica premedida cuando ésta se lee o proporciona en forma encriptada.
- 5
61. Un método para leer un dispositivo de seguridad, que comprende:
- aplicar un campo magnético a un dispositivo de seguridad que comprende dos o más elementos magnéticos,
- medir uno o más parámetros representativos de una respuesta
- 10 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
- 15 determinar si los parámetros respectivos medidos y premedidos son sustancialmente equivalentes.
62. El sistema de la reivindicación 61 en donde dicha respuesta característica medida y dicha respuesta característica premedida
- 20 son representativas de una respuesta agregada producida por dichos dos o más elementos magnéticos.
63. El método de la reivindicación 61 o la reivindicación 62, que comprende aplicar un campo magnético que varía en el tiempo al
- 25 dispositivo de seguridad.

64.El método de cualquiera las reivindicaciones 61 a 63, en donde
medir uno o más parámetros representativos de una respuesta
característica medida de dicho dispositivo de seguridad en
respuesta a dicho campo magnético comprende medir uno o más
5 valores de coercitividad y fluctuación.

65.El método de cualquiera de las reivindicaciones 61 a 64, que
comprende interrogar dicho dispositivo de seguridad utilizando un
rayo de luz.

10

66.El método de cualquiera de las reivindicaciones 61 a 65, que
comprende operar un láser para producir un rayo del visible o
del infra-rojo cercano.

15 67.El método de la reivindicación 65 o la reivindicación 66, que
compende detectar los cambios inducidos en dicho rayo de luz
por los elementos magnéticos de dicho dispositivo de seguridad
utilizando el efecto magneto-óptico Kerr.

20 68.El método de la reivindicación 67 que comprende utilizar el efecto
magneto-óptico Kerr de modo trasverso.

69.El método de cualquiera de las reivindicaciones 61 a 68 que
comprende leer un identificador único desde dicho dispositivo de
25 seguridad.

70. El método de la reivindicación 69 que comprende identificar dicho
identificador único, por lectura de uno o más de : un código de
barras que se puede leer ópticamente; uno o más indicios
ópticos; un ientificador codificado magnéticamente; y un
5 identificador electrónico.

71. El método de cualquiera de las reivindicaciones 61 a 70, que
comprende determinar dichos uno o más parámetros respectivos
de la respuesta característica premedida mediante la lectura de
10 dichos uno más parámetros desde dicho dispositivo de
seguridad.

72. El método de cualquiera de las reivindicaciones 61 a 71, que
comprende determinar dichos uno o más parámetros respectivos
15 de la respuesta característica premedida, mediante la lectura de
dichos uno o más parámetros desde una base de datos.

73. El método de la reivindicación 72, que comprende el acceso a
una base de datos localizada remotamente desde dicho sistema
20 de detección.

74. El método de cualquiera de las reivindicaciones 61 a 73, que
además comprende decriptar la información de respuesta
característica premedida cuando ésta se lee o se proporciona en
25 forma encriptada.

75. Un producto que comprende el dispositivo de seguridad de cualquiera de las reivindicaciones 1 a 32.

76. El producto de la reivindicación 75 que comprende uno o más
5 de: un documento; un pasaporte; una tarjeta de identidad; un disco compacto; un disco digital versátil; un producto de software; empaque; un ítem para vestuario, un ítem para calzado; una tarjeta inteligente; una tarjeta de crédito o bancaria; un ítem cosmético; una parte de ingeniería, un accesorio; y cualquier otro
10 bien y/o ítems de comercio bien sean o no fabricados.

15

20

25

RESUMEN

Se divulga un dispositivo de seguridad (700) que comprende dos o mas
5 elementos magnéticos (702). Los elementos magnéticos (702) son
sensibles o responden a un campo magnético aplicado para
proporcionar una respuesta característica que es difícil de reproducir. El
dispositivo de seguridad (700) encuentra aplicación en la detección de
falsificaciones.

10

15

1/13

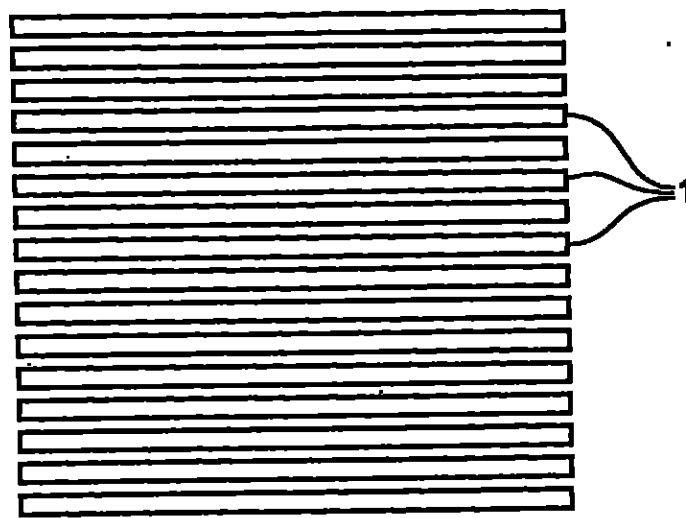


Fig. 1



Fig. 2

3/13

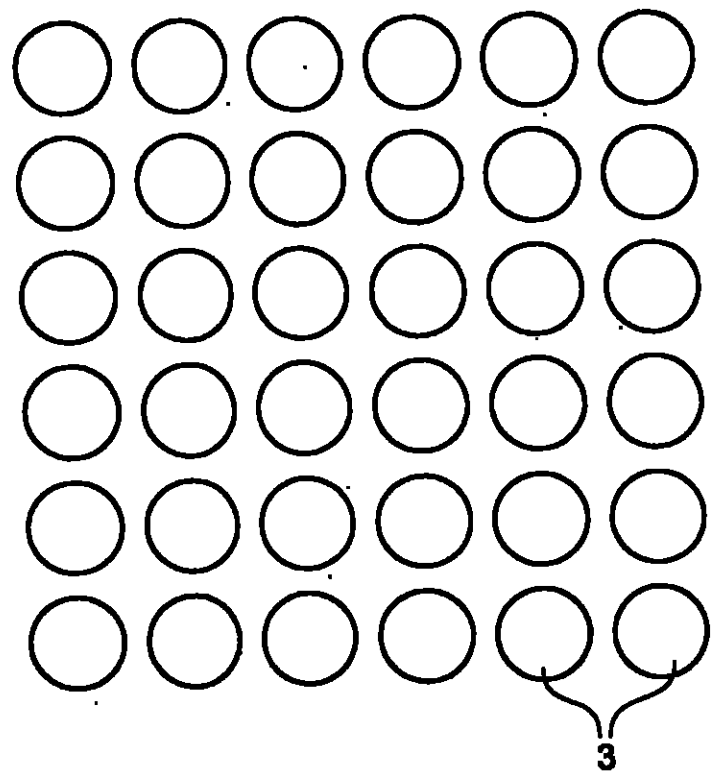


Fig. 3

4/13

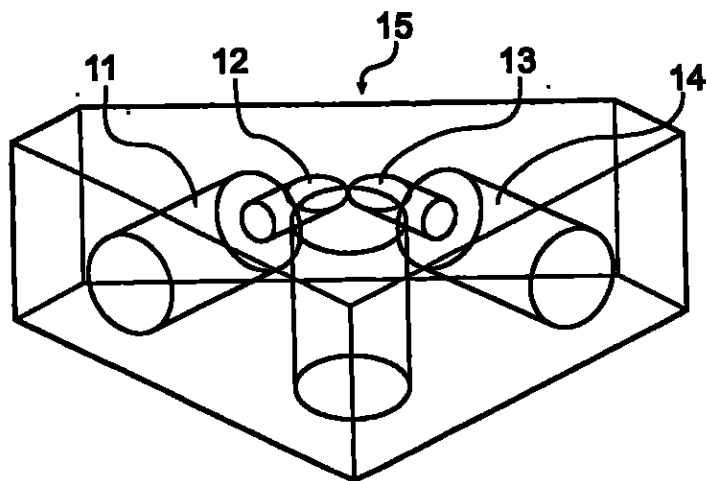


Fig. 4a

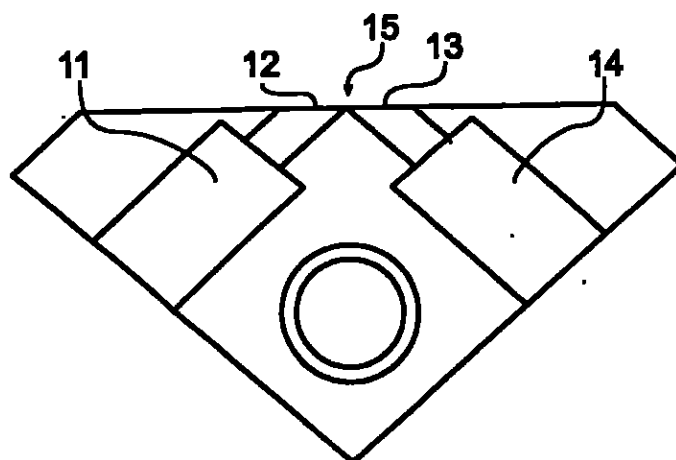


Fig. 4b

5/13

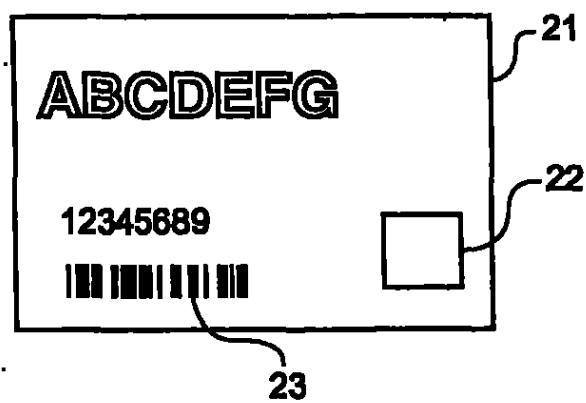


Fig. 5a

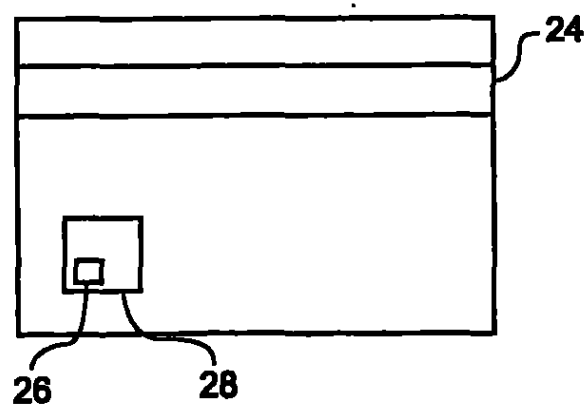


Fig. 5b

6/13

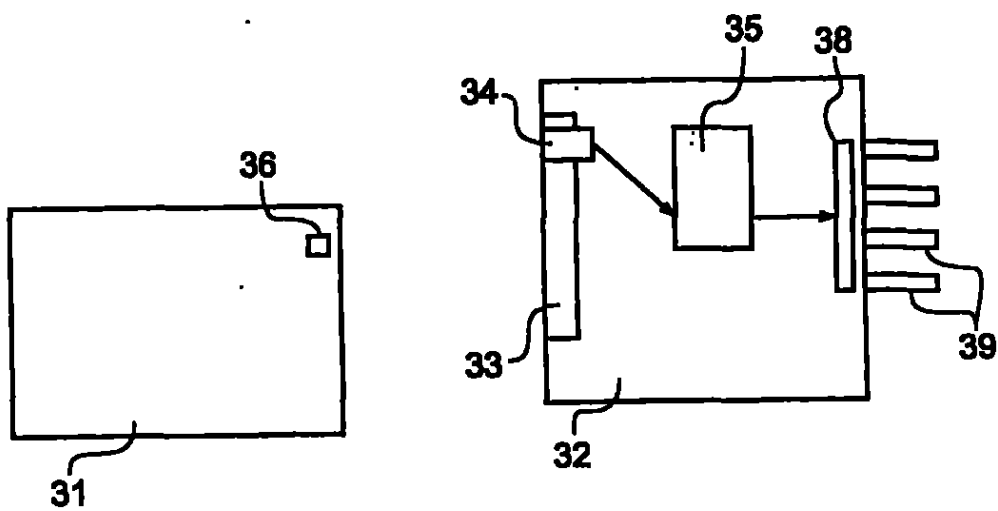


Fig. 6

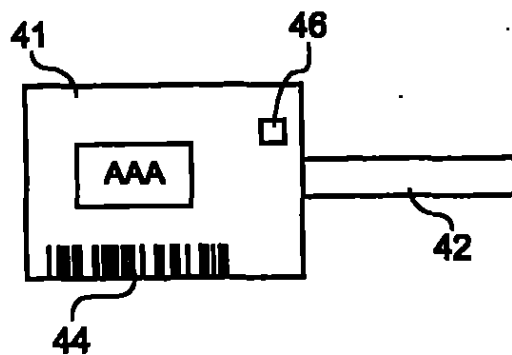


Fig. 7

7/13

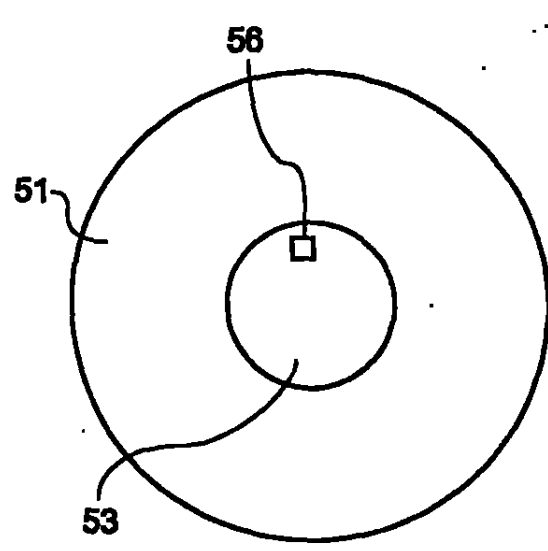


Fig. 8

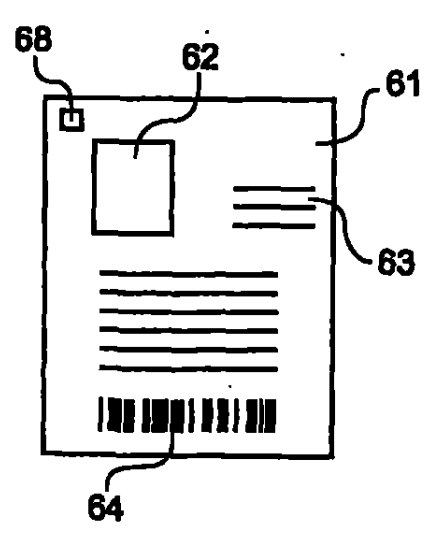


Fig. 9



Fig. 10a



Fig. 10b

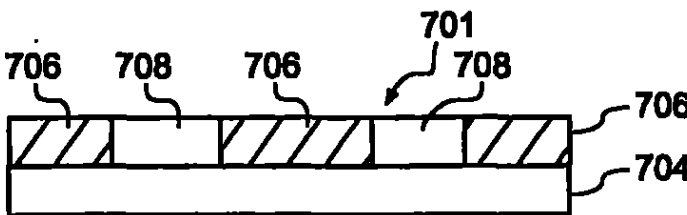


Fig. 10c

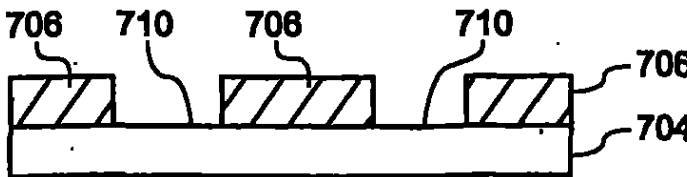


Fig. 10d

9/13

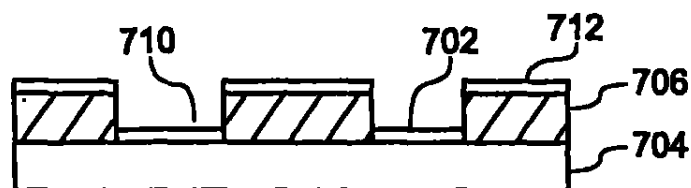


Fig. 10e

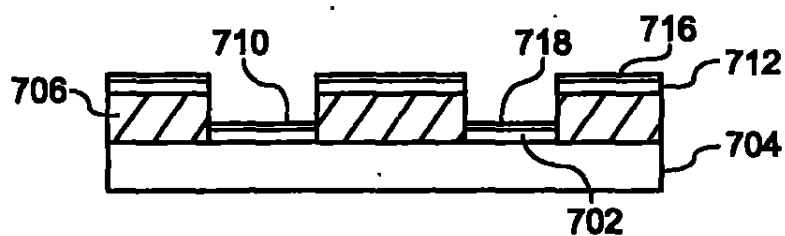


Fig. 10f

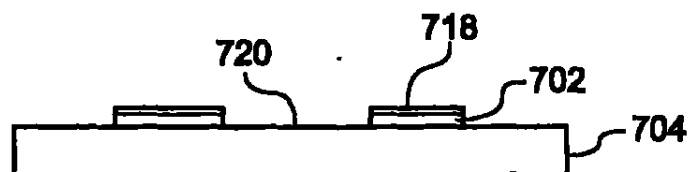


Fig. 10g

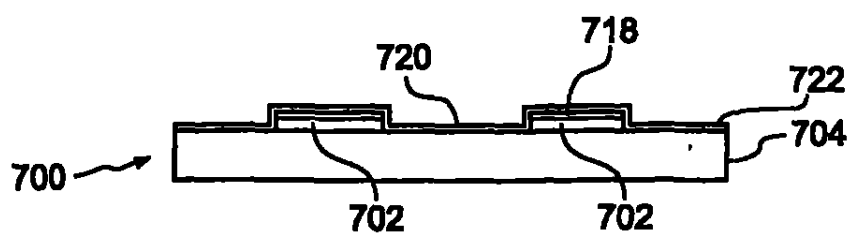


Fig. 10h

10/13

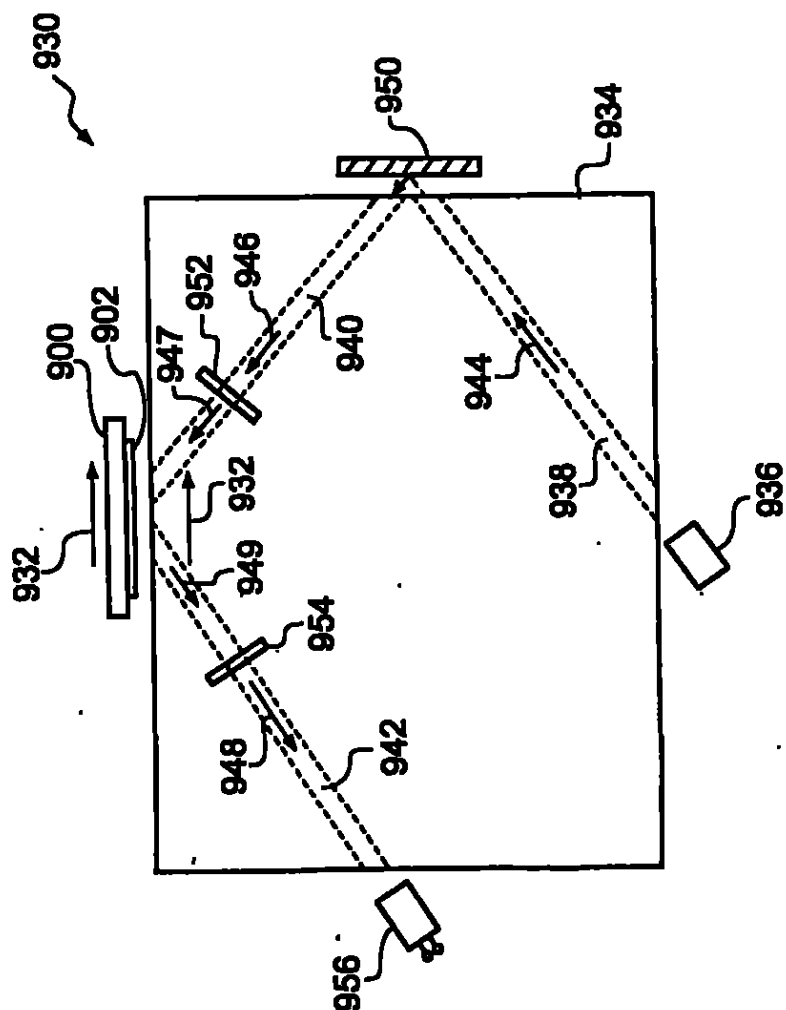


Fig. 11

11/13

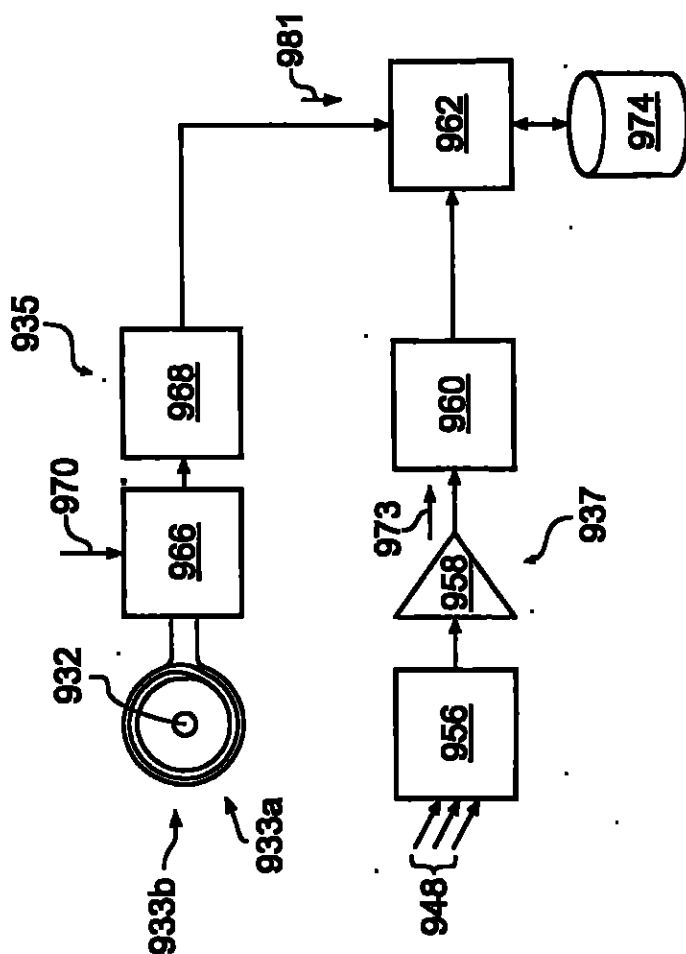


Fig. 12

12/13

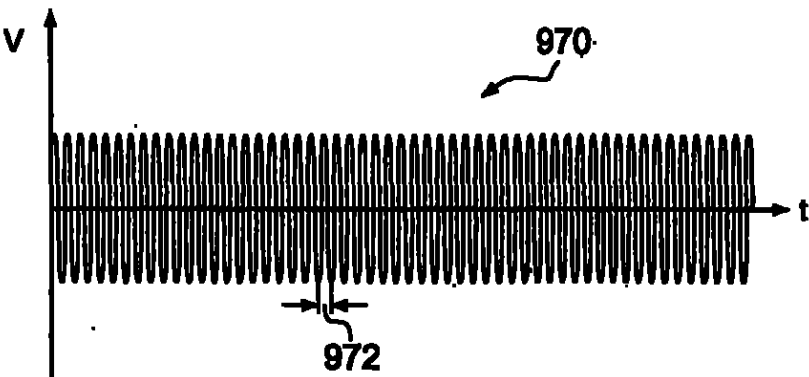


Fig. 13

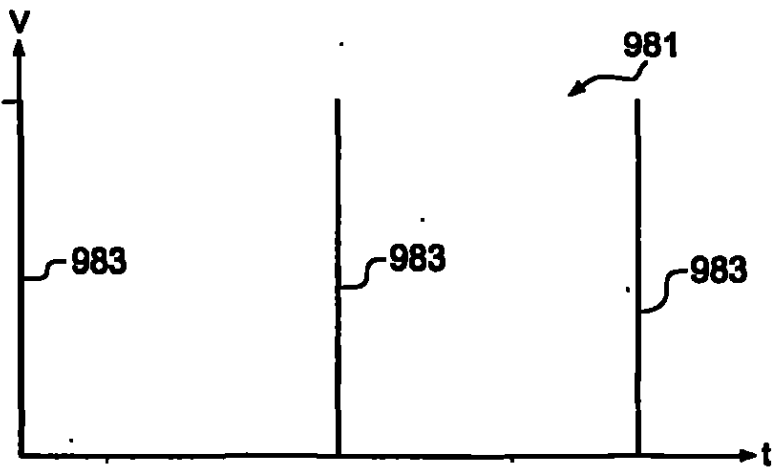


Fig. 14

13/13

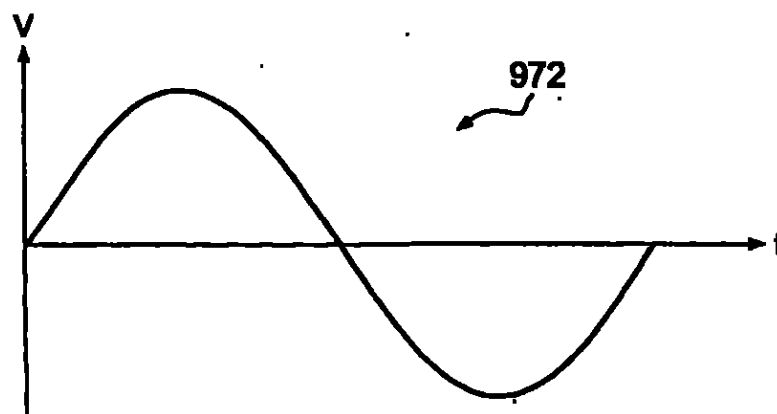


Fig. 15

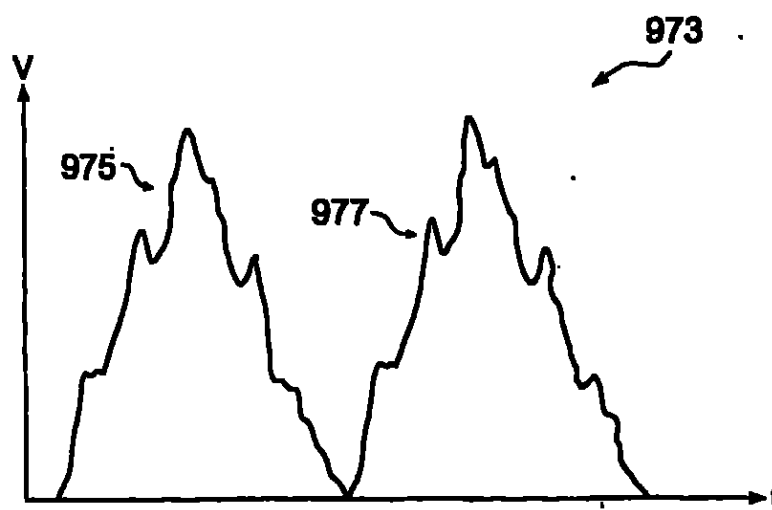


Fig. 16

segundo Exame de forma L72

PATENT COOPERATION TREATY

SOUTHAMPTON
30 DEC 2004

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

PCT

To:	MONEY	£
HAINES, Miles John D YOUNG & CO 21 New Fetter Lane London EC4A 1DA GRANDE BRETAGNE	ORDER	
	DIARY	
	REC'D	30 DEC 2004
	ANSO	
	ENTRY	
	FOR	DS MJH

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

Date of mailing (day/month/year)	28.12.2004
-------------------------------------	------------

Applicant's or agent's file reference P018298WO MJH		IMPORTANT NOTIFICATION	
International application No. PCT/GB 03/03917	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 P018298WO MJH	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEAA/16)	
International application No. PCT/GB 03/03917	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 7 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 10 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 04.03.2004	Date of completion of this report 28.12.2004	
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 apmu d Fax: +49 89 2399 - 4485	Authorized Officer Geiger, J-W Telephone No. +49 89 2399-2584 	

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/GB 03/03917**

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

1-49 as originally filed

Claims, Numbers

1-75 received on 17.11.2004 with letter of 15.11.2004

Drawings, Sheets

1/13-13/13 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 03/03917**

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	7,8,10-14,16-19,21,22,34,35,51,52,66,67
	No: Claims	1-6,9,15,20,23-33,36-50,53-65,68-75
Inventive step (IS)	Yes: Claims	
	No: Claims	7,8,10-14,16-19,21,22,34,35,51,52,66,67
Industrial applicability (IA)	Yes: Claims	1-75
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1*: WO 02 50790

D2*: GB 1 601 362

* These documents were not cited in the International Search Report.

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

The document D1 discloses (the references in parentheses applying to this document):

A security device comprising two or more magnetic elements (cf. D1, fig. 11, 12, or 14), wherein said magnetic elements are responsive to switch magnetisation state in response to an applied magnetic field to provide a characteristic response (cf. D1, page 24, 2nd paragraph), whereby the elements are made of magnetically soft material (cf D1, pages 31, 32, and fig. 20, disclosing MIOX particles which consists of $\alpha\text{-Fe}_2\text{O}_3$. Alpha- Fe_2O_3 is a magnetically soft material), hence, discretely switches magnetisation state at an applied field strength that depends upon inherent structural variations that are present in the magnetically soft material (cf. D1, pages 11, 12).

No

3 Claims 2 - 75 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step.

3.1 The features added by the following dependent claims are known from D1:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/03917

as to claims 2, 31:

the security device stores a premeasured characteristic response, see D1, page 14, second half;

as to claims 3:

"aggregate response", see D1, page 5, last paragraph - page 6, 1st paragraph (reading of the "image");

as to claims 4 - 6:

see D1, e.g. fig. 14;

as to claim 9:

see cf. D1, page 24, 2nd paragraph;

as to claim 15:

see D1, e.g. fig. 21;

as to claim 20:

see D1, page 42, paragraph f);

as to claims 23, 24:

see D1, e.g. fig. 14;

as to claims 25, 26:

see D1, fig. 19, right upper corner;

as to claims 27 - 30:

see D1, page 42, paragraphs h) - j));

as to claims 32, 33:

the features of said claims do not extend beyond the features of claims 1, 3 - 6 resp. in method terms, hence they are objectionable on the same reasons as claims 1, 3 - 6.

as to claims 36 - 38:

see D1, page 4, last paragraph - page 5, 1st paragraph, page 24, 2nd paragraph; "measurement" via the analysis of the image pattern;

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB 03/03917

as to claims 39 - 44:
see D1, page 31, 2nd paragraph;

as to claims 45, 46, 48 - 50, 53 - 59:
see D1, page 24, 2nd paragraph; page 27, 2nd paragraph - page 28, 2nd paragraph; page 42; fig. 9, 17, 19;

as to claim 47:
in D1 the magnetic field is switched on/off for analyzing the images, hence the magnetic field varies in time as claimed;

as to claims 74, 75:
see D1, fig. 18.

3.2 The features of following claims do not add any inventive step since they are either straightforward design alternatives which would be within the abilities of a skilled person in the field of forming security devices or can be derived without inventive efforts by combining D1 with document D2.

as to claims 7, 8:
standard dimensions in the field of layered security devices;

as to claims 10, 11:
the claimed materials are some of several straightforward possibilities from which the skilled person would select, see e.g. D2, page 2, line 104 - page 3, line 61;

as to claims 12 - 14:
combining D1, page 44, paragraph t) with D2, fig.2 would directly lead without applying an inventive step to the features of said claims;

as to claims 16 - 19:
their features are already disclosed by D2, fig. 2. It would be obvious to apply these features in the device of D1;

as to claims 21, 22:
design alternatives of the device of D1 which do not justify an inventive step;

as to claims 34, 35:

these features are standard technology processes from which the skilled person would select to realize a security device;

as to claim 51, 52:

the feature of said claim is one of several straightforward alternatives from which the skilled person would select if a magnetically controlled optical effect has to be used.

3.3 The features of claims 60 - 73 do not extend beyond the features of claims 45 - 59 resp. in method terms.

Hence, the subject-matter of claims 60 - 73 does not fulfill the requirements of Articles 33(2)(3) PCT, resp..

CLAIMS

1. A security device comprising two or more magnetic elements, wherein said
5 magnetic elements are responsive to switch magnetisation state in response to an
applied magnetic field to provide a characteristic response, characterised in that the
elements are made of magnetically soft material that discretely switches
magnetisation state at an applied field strength that depends upon inherent structural
variations that are present in the magnetically soft material.
- 10 2. The security device of Claim 1, wherein the security device stores a
premeasured characteristic response.
3. The security device of Claim 1 or Claim 2, wherein said characteristic
15 response represents an aggregate response of said magnetic elements to said applied
magnetic field.
4. The security device of any preceding Claim, wherein said magnetic elements
are supported by a substrate.
- 20 5. The security device of Claim 4, wherein said magnetic elements are
supported on said substrate.
6. The security device of any preceding Claim, wherein the magnetic elements
25 comprise thin layer magnetic material.
7. The security device of Claim 6, wherein the thin layers of magnetic material
are less than 1 μm thick.
- 30 8. The security device of Claim 7, wherein the thin layers of magnetic material
between 10 nm and 100 nm thick.

P18298WO

AMENDED SHEET

9. The security device of any preceding Claim, wherein said magnetic elements are responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of at least one of the magnetic elements.

5

10. The security device of any preceding claim, wherein at least one of the magnetic elements 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.

10

11. The security device of Claim 10, wherein said magnetically soft material is a permalloy material.

12. The security device of any preceding Claim, wherein at least one of the magnetic elements is substantially wire-shaped or flattened wire shaped.

15

13. The security device of any preceding Claim, wherein the device comprises a generally parallel array of elongate rectangular magnetic elements.

14. The security device of Claim 13, wherein the magnetic elements comprise an array of generally parallel magnetic nanowires.

20

15. The security device of any preceding Claim, wherein the magnetic elements have generally the same size and/or shape.

25

16. The security device of any preceding Claim, wherein several discrete groups of differently sized and/or shaped magnetic elements, the magnetic elements being generally similarly sized and/or shaped within each group, are provided so that several different switching fields can be identified.

30

PIB298WO

AMENDED SHEET

17. The security device of Claim 16, comprising an ensemble of rectangular magnetic elements in parallel array including several discrete groups of magnetic elements of different widths.

5 18. The security device of any preceding Claim, wherein differently sized and/or shaped magnetic elements are provided in a continuously varying array, so that variations in sized and/or shape between a magnetic element and its neighbours are minimised to avoid large discontinuities.

10 19. The security device of Claim 18, comprising an ensemble of rectangular magnetic elements in parallel array of width varying continuously across the array.

20. The security device of any preceding Claim, further comprising a single relatively large area magnetic element for use as a reference element.

15

21. The security device of any preceding Claim, wherein at least one of the magnetic elements is backed by a light reflective layer.

20 22. The security device of any preceding Claim, wherein at least one of the magnetic elements is provided proximal a reduced light reflectivity portion of said security device.

23. The security device of any preceding Claim, wherein the magnetic elements are arranged to provide a linear pattern.

25

24. The security device of any preceding Claim, wherein said magnetic elements are arranged to provide a two-dimensional pattern.

30 25. The security device of any preceding Claim, further comprising a unique identifier incorporated therewith.

P18298WO

AMENDED SHEET

26. The security device of claim 25, 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.

5 27. The security device of claim 26, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.

10 28. 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.

29. The security device of Claim 28, wherein said premeasured characteristic response information is in encrypted form.

15 30. The security device of Claim 29, wherein said premeasured characteristic response information 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 security device.

20 31. The security device of Claim 2 or any one of Claims 3 to 30 when dependent on Claim 2, wherein the premeasured characteristic response is stored in machine-readable form.

25 32. A method of manufacturing a security device, comprising:
providing two or more magnetic elements made of magnetically soft material having random variations introduced into the magnetically soft material during fabrication, wherein said magnetic elements discretely switch magnetisation state in response to an applied magnetic field in order to generate a characteristic response.

30 33. The method of Claim 32, comprising providing said magnetic elements on a substrate.

P18298WO

AMENDED SHEET

34. The method of Claim 32 or Claim 33, comprising forming at least one of the magnetic elements using a lift off or wet etching process.

5 35. The method of Claim 32 or Claim 33, comprising forming at least one of the magnetic elements using an ion beam etching process.

36. The method of any one of Claims 32 to 35, comprising measuring the magnitude(s) of one or more magnetic parameters of said magnetic elements.

10

37. The method of Claim 36, comprising measuring one or more of coercivity and jitter values.

15

38. The method of Claim 36 or Claim 37, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.

39. The method of Claim 38, comprising encrypting said premeasured characteristic response information.

20

40. The method of Claim 38 or Claim 39, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.

25

41. The method of Claim 38 or Claim 39, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.

30

42. The method of Claim 41, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.

P18298WO

AMENDED SHEET

43. The method of any one of Claims 32 to 42, further comprising providing said security device with a unique identifier.

44. The method of Claim 43 when dependant upon any one of Claims 38 to 42, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.

45. A system for reading a security device, comprising:
a magnetic field generation system for applying a magnetic field to the security device according to any one of claims 1 to 31 comprising two or more magnetic elements; and

a detection system for measuring one or more discrete magnetisation switching parameters representative of a measured characteristic response of said security device generated in response to said magnetic field,

wherein said system is operable to compare said one or more discrete magnetisation switching 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.

20

46. The system of Claim 45, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

47. The system of Claim 45 or Claim 46, wherein the magnetic field generation system is operable to apply a time varying magnetic field to a security device.

48. The system of any one of Claims 45 to 47, wherein a light beam is used to interrogate said security device.

30

P18298WO

AMENDED SHEET

49. The system of Claim 48, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

50. The system of any one of Claims 45 to 49, wherein said parameters represent
5 one or more of coercivity and jitter values.

51. The system of any one of Claims 48 to 50, 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.

10

52. The system of Claim 51, wherein said magneto-optic Kerr effect detection apparatus is configured to operate in transverse mode.

53. The system of any one of Claims 45 to 52, further operable to deflect said
15 light beam across the surface of said security device.

54. The system of any one of Claims 45 to 53, further operable to read a unique identifier from said security device.

20 55. The system of Claim 54, 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.

56. The system of any one of Claims 45 to 55, further operable to determine said
25 one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

57. The system of any one of Claims 45 to 56, further operable to determine said
30 one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

P18298WO

AMENDED SHEET

58. The system of Claim 57, wherein said database is remotely located from said detection system.

59. The system of any one of Claims 45 to 58, further operable to decrypt
5 premeasured characteristic response information where it is read or provided in encrypted form.

60. A method for reading the security device according to any one of claims 1 to 31, comprising:

10 applying a magnetic field to a security device comprising two or more magnetic elements made of magnetically soft material;

measuring one or more discrete magnetisation switching parameters representative of a measured characteristic response of said security device generated
in response to said magnetic field; and

15 comparing said one or more discrete magnetisation switching 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.

20 61. The system of Claim 60, wherein said measured characteristic response and said premeasured characteristic response are representative of an aggregate response produced by said two or more magnetic elements.

25 62. The method of Claim 60 or Claim 61, comprising applying a time varying magnetic field to a security device.

63. The method of any one of Claims 60 to 62, wherein measuring of one or more parameters representative of a measured characteristic response of said security device generated in response to said magnetic field comprises measuring one or more
30 of coercivity and jitter values.

P18298WO

AMENDED SHEET

64. The method of any one of Claims 60 to 63, comprising interrogating said security device using a light beam.
65. The method of any one of Claims 60 to 64, comprising operating a laser to produce a visible or near-infrared beam.
66. The method of Claim 64 or Claim 65, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.
67. The method of Claim 66, comprising using the magneto-optic Kerr effect transverse mode.
68. The method of any one of Claims 60 to 67, comprising reading a unique identifier from said security device.
69. The method of Claim 68, 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.
70. The method of any one of Claims 60 to 69, comprising determining said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.
71. The method of any one of Claims 60 to 70, comprising determining said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.
72. The method of Claim 71, comprising accessing a database remotely located from said detection system.

P18298WO

AMENDED SHEET

73. The method of any one of Claims 60 to 72, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.

5 74. A product comprising the security device of any one of Claims 1 to 31.

75. The product of Claim 74, 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
10 card; a cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.

TRATADO DE COOPERACIÓN DE PATENTES

De
LA AUTORIDAD INTERNACIONAL DE EXAMEN PRELIMINAR

PCT

Para:
HAINES, MILES JOHN
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) 28/12/2004

Archivo de referencia del solicitante o
del agente

P018298WO MJH

NOTIFICACIÓN IMPORTANTE

Solicitud Internacional No.

PCT/GB 03/03917

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 solicitantes 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) 2399-4485

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 P018298WO MJH	PARA ACCION POSTERIOR Ver Notificación de Transmisión del Informe del Examen Preliminar Internacional (Formato PCT/1PEA/416)
Solicitud internacional No. PCT/GB03/03917	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>7</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>10</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 04/03/2004	Fecha de completamiento de este Informe 28/12/2004
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 Gelger, J-W Teléfono No. 49 89 2399 2584

INFORME DE EXAMEN PRELIMINAR INTERNACIONAL

Solicitud Internacional No.
PCT/GB 03/03917

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 - 49 como se presentaron originalmente

Reivindicaciones Nos.:

1 - 75 como se recibieron en 17/11/2004 con carta de 15/11/2004

Dibujos, páginas:

1/13 - 13/13 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.

INF RME DE EXAMEN PRELIMINAR INTERNACIONAL

Solicitud Internacional No.
PCT/GB 03/03917

- 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 anexo 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	7,8,10-14,16-19,21,22,34,35,51,52,66,67	Si
	Reivindicaciones	1-6,9,15,20,23-33,36-50,53-65,68-75	No
Altura inventiva (IS)	Reivindicaciones		Si
	Reivindicaciones	7,8,10-14,16-19,21,22,34,35,51,52,66,67	No
Aplicación industrial (IA)	Reivindicaciones	1 - 75	Si
	Reivindicaciones		No

2 Citas y explicaciones

Ver hoja separada

INFORME DEL EXAMEN PRELIMINAR INTERNACIONAL-HOJA ANEXA
Solicitud Internacional No. PCT/GB 03/03917

Numeral V

Declaración razonada de conformidad con la Regla 66.2 (a) (ii) con relación; citaciones y explicaciones que apoyan tal declaración.

1. Se hace referencia a los siguientes documentos:

D1*: WO 0250790

D2*: GB 1601362

*estos documentos no fueron citados en el informe de búsqueda internacional. Se anexan copias de los documentos.

2. La presente solicitud no cumple con los criterios del Artículo 33 (1) PCT ya que materia de la reivindicación 1 no es nueva en el sentido del Artículo 33 (2) PCT.

El documento D1 revela (las referencias en paréntesis aplican a este documento):

Un dispositivo de seguridad que comprende dos o más elementos magnéticos (ver D1, fig. 11, 12, o 14), donde dichos elementos magnéticos son sensibles al cambiar el estado de magnetización en respuesta a un campo magnético aplicado para proporcionar una respuesta característica. (ver D1, página 24, segundo párrafo), por lo cual los elementos son hechos de un material suave magnéticamente (ver D1, páginas 31, 32, y fig. 20, revelando partículas MIOX las cuales consisten de alfa Fe₂O₃ es un material suave magnéticamente), por lo tanto, discretamente el estado de magnetización de los interruptores a un campo aplicado fortalece la dependencia sobre variaciones estructurales inherentes que están presentes en el material suave magnéticamente. (ver D1, páginas 11, 12).

3. Las reivindicaciones 2 a 75 no contienen características que, en combinación con las características de cualquier reivindicación a la cuales están referidas, cumplan con los requerimientos del PCT con respecto a la novedad y/o nivel inventivo.

3.1 Las características adicionales son conocidas de D1, por las siguientes reivindicaciones dependientes:

Para las reivindicaciones 2, 31:

El dispositivo de seguridad almacena la respuesta característica premeditada, ver D1, página 14, segunda mitad;

Para la reivindicación 3:

"respuesta agregada", ver D1, página 5, último párrafo- página 6, primer párrafo (lectura de la "imagen");

Para las reivindicaciones 4-6: ver D1, ejemplo, figura 14;

Para la reivindicación 9: ver D1, página 24, segundo párrafo;

Para la reivindicación 15:

Ver D1, ejemplo fig 21;

Para la reivindicación 20: ver D1, página 42, párrafo f);

Para las reivindicaciones 23,24: Ver D1, ejemplo figura 14;

Para las reivindicaciones 25, 26: ver D1, fig. 19, esquina superior derecha;

Para las reivindicaciones 27-30: ver D1, página 42, párrafos h)-j);

Para las reivindicaciones 32-33: las características de dichas reivindicaciones no van más allá de las características de las reivindicaciones 1,3-6 respectivamente, en los términos

del método, por lo tanto, estos se objetan por las mismas razones de las reivindicaciones 1,3-6.

Para las reivindicaciones 36-38: ver D1, página 4, último párrafo-página 5, primer párrafo, página 24, segundo párrafo; "medición" por el análisis del patrón de imagen.

Para las reivindicaciones 39-44: ver D1, página 31, segundo párrafo;

Para las reivindicaciones 45, 46, 48, 50, 53-59: ver D1, página 24, segundo párrafo; página 27- página 28, segundo párrafo; página 42; figura 9, 17,19.

Para la reivindicación 47: ver en D1, el campo magnético se cambia de encendido/apagado para el análisis de imágenes, por lo tanto, el campo magnético como reivindicado varía en el tiempo.

Para las reivindicaciones 74,75: ver D1, figura 18.

3.2 Las características de las siguientes reivindicaciones no aportan nada inventivo ya que estas son alternativas tanto directas de diseños que están dentro de las habilidades de una persona conocedora del arte en el campo de formar dispositivos de seguridad o pueden derivarse sin ningún esfuerzo inventivo por la combinación de D1 y D2.

Para las reivindicaciones 7, 8: dimensiones estándares en el campo de los dispositivos de seguridad por capas.

Para las reivindicaciones 10-11: los materiales reivindicados son de las muchas posibilidades directas que un conocedor del arte seleccionaría, ver, por ejemplo. D2, página 2, línea 104-página 3, línea 61;

Para las reivindicaciones 12-14: combinando D1, página 44, párrafo t) con D2, figura 2 conduciría directamente a las características de dichas reivindicaciones sin aplicar nivel inventivo.

Para las reivindicaciones 16-19: sus características ya han sido reveladas por D2, figura 2. Sería obvio aplicar éstas características en el dispositivo de D1;

Para las reivindicaciones 21-22: alternativas del diseño del dispositivo de D1, lo que no justifica el nivel inventivo;

Para las reivindicaciones 34,35: Estas características son estándares de los procesos de tecnología de los cuales una persona del arte seleccionaría para realizar el dispositivo de seguridad.

Para las reivindicaciones 51,52: la característica de dicha reivindicación es una de las muchas alternativas directas de las cuales una persona del arte seleccionaría si tiene que usarse un efecto óptico controlado magnéticamente.

3.3 Las características de las reivindicaciones 60-73 no van más allá de las características de las reivindicaciones 45-59 respectivamente. En términos del método. Por lo tanto, el contenido de las reivindicaciones 60-73 no cumple con los requerimientos de los artículos 33 (2) (3) del PCT respectivamente.

PATENT C OPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

PCT

WRITTEN OPINION
(PCT Rule 66)

To: HAINES, Miles John D YOUNG & CO 21 New Fetter Lane London EC4A 1DA GRANDS-BRETAGNE SOUTHAMP 10 JUN 2004	MONEY	£	
	ORDER		
	DIARY	8/9/04	
	REC'D	10 JUN 2004	
	ANSO		
	ENTRY		
	FOR		
			Date of mailing (day/month/year)
			08.06.2004
Applicant's or agent's file reference P018298WO MJH		REPLY DUE within 3 month(s) from the above date of mailing	
International application No. PCT/GB 03/03917	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.			

- This written opinion is the first drawn up by this International Preliminary Examining Authority.
- This opinion contains indications relating to the following items:
 - ☒ Basis of the opinion
 - ☐ Priority
 - ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - ☐ Lack of unity of invention
 - ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - ☐ Certain documents cited
 - ☐ Certain defects in the international application
 - ☐ Certain observations on the international application
- The applicant is hereby invited to reply to this opinion.

When? See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also: For an additional opportunity to submit amendments, see Rule 66.4. For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis. For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.
- The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 10.01.2005

Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tlx 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Geiger, J-W Formalities officer (incl. extension of time limits) García Soló, J Telephone No. +49 89 2399-7949	
---	---	---

WRITTEN OPINION

International application No. **PCT/GB 03/03917**

I. Basis of the opinion

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 opinion as "originally filed"*):

Description, Pages

1-49 as originally filed

Claims, Numbers

1-76 as originally filed

Drawings, Sheets

1/13-13/13 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:

5. ☐ This opinion 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)).

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been and will not be examined in respect of:

☐ the entire international application,

☒ claims Nos. 2, 32

because:

☐ the said International application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (specify):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 2, 32 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos.

2. A written opinion cannot be drawn due to the failure of the nucleotide and/or amino acid sequence listing to comply with the Standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the Standard.

☐ the computer readable form has not been furnished or does not comply with the Standard.

V. Reasoned statement under Rule 68.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	no: 1, 3-6, 9, 16, 21, 24-31, 33, 34, 37-52, 54-67, 69-76;
-------------	--------	--

Inventive step (IS)	Claims	no: 7, 8, 10-15, 17-20, 22, 23, 35, 36, 53;
---------------------	--------	---

Industrial applicability (IA)	Claims	
-------------------------------	--------	--

2. Citations and explanations

see separate sheet

**WRITTEN OPINION
SEPARATE SHEET**

International application No. PCT/GB03/03917

Re Item III

Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

Claim 2 does not meet the requirements of Article 6 PCT in that the matter for which protection is sought is not clearly defined. The functional statements that

"said characteristic response is provided with a remeasured characteristic"

do not enable the skilled person to determine which technical features are necessary to perform the stated function.

This feature in the apparatus claim 2 relates to a method of manufacturing the apparatus rather than clearly defining the apparatus in terms of its technical features. The intended limitations are therefore not clear from this claim, contrary to the requirements of Article 6 PCT.

Since claim 32 refers to claim 2, claim 32 lacks clarity, too.

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents:

D1*: WO 02 50790

D2*: GB 1 601 362

* These documents were not cited in the International Search Report.
Copies of the documents are appended hereto.

2. The present application does not meet the criteria of Article 33(1) PCT, because

**WRITTEN OPINION
SEPARATE SHEET**

International application No. PCT/GB03/03917

the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

The document D1 discloses (the references in parentheses applying to this document):

A security device comprising two or more magnetic elements (cf. D1, fig. 11, 12, or 14), wherein said magnetic elements are responsive to an applied magnetic field to provide a characteristic response (cf. D1, page 24, 2nd paragraph).

3. Claims 3 - 31 and 33 - 76 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step.

3.1 The features added by the following dependent claims are known from D1:

as to claims 3:

"aggregate response", see D1, page 5, last paragraph - page 6, 1st paragraph (reading of the "image");

as to claims 4 - 6:

see D1, e.g. fig. 14;

as to claim 9:

see cf. D1, page 24, 2nd paragraph;

as to claim 16:

see D1, e.g. fig. 21;

as to claim 21:

see D1, page 42, paragraph f);

as to claims 24, 25:

see D1, e.g. fig. 14;

as to claims 26, 27:

**WRITTEN OPINION
SEPARATE SHEET**

International application No. PCT/GB03/03917

see D1, fig. 19, right upper corner;

as to claims 28 - 31:

see D1, page 42, paragraphs h) - j);

as to claims 33, 34:

the features of said claims do not extend beyond the features of claims 1, 3- 6 resp. in method terms, hence they are objectionable on the same reasons as claims 1, 3 - 6.

as to claims 37 - 39:

see D1, page 4, last paragraph - page 5, 1st paragraph, page 24, 2nd paragraph; "measurement" via the analysis of the image pattern;

as to claims 40 - 45:

see D1, page 31, 2nd paragraph;

as to claims 46, 47, 49 - 52, 54 - 60:

see D1, page 24, 2nd paragraph; page 27, 2nd paragraph - page 28, 2nd paragraph; page 42; fig. 9, 17, 19;

as to claim 48:

in D1 the magnetic field is switched on/off for analyzing the images, hence the magnetic field varies in time as claimed;

as to claims 75, 76:

see D1, fig. 18.

- 3.2** The features of following claims do not add any inventive step since they are either straightforward design alternatives which would be within the abilities of a skilled person in the field of forming security devices or can be derived without inventive efforts by combining D1 with document D2.

as to claims 7, 8:

standard dimensions in the field of layered security devices;

**WRITTEN OPINION
SEPARATE SHEET**

International application No. PCT/GB03/03917

as to claims 10 - 12:

the claimed materials are some of several straightforward possibilities from which the skilled person would select, see e.g. D2, page 2, line 104 - page 3, line 61;

as to claims 13 - 15:

combining D1, page 44, paragraph t) with D2, fig.2 would directly lead without applying an inventive step to the features of said claims;

as to claims 17 - 20:

their features are already disclosed by D2, fig. 2. It would be obvious to apply these features in the device of D1;

as to claims 22, 23:

design alternatives of the device of D1 which do not justify an inventive step;

as to claims 35, 36:

these features are standard technology processes from which the skilled person would select to realize a security device;

as to claim 53:

the feature of said claim is one of several straightforward alternatives from which the skilled person would select when using the Kerr effect.

3.3 The features of claims 61 - 74 do not extend beyond the features of claims 46 - 60 resp. in method terms.

Hence, the subject-matter of claims 61 - 74 does not fulfill the requirements of Articles 33(2)(3) PCT, resp..

TRATADO DE COOPERACION DE PATENTES

De
LA AUTORIDAD INTERNACIONAL DE EXAMEN PRELIMINAR

Para:

HAINES, MILES JOHN
D. YOUNG & CO.
21 New Fetter Lane
Londres EC4A 1DA
GRAN BRETAÑA

PCT

OPINION ESCRITA
(PCT Regla 66)

Fecha de Correo
(día/mes/año)

28/12/2004

Archivo de referencia del solicitante o
del agente

P018298WO MJH

FECHA DE RESPUESTA

tres (3) meses contados a partir de la fecha de correo
arriba citada

Solicitud Internacional No.

PCT/GB 03/03917

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 19/08

Solicitante:

INGENIA HOLDINGS LIMITED et al.

1 Este es el primer (primero, etc.) redactado por esta Autoridad Examinadora Preliminar Internacional.

2 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 la regla 66.2(a)(ii) 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

3 Se invita aquí al solicitante para que de respuesta a este informe.

Cuándo? Ver arriba el tiempo límite indicado

Cómo? Entregando respuesta al informe, adjuntando, cuando sea apropiado, correcciones de acuerdo con la regla 66.3 en el formato y el idioma de las modificaciones, ver regla 66.8 y 66.9.

También Para otra oportunidad presentar correcciones, ver regla 66.4

Es obligación del examinador considerar correcciones y/o argumentos, ver regla 66.4 bis

Para una comunicación informal con el examinador, ver regla 66.6

Si no se presenta respuesta, el reporte de Examen Preliminar Internacional se establecerá con base en este informe.

4 La fecha final por la cual el informe del examen preliminar deberá establecerse, de acuerdo a la regla 69.2 es:
10/01/2005

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

Tel.: +49 89 2399 - 0 Tx: 523858 epmu d
Fax.: +49 89 2399 - 4485

Funcionario autorizado
Gelger, J-W

Oficina de Formalidades
(Incl. Extensión de limitación de tiempo)
García Solé, J

Tel.: (+49-89) 2399 7949

OPINION ESCRITA

**Solicitud Internacional No.
PCT/GB 03/03917**

I. Base de la opinión

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"):

Descripción, páginas:

1 - 49 como se presentaron originalmente

Reivindicaciones Nos.:

1 - 76 como se presentaron originalmente

Dibujos, páginas:

1/13 - 13/13 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 _____ 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.

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)).

6 Observaciones adicionales, si es necesario:

OPINION ESCRITA

**Solicitud Internacional No.
PCT/GB 03/03917**

III. No-establecimiento de opinión con respecto a la novedad, nivel inventivo y aplicación Industrial

La pregunta de si la invención reclamada parece ser novedosa, posee nivel inventivo (no ser obvia), o tener aplicación Industrial no ha sido ni será examinada con respecto de:

Las reivindicaciones 2, 32

La descripción, reivindicaciones o dibujos (indican abajo elementos particulares) o dichas reivindicaciones 2, 32 no son claras y ninguna opinión significativa puede darse (específica):

ver hoja separada

V. Declaración razonada bajo la Regla 68.2(a)(II) con relación a la novedad, altura inventiva o aplicación Industrial: citas y explicaciones que apoyan tal declaración.

1 Declaración

Novedad (N)	Reivindicaciones No.	1,3-8,9,16,21,24-31,33,34,37-52,54-67,69-76;
Altura inventiva (IS)	Reivindicaciones No.	7,8,10-15,17-20,22,23,35,36,53;
Aplicación industrial (IA)	Reivindicaciones	

2 Citas y explicaciones

Ver hoja separada

OPINION ESCRITA-HOJA ANEXA
Solicitud Internacional No. PCT/GB 03/03917

Numeral III

No establecimiento de opinión con respecto a la novedad, nivel inventivo y aplicación industrial.

La reivindicación 2 no cumple con los requerimientos del Artículo 6 del PCT ya que no está claramente definida la materia para la cual se busca protección. Las afirmaciones funcionales que

"dicha respuesta característica suministra....con una característica remedida"

No permiten a una persona conocedora del arte determinar que características técnicas son necesarias para ejecutar la función establecida.

Esta característica en el aparato de la reivindicación 2 se relaciona con un método para fabricar el aparato en vez de definir claramente el aparato en términos de sus características técnicas. Las limitaciones que se intentan, no son por lo tanto claras en esta reivindicación, contrario a los requerimientos del Artículo 6 del PCT.

Como la reivindicación 32 se refiere a la reivindicación 2, la reivindicación 32 también carece de claridad.

Numeral V

Declaración razonada de conformidad con la Regla 66.2 (a) (ii) con relación; citaciones y explicaciones que apoyan tal declaración.

1. Se hace referencia a los siguientes documentos:

D1*: WO 0250790

D2*: GB 1601362

*estos documentos no fueron citados en el informe de búsqueda internacional. Se anexan copias de los documentos.

2. La presente solicitud no cumple con los criterios del Artículo 33 (1) PCT ya que materia de la reivindicación 1 no es nueva en el sentido del Artículo 33 (2) PCT.

El documento D1 revela (las referencias en paréntesis aplican a este documento):

Un dispositivo de seguridad que comprende dos o más elementos magnéticos (ver D1, fig.11,12, o 14), donde dichos elementos magnéticos son sensibles a un campo magnético aplicado para proporcionar una respuesta característica. (ver D1, página 24, segundo párrafo).

3. Las reivindicaciones 3-31 y 33-76 no contienen características que, en combinación con las características de cualquier reivindicación a la cuales están referidas, cumplan con los requerimientos del PCT con respecto a la novedad y/o nivel inventivo.

3.1 Las características adicionales son conocidas de D1, por las siguientes reivindicaciones dependientes:

Para la reivindicación 3:

"respuesta agregada", ver D1, página 5, último párrafo- página6, primer párrafo (lectura de la "imagen");

Para las reivindicaciones 4-6: ver D1, ejemplo, figura 14;

Para la reivindicación 9: ver D1, página 24, segundo párrafo;

Para la reivindicación 16:

Ver D1, ejemplo fig 21;

Para la reivindicación 21: ver D1, página 42, párrafo f);

Para las reivindicaciones 24,25: Ver D1, ejemplo figura 14;

Para las reivindicaciones 26, 27: ver D1, fig. 19, esquina superior derecha;

Para las reivindicaciones 28-31: ver D1, página 42, párrafos h)-j));

Para las reivindicaciones 33-34: las características de dichas reivindicaciones no van más allá de las características de las reivindicaciones 1,3-6 respectivamente, en los términos del método, por lo tanto, estos se objetan por las mismas razones de las reivindicaciones 1,3-6.

Para las reivindicaciones 37-39: ver D1, página 4, último párrafo-página 5, primer párrafo, página 24, segundo párrafo; "medición" por el análisis del patrón de imagen.

Para las reivindicaciones 40-45: ver D1, página 31, segundo párrafo;

Para las reivindicaciones 46, 47,49-52,54-60: ver D1, página 24, segundo párrafo; página 27- página 28, segundo párrafo; página 42; figura 9, 17,19.

Para las reivindicación 48: ver en D1, el campo magnético se cambia de encendido/apagado para el análisis de imágenes, por lo tanto, el campo magnético como reivindicado varía en el tiempo.

Para las reivindicaciones 75,76: ver D1, figura 18.

3.2 Las características de las siguientes reivindicaciones no aportan nada inventivo ya que estas son alternativas tanto directas de diseños que están dentro de las habilidades de una persona conocedora del arte en el campo de formar dispositivos de seguridad o pueden derivarse sin ningún esfuerzo inventivo por la combinación de D1 y D2.

Para las reivindicaciones 7, 8: dimensiones estándares en el campo de los dispositivos de seguridad por capas.

Para las reivindicaciones 10-12: los materiales reivindicados son de las muchas posibilidades directas que un conocedor del arte seleccionaría, ver, por ejemplo. D2, página 2, línea 104-página 3, línea 61;

Para las reivindicaciones 13-15: combinando D1, página 44, párrafo t) con D2, figura 2 conduciría directamente a las características de dichas reivindicaciones sin aplicar nivel inventivo.

Para las reivindicaciones 17-20: sus características ya han sido reveladas por D2, figura 2. Sería obvio aplicar éstas características en el dispositivo de D1;

Para las reivindicaciones 22-23: alternativas del diseño del dispositivo de D1, lo que no justifica el nivel inventivo;

Para las reivindicaciones 35,36: Estas características son estándares de los procesos de tecnología de los cuales una persona del arte seleccionaría para realizar el dispositivo de seguridad.

Para la reivindicación 53: la característica de dicha reivindicación es una de las muchas alternativas directas de las cuales una persona del arte seleccionaría cuando se usa el efecto Kerr.

3.3 Las características de las reivindicaciones 61-74 no van más allá de las características de las reivindicaciones 46-60 respectivamente. En términos del método.

Por lo tanto, el contenido de las reivindicaciones 61-74 no cumple con los requerimientos de los artículos 33 (2) (3) del PCT respectivamente.