

REIVINDICACIONES

1. Un método implementado por computadora para certificar un documento de seguridad (10), comprendiendo:

proporcionar un documento de seguridad (10) manufacturado por una pluralidad de diferentes procesos o etapas, que proporcionan al documento un número correspondiente de elementos, teniendo tal documento de seguridad (10) una variación en el registro de elementos única con respecto de otros documentos de seguridad también manufacturados con los mismos procesos;

seleccionar, vía procesadores, un área determinada del documento que tiene un conjunto de características únicas de registro de dichos elementos o la posición relativa entre dichos elementos;

obtener una imagen digital de un documento de seguridad (10);

obtener los datos (20) del conjunto de elementos de la área determinada del documento que tiene características únicas de registro;

obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos (20) de la ID del documento;

construir un mensaje con una función de hash (40), en donde el mensaje de hash (50) es el mensaje obtenido después de ser codificado por medio de una función de hash (40) criptográfica unidireccional;

encriptar el mensaje de hash (50) utilizando una clave privada (70) en un sistema criptográfico de clave pública (60) para obtener un certificado digital (80); y

almacenar el certificado digital (80) obtenido en una base de datos (90) externa.

2. El método para certificar un documento de seguridad (10) de conformidad con la reivindicación 1, en donde el certificado digital (80) se marca o imprime (97) en el documento de seguridad (10).

3. El método para la certificación de acuerdo con la reivindicación 1, en donde la imagen digital es tomada con luz con una longitud de onda entre 200 y 1500 nanómetros.

4. El método para la certificación de acuerdo con la reivindicación 1, en donde la imagen digital es tomada con luz visible.

5. El método para la certificación de acuerdo con la reivindicación 1, en donde varias partes del mismo documento son certificadas independientemente.

6. El método para la certificación de acuerdo con la reivindicación 1, en donde el documento de seguridad (10) es un billete, un cheque, un pasaporte o un certificado de nacimiento.

7. El método para certificar un documento de seguridad (10) de acuerdo con la reivindicación 1, en donde los datos (20) se obtienen durante la línea de producción.

8. El método para certificar un documento de seguridad (10) de acuerdo con la reivindicación 1, en donde los datos (20) se obtienen durante la inspección de calidad.

9. Un método de autenticación de un documento de seguridad (10) comprendiendo los pasos de:

documento de seguridad (10) documento de seguridad (10)

recibir por parte de un usuario, una una imagen digital de un documento de seguridad (10), presuntamente manufacturado por una pluralidad de diferentes procesos o etapas, que proporcionan al documento un número correspondiente de elementos, teniendo tal documento de seguridad (10) una variación en el registro o posición relativa de elementos única;

obtener datos (20) de un conjunto de elementos de una área determinada del documento que tiene características únicas de registro,

obtener una medida del registro del conjunto determinado de elementos del documento y los datos (20) de la ID del documento,

aplicar una función de hash (40) para obtener un mensaje de hash (50) para la verificación,

obtener y descryptar un mensaje certificado con una función de hash (40) almacenado, para el documento de seguridad (10) certificado, y

autenticar el documento comparando el mensaje certificado con una función de hash (40) y el mensaje con una función de hash (40) para la verificación, en donde si el mensaje certificado con una función de hash (40) y el mensaje con una función de hash (40) para la verificación es una coincidencia, el documento se considera como genuino, si el mensaje certificado con una función de hash (40) y el mensaje con una función de hash (40) para la verificación no coinciden, el documento se considera como una falsificación.

10. El método para la autenticación de un documento de seguridad (10) de conformidad con la reivindicación 9, en donde el mensaje certificado con una función de hash (40) se obtiene del certificado digital (80) marcado o impreso en el documento de seguridad (10), el certificado digital (80) se descrypta a través del uso de una clave pública para interpretar un mensaje con una función de hash (40) para la referencia.

11. El método para la autenticación de un documento de seguridad (10) de conformidad con la reivindicación 9, en donde el mensaje certificado con una función de hash (40) se obtiene accediendo a la base de datos (90).

12. El método para la autenticación de acuerdo con la reivindicación 9, en donde las materias primas son verificadas via análisis de imagen y métodos de patrón de reconocimiento.

13. El método para la autenticación de acuerdo con la reivindicación 9, en donde el documento de seguridad (10) es un billete.

14. El método para la autenticación de acuerdo con la reivindicación 9, en donde el documento de seguridad (10) es un billete con un sustrato conteniendo marcas de agua, o un hilo de seguridad, o una lámina o una ventana transparente o fibras fluorescentes.

15. El método para la autenticación de acuerdo con la reivindicación 9, en donde el billete se imprime utilizando impresión en offset e impresión intaglio.

16. El método para la autenticación de un documento de seguridad (10) de acuerdo con la reivindicación 9, en donde la autenticación se realiza por escáneres o cámaras digitales comercialmente disponibles conectados a computadoras.

17. El método para la autenticación de un documento de seguridad (10) de acuerdo con la reivindicación 9, en donde la autenticación se realiza mediante teléfonos inteligentes o tabletas.

18. El método para la autenticación de un documento de seguridad (10) de acuerdo con la reivindicación 9, en donde la autenticación se realiza mediante equipo de procesamiento de billetes.

Señor

Director de la Dirección de Nuevas Creaciones

Superintendencia de Industria y Comercio

Ministerio de Comercio, Industria y Turismo

E. S. D.

Re.: Expediente No. **NC2017/0007331**

Solicitud de Patente PCT entrada en Fase Nacional, para:

"MÉTODO PARA CERTIFICAR Y AUTENTIFICAR DOCUMENTOS DE SEGURIDAD BASÁNDOSE EN UNA MEDICIÓN DE LAS VARIACIONES DE LA POSICIÓN RELATIVA DE LOS DIFERENTES PROCESOS INVOLUCRADOS EN SU FABRICACIÓN"

Solicitante: **BANCO DE MÉXICO**

RESPUESTA A EXAMEN DE FONDO

Yo, **MARGARITA CASTELLANOS ABONDANO**, mayor de edad, identificada y domiciliada como aparece al pie de mi firma, obrando en mi calidad de apoderada de la sociedad solicitante del asunto citado en la referencia, en atención a su oficio No. **5489** notificado el **4 de mayo de 2018**, atentamente me permito dar respuesta al mismo de la siguiente manera:

1. Objeto de la invención.

El objeto de la invención, como lo establece el Examinador consiste en:

"...El problema planteado en esta solicitud consiste en la necesidad de suministrar un método para certificar los documentos de seguridad como requisito para un proceso confiable y rápido para autenticar documentos. Para resolver este problema técnico, la solicitud en estudio proporciona métodos para certificar y autenticar documentos de seguridad. La certificación comprende las etapas de

a) seleccionar un conjunto de características únicas, obtenidas como resultado de las variaciones en el proceso de fabricación y los suministros,

b) obtener una imagen digital de un documento de seguridad y obtener los datos de la posición relativa entre los elementos seleccionados de diferentes procesos de fabricación (registro),

c) construir un mensaje midiendo el registro de los elementos seleccionados del documento y los datos de la ID del documento,

- d) construir un mensaje de hash, siendo este el mensaje obtenido después de ser codificado por medio de una función de hash criptográfica unidireccional,
- e) encriptar el mensaje de hash utilizando un sistema criptográfico de clave pública para obtener un certificado digital, por medio de una clave privada, y
- f) almacenar el certificado digital en una base de datos externa...”

Es importante señalar que la característica esencial de la invención consiste en la selección de las características únicas que son el resultado de las variaciones en el proceso de fabricación y las variaciones en los suministros. Se considera que dicha característica no está comprendida en el estado de la técnica citado, ni es evidente para una persona versada en la materia y por tanto, la invención debe considerarse inventiva.

2. En relación con las objeciones a la claridad de las reivindicaciones

De acuerdo con el Examinador, las reivindicaciones 9, 14 y 18 no son claras, debido a que poseen términos generales que no permiten establecer un concepto suficiente de la invención que se está reclamando. Los términos objetados son:

- “(...) documento (...)” Reiv. 9
- “(...) lámina (...)” Reiv. 14
- “(...) ventana transparente (...)” Reiv. 14
- “(...) equipo de procesamiento de dinero en efectivo (...)” Reiv. 18

Además, el Examinador afirma que las reivindicaciones 1, 9, 14 y 15 no son claras, debido a que se presentan términos imprecisos por lo cual no permiten distinguir la invención del estado de la técnica.

- “uno o más” Reivindicación 1 y 9
- “tales como” Reivindicación 1
- “al menos” Reivindicación 14 y 15

Respetuosamente, mi representada desea poner de presente que no comparte la opinión del Examinador, considerando el campo técnico y el problema que busca resolver la presente invención. En particular, vale la pena resaltar que la definición de las características únicas está dada en la página 11 línea 21 a página 12 línea 4; páginas 15, líneas 4 a 8. En tanto que la etapa de selección del conjunto de

características está descrita en detalle en los párrafos de la página 17 línea 25 a la página 20 línea 2, y se encuentra además ilustrada en las figuras 2 y 3.

De tal manera que la expresión “*seleccionar un conjunto de características únicas en donde las características únicas están relacionadas a las variaciones en el proceso de fabricación y los suministros para manufacturar documentos de seguridad*” es clara a la luz de la descripción. Pues las características únicas tienen que ver con las posiciones relativas o “registro” que ocupan los elementos impresos o derivados de los insumos en el documento final.

No obstante lo anterior, con objeto de hacer más clara las reivindicaciones, la reivindicación 1 ha sido enmendada de la siguiente manera:

1. Un método implementado por computadora para certificar un documento de seguridad (10), comprendiendo:

proporcionar un documento de seguridad (10) manufacturado por una pluralidad de diferentes procesos o etapas, que proporcionan al documento un número correspondiente de elementos, teniendo tal documento de seguridad (10) una variación en el registro de elementos única con respecto de otros documentos de seguridad también manufacturados con los mismos procesos;

seleccionar, vía procesadores, un área determinada del documento que tiene un conjunto de características únicas de registro de dichos elementos o la posición relativa entre dichos elementos;

obtener una imagen digital de un documento de seguridad (10);

obtener los datos (20) del conjunto de elementos de la área determinada del documento que tiene características únicas de registro;

obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos (20) de la ID del documento;

construir un mensaje con una función de hash (40), en donde el mensaje de hash (50) es el mensaje obtenido después de ser codificado por medio de una función de hash (40) criptográfica unidireccional;

encriptar el mensaje de hash (50) utilizando una clave privada (70) en un sistema criptográfico de clave pública (60) para obtener un certificado digital (80); y

almacenar el certificado digital (80) obtenido en una base de datos (90) externa.

Con dicha modificación, se han especificado las características a medir.

3. En relación con el estado de la técnica coitado por el Examinador

El Examinador ha señalado que:

El documento D1 (WO-01/91007A1) divulga un sistema y método para autenticar documentos y contenido de los mismos. Se proporciona un medio de grabación de documentos resistente a la falsificación, que tiene un identificador de documento único predefinido y al menos una característica de seguridad (Fl. 1, resumen).

Me permito observar que el D1 (página 34, tercer párrafo) describe un método para fabricar documentos que tienen marcas que no sean fácilmente reproducibles.

Thus, there remains a need for a system and method for efficiently authenticating documents as being unaltered originals, while providing high throughput document production. In addition, there remains a need for a method and system for marking documents such that the markings are not readily reproducible with commonly available technologies and so that the markings contain sufficient information for document authentication, identification, and verification. Heretofore, such systems have had various shortcomings.

(Traducción): Así, permanece una necesidad de un sistema y método para autenticar de manera eficiente documentos como originales inalterados, mientras que se proporciona alta producción de documentos de alto rendimiento. Además, permanece una necesidad de un método y sistema para hacer documentos de tal manera que las marcas no sean fácilmente reproducibles con tecnologías comúnmente disponibles y de manera que la marcas contengan suficiente información para la autenticación del documento, identificación y verificación. Hasta ahora, tales sistemas han tenido varios defectos

A diferencia del arte previo citado, la presente invención no incluye agregar marcas al documento.

En D1 la autenticación se consigue por una marca que se denomina “*Apparently non deterministic characteristics of a recording médium of the document*” (características aparentemente no-determinísticas de un medio de registro del documento).

Dichas “*características aparentemente no-determinísticas*” se refieren a una representación en tres colores. En la página 54 primer y segundo párrafo se describen algunas características de las “*características aparentemente no-determinísticas*”:

“...The apparently non-deterministic characteristic may, for example, comprises one or more characteristics selected from the group consisting of: a pseudorandom imprint pattern, a non-deterministic pattern of elements comprising the media, an interaction of an aliquot of liquid dye with non-deterministic pattern of elements comprising the media, and a non-deterministic pattern of an imprint on the medium.

The apparently non-deterministic characteristic comprises, for example, a feature that is incompletely represented in a tri color representation, e.g., RGB, MCY, YUV, CIE 1931, etc. Thus, the feature may include, for example, non-optically detectable features, such as a magnetic or thermal signature, an optical characteristic which involves a narrowband spectral analysis or more than three color bands, or an optical characteristic relating to optical polarization.”

(TRADUCCIÓN: La característica aparentemente no determinística puede, por ejemplo comprende una o más características seleccionadas del grupo que consiste de: un patrón impreso pseudo-aleatorio, un patrón no-determinístico de elementos que comprenden el medio. Una interacción de una alícuota de tinta líquida con patrones no determinísticos de elementos que comprenden el medio y un patrón no determinístico de un impreso en el medio.

Las características aparentemente no determinísticas, comprenden por ejemplo una característica que esta incompletamente representada en una representación de tres colores, por ejemplo RGB, MCY, YUV, CIE 1931, etc. Así, la característica puede incluir por ejemplo, características ópticas no detectables, tales como firmas magnéticas o térmicas, una característica óptica que involucre un análisis espectral de banda angosta o bandas de más de tres colores, o una característica óptica relativa a la polarización óptica”

En el Ejemplo 1 de D1, dicha característica aparentemente no determinística consiste de la orientación y posición de fibras dicróicas fluorescentes. incorporadas al papel.

En el Ejemplo 2 de D1, dicha característica aparentemente no determinística consiste de un “identificados esencialmente único fácilmente verificable” impreso en el documento que consiste de una porción serializada y una porción aleatoria.

D1 es claramente omiso en señalar las variaciones naturales de la posición de los elementos debidos a los procesos de manufactura como la característica que permite la autenticación del documento.

Respecto del documento D2 (US-2006/0021065A1), el examinador menciona que:

“El documento D2 divulga métodos y dispositivos para autorizar una operación solicitada por un primer usuario en un elemento de contenido de acuerdo con un derecho de usuario (Fl. 1, resumen).”

La presente invención nada tiene que ver con métodos y dispositivos para autorizar a un primer usuario.

De acuerdo con la reivindicación 1 de D2, en D2 se describe

1. A method of authorizing an operation requested by a first user on a content item in accordance with a user right identifying a second user and authorizing the second user to perform the requested operation on the content item, in which the operation is authorized upon receipt of information linking a user right of the first user and the user right of the second user.

(Traducción: Un método para autorizar una operación solicitada por un primer usuario en un artículo contenido conforme a un derecho de usuario identificando un segundo usuario y autorizando al segundo usuario a realizar la operación solicitada en el artículo contenido, en el cual la operación se autoriza una vez que se recibe información que liga un derecho de usuario del primer usuario y el derecho de usuario del segundo usuario

La presente invención nada tiene que ver con derechos de usuarios para realizar operaciones en sistemas computacionales.

Respecto del D3 (WO-2009/150622A2), El examinador menciona que:

El documento D3 divulga un marcado encriptado y un método de protección, verificación y certificación de la autenticidad de los productos por medio de un marcado encriptado único que contiene una gran cantidad de información encriptada incrustada en cada elemento muy pequeño del marcado, que está protegido y que se puede recuperar en caso de desgaste, contaminación o eliminación (Fl. 1, resumen).

D3 se refiere también a un método de autenticar por medio de la inclusión de marcas. D3 es claramente omiso en señalar las variaciones naturales de la posición de los elementos debidos a los procesos de manufactura como la característica que permite la autenticación del documento, de acuerdo con la presente invención.

4. En relación con la supuesta falta de nivel inventivo de la invención.

La reivindicación 1 de la presente solicitud requiere que el método incluya las siguientes etapas:

proporcionar un documento de seguridad manufacturado por una pluralidad de diferentes procesos o etapas, que proporcionan al documento un número correspondiente de elementos, teniendo tal documento de seguridad una variación en el registro de elementos única con respecto de otros documentos de seguridad también manufacturados con los mismos procesos;

seleccionar, vía uno o más procesadores, una área determinada del documento que tiene un conjunto de características únicas de registro de dichos elementos ó la posición relativa entre dichos elementos;

obtener una imagen digital de un documento de seguridad;

obtener los datos de un conjunto de elementos de una área determinada del documento que tiene características únicas de registro;

obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos de la ID del documento;

Es decir, conforme a la presente invención la autenticación se realiza con bases a las características únicas de REGISTRO del documento, o sea la posición de los elementos del documento que es el resultado del proceso de fabricación. El registro es una característica única de cada documento. Conforme a la presente invención, NO SE ADICIONA NINGÚN ELEMENTO DISTINTIVO AJENO DEL DOCUMENTO.

D1 claramente es omiso respecto de un proceso de autenticación que utilice la variabilidad de registro o posición relativa de los elementos dispuestos en el documento que son el resultado de sus respectivos procesos o etapas de manufactura.

Claramente D1 es omiso respecto de las etapas de:

seleccionar, vía uno o más procesadores, una área determinada del documento que tiene un conjunto de características únicas de registro de dichos elementos ó la posición relativa entre dichos elementos;

obtener una imagen digital de un documento de seguridad;

obtener los datos del conjunto de elementos de la área determinada del documento que tiene características únicas de registro;

obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos de la ID del documento;

El arte previo citado falla en describir todas y cada una de las características antes indicadas.

En virtud de lo antes expresado, debe considerarse que la invención es novedosa y resultado de una actividad inventiva, por lo que dicho requerimiento debe ser desestimado.

El Examinador considera que el documento D1 es el estado de la técnica más cercano a la invención definida en la reivindicación 1, un sistema y método para autenticar documentos y contenido de los mismos. Se proporciona un medio de grabación de documentos resistente a la falsificación, que tiene un identificador de documento único predefinido y al menos una característica de seguridad (Fl. 1, resumen). “

El Examinador ha manifestado que:

La diferencia entre la invención, definida en la reivindicación 1 y el sistema de D1 consiste en que el método de la reivindicación 1 posee almacenar el certificado digital en una base de datos externa.

Tal interpretación es errónea. La diferencia entre el estado de la técnica contenido en D1 y la presente invención radica en que los datos de autenticación provienen de las variaciones naturales en la posición de los elementos debidos a los procesos de manufactura.

El Examinador señala que:

“Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: *“¿Cómo modificar el sistema conocido en D1 para lograr evitar la falsificación de los documentos de seguridad?”*.

Sin embargo, la utilización del almacenar el certificado digital en una base de datos externa, ya está divulgada en el documento D2 que se refiere a que el dispositivo D1 obtiene un derecho de usuario, preferiblemente incorporado como un certificado digital, desde una base de datos remota URDB en Internet y lo almacena en el medio de almacenamiento local UR (Pág. 4, Fl. 7, Párr. 056). ”

Almacenar el certificado digital en una base de datos, no es la solución al problema técnico abordado por la presente invención. La solución al problema es

seleccionar, vía uno o más procesadores, una área determinada del documento que tiene un conjunto de características únicas de registro de dichos elementos ó la posición relativa entre dichos elementos;

obtener una imagen digital de un documento de seguridad;

obtener los datos del conjunto de elementos de la área determinada del documento que tiene características únicas de registro;

obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos de la ID del documento;

El Examinador concluye que:

“ En consecuencia, la persona del oficio normalmente versada en la materia, incluiría el certificado digital almacenado en la base de datos remota del documento D2 en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 1 de la solicitud. Por lo cual se considera obvia.

El efecto que logra el incluir el almacenar el certificado digital en una base de datos externa es poder evitar la falsificación de los documentos de seguridad.”

La Persona del oficio normalmente versada en la materia, no encontraría en D1 alguna sugerencia para utilizar las variaciones en el registros de los elementos impresos en el documento para establecer la autenticidad de un documento. En efecto, una Persona del oficio normalmente versada en la materia no encontraría en D1, D2 o D3 alguna sugerencia que le llevara a obtener una imagen digital de un documento de seguridad y obtener los datos de un conjunto de características relativas a la posición relativa entre uno o más elementos.

5. Conclusión

Teniendo en cuenta las modificaciones introducidas en esta oportunidad y los argumentos que se presentan, es posible establecer que las reivindicaciones cumplen con los requerimientos de la Decisión 486.

6. Anexos

- Nuevo pliego reivindicatorio conformado por 18 reivindicaciones.
- Nuevo pliego descriptivo incluyendo números de referencia

Señor Director,



Margarita Castellanos Abondano

C.C. No. **39.779.654** de Bogotá

T.P.A. No. **70.819** del C.S.J.

Calle 94A No. 7A-09 - Bogotá, D.C.

Teléfono: 7560770

Bogotá, D.C.

MCA/mg

P4715

**MÉTODO PARA CERTIFICAR Y AUTENTIFICAR DOCUMENTOS DE
SEGURIDAD BASÁNDOSE EN UNA MEDICIÓN DE LAS VARIACIONES DE
LA POSICIÓN RELATIVA DE LOS DIFERENTES PROCESOS
INVOLUCRADOS EN SU FABRICACIÓN**

5

ANTECEDENTES DE LA INVENCION

1. Campo de la Invención

Esta descripción se relaciona con un proceso para la certificación y autenticación de documentos de seguridad. De manera específica, se refiere
10 al uso de los elementos de seguridad y las características únicas, que ya están presentes en los documentos de seguridad, con el fin de certificar y autenticar este tipo de documentos. De forma más particular, se relaciona con la certificación y autenticación de billetes, cheques o cualesquiera otros documentos de seguridad, por medio de la utilización de las variaciones
15 naturales durante el proceso de producción, que es cuando los procesos de impresión, los elementos de seguridad y otras características son incorporadas al documento.

2. Antecedentes de la invención

20 Debido al avance notable en las tecnologías existentes para la reproducción gráfica que están comúnmente disponibles en el mercado, la aparición de falsificaciones de buena calidad de documentos de seguridad tales como cheques, billetes, etc., está en aumento. Por lo tanto, un método de certificación y autenticación para los documentos de seguridad utilizando
25 métodos que puedan soportar el avance tecnológico del equipo gráfico y que

haga uso de dispositivos disponibles comúnmente, tales como escáneres y equipos con cámaras digitales, es de máxima importancia.

Además, el crimen organizado ha encontrado una manera de utilizar estas tecnologías profesionales para producir grandes volúmenes de falsificaciones de alta calidad, este hecho compromete la credibilidad que la sociedad tiene en la institución emisora, y su capacidad para proporcionar un instrumento confiable para detectar falsificaciones.

Los métodos de autenticación conocidos comúnmente enfocados en la verificación, dependen de procesos y sistemas que a su vez requieren equipos diseñados con características específicas para verificar la autenticidad de un elemento de seguridad del documento, en donde la dificultad proviene ya sea del alto costo del equipo o del material especial que se requiere. Como ejemplo tenemos la inclusión de materiales magnéticos, tintas fluorescentes UV, pigmentos que absorben zonas del espectro infrarrojo, sistemas de respuesta óptica dinámica tales como decaimiento de la fosforescencia, bandas magnéticas y hologramas que son incluidos en los documentos de seguridad. Desafortunadamente, los criminales también están utilizando métodos que son más sofisticados, y con la facilidad del acceso a la información que existe actualmente, es posible imitar casi cualquier elemento de seguridad que los fabricantes hayan incorporado en los documentos por medio de materiales y equipos disponibles comercialmente. La falsificación de los documentos puede abarcar falsificaciones basadas en sistemas que utilizan impresoras láser o de inyección de tinta (falsificación del tipo fotocopia) y falsificaciones que utilizan procesos y materiales similares a los auténticos (falsificaciones industriales). En el caso de las falsificaciones del tipo fotocopia, los bancos centrales incluyen elementos especiales que las impresoras no pueden imitar, por ejemplo, marcas de agua, hilos magnéticos, ventanas transparentes y relieve grabado con propiedades táctiles, hologramas y elementos y tintas ópticamente

variables que cambian con el ángulo de visión. En el caso de las falsificaciones industriales, la autenticidad es difícil de determinar mediante la simple verificación de un usuario no entrenado. Además, para el caso particular de la falsificación de billetes, esto tiene un alto impacto en las finanzas de una nación. Actualmente, los esfuerzos para contrarrestar tales falsificaciones se enfocan en los materiales y tintas para ser utilizados en la fabricación de los nuevos documentos de seguridad, tratando de evitar que tengan un alto riesgo de volverse comercialmente disponibles durante la vida pretendida del documento, con el fin de evitarlos. En general, el enfoque estándar requiere prever si la brecha entre las tecnologías comercialmente disponibles y aquéllas que se pretenden utilizar para los documentos de seguridad se está cerrando debido al inevitable progreso tecnológico.

En el caso de las divisas tales como los dólares de los Estados Unidos y los Euros, que se utilizan en muchos países, el riesgo de falsificación se incrementa, puesto que esto abre una oportunidad para los criminales de otros países, incluyendo las organizaciones criminales apoyadas por el estado.

Por lo tanto, sería deseable que la autenticidad de un documento de seguridad (10) no sólo dependa del hecho de que los materiales y procesos originales sean difíciles, pero no imposibles de falsificar; sino también de la seguridad matemáticamente probada, tal como la de un certificado digital (80).

Por otra parte, en el caso de los billetes que son utilizados de manera extensa para las transacciones diarias, se requiere la determinación inmediata de su autenticidad. Como un ejemplo, si una persona durante una transacción falla en reconocer una falsificación, esto resultará en una pérdida, puesto que recibirá un documento sin valor, entregará una mercancía valiosa y en algunos casos, proporcionará el cambio en efectivo, cuando los valores de la mercancía son menores que el valor de la falsificación. De forma que es necesario autenticar rápidamente los documentos de seguridad, tales como los cheques

y billetes, para evitar la entrada de tal documento falsificado en la economía nacional que afecta al público en general, y mantener la confianza en las instituciones emisoras.

5 Las pruebas forenses son muy exactas para determinar si un documento es auténtico o no, sin embargo, el tiempo que toma procesar un sólo documento es muy largo, y usualmente requiere equipo especializado y costoso. Por otra parte, las computadoras y los dispositivos están presentando un aumento en la calidad de adquisición de imagen y en la capacidad de cómputo, asimismo, se están volviendo más populares y económicamente más
10 accesibles para las personas y empresas. Así, sería deseable autenticar documentos de seguridad mediante el uso de la tecnología actualmente disponible para la adquisición de una imagen digital en los dispositivos como teléfonos inteligentes o escáneres conectados a las computadoras, que puedan analizar los datos (20) para verificar la autenticidad de un documento de seguridad (10), particularmente en el caso de los billetes.
15

También se ha reconocido en el campo de pruebas de documentos de seguridad, que debe encontrarse un equilibrio entre los objetivos en conflicto de “aceptación” y “rechazo”. Siendo una aceptación positiva, la capacidad de autenticar de manera correcta -identificar y aceptar- todos los documentos de
20 seguridad auténticos sin importar su condición, y un rechazo positivo siendo la capacidad de discriminar y rechazar de manera correcta todos los documentos de seguridad no auténticos. Sin embargo, es posible caer en una aceptación negativa, cuando un documento no auténtico se acepta como auténtico; y un rechazo negativo, cuando un documento auténtico se considera como una
25 falsificación y se rechaza. Es necesario que el proceso de autenticación tenga un alto nivel de exactitud con respecto a estas definiciones, evitando las aceptaciones negativas y los rechazos negativos.

La Solicitud de Patente de los Estados Unidos No. 2004/0268130, describe un sistema y método para autenticar un artículo, que incluye los pasos de selección de un elemento inherente del artículo, y conversión del elemento en datos (20) digitales, para formar un código de identificación para el artículo. Se encripta el código de identificación, utilizando una clave privada (70) secreta de un par de claves de encriptación asimétricas y uno asociado con la parte emisora. El código encriptado se hace disponible en una etiqueta que acompaña al artículo. Durante la fase subsiguiente, durante la autenticación, los datos (20) digitales que se relacionan con el elemento se determinan directamente a partir del artículo, y el código se desencripta utilizando una clave pública del par obtenido de una tercera parte, de acuerdo con las reglas de una infraestructura de la clave pública. De acuerdo con el sistema y método de la Solicitud de Patente de los Estados Unidos No. 2004/0268130, el elemento inherente es el resultado de una manipulación química de un artículo o la inclusión de características únicas en, o sobre el artículo, esto también requiere que el código encriptado esté disponible en una etiqueta que acompaña al artículo; sin embargo, el código se encripta sin aplicar una función de hash (40). Esta falla permitirá a un falsificador obtener los datos (20) originales que definen la singularidad del artículo, y empezar a hacer modificaciones con el fin de acercarse a los datos (20) originales. Al utilizar una función de hash (40), el falsificador no tendrá una pista de cómo modificar el artículo para tratar de hacerlo pasar la autenticación. Además, no está claro si las características elegidas serán capaces de soportar el deterioro natural del uso de los artículos.

Advanced Track and Trace (ATT), ha desarrollado un método para certificar planchas y láminas de impresión, y sus billetes impresos de manera correspondiente. Utiliza métodos criptográficos robustos. Sin embargo, tiene como desventaja principal, el hecho de que el número de códigos está restringido a las placas diseñadas para la fabricación de billetes, utilizando el proceso ATT sólo puede reproducir las series que se imprimieron con la misma placa debido a

protección criptográfica. Además, debido a la complejidad del patrón que tiene que imprimirse, requiere un microscopio o algún dispositivo de amplificación, así como un control de calidad mejorado, con el fin de reducir al mínimo las variaciones de las partidas de los billetes de seguridad.

5 Como puede notarse, existe la necesidad de un método para certificar los documentos de seguridad como requisito para un proceso confiable y rápido para autenticar documentos. Además, con el desarrollo siempre creciente de la tecnología de la información, este método agrega seguridad y confianza a un documento de seguridad (10) físico con una contraparte de un certificado digital
10 (80), con el entendimiento de que ambos se necesitan para valorar la autenticidad del documento. Particularmente, en este escenario, considerando que el documento físico y el certificado digital (80) están enlazados de manera única, un billete sin un certificado digital (80) válido, no tendrá valor incluso en el caso de que el documento sea genuino.

15

SUMARIO DE LA INVENCION

Uno de los objetivos de la presente invención es proporcionar un sistema de certificación de billetes, cheques o cualquier otro documento de seguridad (10). Objetivos que comprenden la certificación digital de los documentos que
20 involucran estas variaciones, que implican la singularidad de cada pieza. Esto es posible debido a la variabilidad natural de los procesos de producción industrial, así como la información que cambia de una manera predecible y controlada, tal como: números de serie, carácter de la serie, etc.

Otro objetivo de la invención consiste en proporcionar un proceso de
25 certificación que consiste de un mensaje con una función de hash (40), que incluso si se descripta, sólo es útil para verificar la autenticidad, y no revelará

ninguna información sobre las características del documento original que podría ser útil en el proceso de falsificación.

Otro objetivo de la invención es proporcionar un proceso de autenticación para billetes, cheques o cualesquier otros documentos de seguridad.

Otro objetivo de la invención es proporcionar un método de autenticación, para ser implementado de una manera automatizada.

Otro objetivo de la invención es proporcionar un método para la identificación positiva de documentos de seguridad falsificados con una baja incidencia de una autenticación negativa falsa y positiva falsa.

Aún otro objetivo de la invención, es clasificar las falsificaciones por su calidad y grado de sofisticación.

Obtener los datos (20) para individualizar cada documento de seguridad (10) que se obtiene de un conjunto de características de las variaciones del registro entre los elementos agregados en diferentes procesos de fabricación. Estas características se relacionan con la particularidad del proceso de producción, e incluso con la unicidad de cada documento de seguridad (10).

La creación de un mensaje diferente para cada documento de seguridad (10) utilizando el conjunto de características previamente mencionado y los datos (20) relacionados con la ID del documento.

Además, esta invención proporciona un método de certificación y autenticación de cualesquier documentos de seguridad, basándose en el mensaje descrito anteriormente, que requiere una variación del registro que es el resultado de al menos dos procesos de producción. El método de certificación comprende los pasos de:

seleccionar un conjunto de características únicas, obtenido como resultado de las variaciones en el proceso de fabricación y los suministros,

obtener una imagen digital de un documento de seguridad (10) y obtener los datos (20),

5 construir un mensaje midiendo las diferencias del registro entre los elementos del documento y los relacionados con los datos (20) de identificación del documento.

10 construir un mensaje de hash (50), siendo este el mensaje obtenido después de ser codificado por medio de una función de hash (40) criptográfica unidireccional,

 encriptar el hash del mensaje utilizando un sistema criptográfico de clave pública para obtener un certificado digital (80) por medio de una clave privada (70), y

15 almacenar el certificado digital (80) en una base de datos (20) externa y/o, marcar/imprimir el certificado digital (80) en el documento de seguridad (10).

 De acuerdo con otro aspecto de la invención, un método de autenticación comprendiendo los pasos de:

 proporcionar un documento de seguridad (10) a ser autenticado;

20 verificar que las materias primas, elementos de seguridad y los procesos de fabricación originales están presentes en el documento de seguridad (10) por medio de técnicas de análisis de imágenes bien conocidos, o mediante otra clase de verificación tradicional.

construir el mensaje correspondiente midiendo las diferencias del registro entre los elementos del documento y los datos (20) relacionados con los datos (20) de identificación del documento.

5 aplicar una función de hash (40) para obtener un mensaje de hash (50) que se utilizará para la verificación,

10 obtener el mensaje certificado de hash, en una modalidad de la invención, el mensaje de hash (50) se obtiene del certificado digital (80) marcado o impreso en el documento de seguridad (10), el certificado digital (80) se descripta a través del uso de una clave pública, para recuperar el mensaje de hash (50) para la referencia. En una segunda modalidad de la invención, el mensaje certificado se obtiene accediendo a la base de datos (20). Así, se obtiene un mensaje certificado.

15 autenticar el documento comparando el mensaje de hash (50) certificado y el mensaje de hash (50) para la verificación, en donde si el mensaje de hash (50) certificado y el mensaje de hash (50) de la verificación coinciden, el documento se considera como auténtico y si el mensaje de hash (50) certificado y el mensaje de hash (50) de la verificación no coinciden, el documento se considera como una falsificación.

20 **BREVE DESCRIPCIÓN DE LOS DIBUJOS**

La Figura 1 muestra el proceso de certificación general.

La Figura 2 muestra un documento de seguridad (10) que contiene imágenes y caracteres provenientes de diferentes procesos.

La Figura 3 muestra un ejemplo de un documento de seguridad (10) que tiene diferentes imágenes de diferentes procesos, y que muestra puntos de referencia y puntos relativos.

La Figura 4 es un ejemplo de una función MD para el tratamiento matemático de los datos (20) para obtener un mensaje.

La Figura 5 es un ejemplo de un proceso de autenticación de un documento de seguridad (10).

La Figura 6 es un algoritmo para la autenticación de un documento de seguridad (10).

10

DESCRIPCIÓN DETALLADA DE UNA MODALIDAD PREFERIDA

El proceso de certificación y autenticación se basa en las variaciones que tienen lugar durante los pasos del proceso de fabricación de los documentos de seguridad. Particularmente, en la interacción de esos procesos.

Esta invención se relaciona con un sistema para la certificación y autenticación de documentos de seguridad. Los documentos de seguridad incluyen por ejemplo un billete, un cheque, un pasaporte o un certificado de nacimiento.

La invención también se relaciona con un método para la certificación y autenticación de un documento original, en donde las características únicas de cada documento se identifican, codifican y se insertan opcionalmente en el documento de seguridad (10) mismo, o se almacenan en una base de datos (20) externa. Este método y el sistema propuesto evitan la falsificación de los documentos de seguridad.

La presente invención se entenderá mejor a partir de la descripción detallada dada a continuación, y los dibujos acompañantes que se dan a manera de ilustración únicamente, y por lo tanto, no limitan la presente invención.

5 Bajo la presente invención, los siguientes términos tienen el significado indicado.

Certificación - Procedimiento formal mediante el cual una persona o agencia acreditada o autorizada valora (emitiendo un certificado) los atributos, características, calidad, calificación o estado de individuos u organizaciones, bienes o servicios, procedimientos o procesos, o eventos o situaciones, de
10 acuerdo con los requisitos o estándares establecidos.

Autenticación - es el acto de confirmar la veracidad de un atributo de una sola pieza de datos (20) (dato) o entidad. La autenticación es el proceso de determinar si alguien o algo es, de hecho, quién o lo que declara ser.

15 **Proceso de impresión de seguridad** - Procesos de impresión especiales que a diferencia de los procesos comercialmente disponibles no pueden imitarse fácilmente, por ejemplo, aquéllos utilizados en la impresión de billetes.

Elementos de seguridad – se refiere a las características de seguridad presentes en el documento de seguridad (10). Tales características pretenden ser difíciles de imitar a través del uso de productos comercialmente disponibles, como es el caso de papel de seguridad, tintas de seguridad, marcas de agua, hilos magnéticos, ventanas transparentes, elementos táctiles, láminas, parches, hologramas, etc.
20

25 **Documentos de seguridad** – es un documento que indica por escrito alguna garantía (de cada uno de los Garantes), y si se produjo utilizando

procesos de impresión de seguridad y también puede incluir elementos de seguridad.

Características únicas – son las características que hacen único a un documento, pueden ser introducidas a propósito como por ejemplo un número de serie o pueden ser debidas a variaciones naturales en cualquiera de las partes del proceso de producción. Un caso particular de las últimas son las variaciones del registro natural entre los elementos agregados en diferentes procesos de fabricación. Estas características se relacionan con la particularidad, e incluso con la unicidad de cada documento de seguridad (10) fabricado. Las características pueden ser señales acústicas, eléctricas y magnéticas, y medirse en una parte del espectro electromagnético. Incluye errores o variaciones de impresión: manchas de tinta, el llenado de las líneas, color, etc.

Registro – el registro se refiere a la posición relativa entre los elementos de un documento de seguridad (10), y que se incluyeron por los diferentes procesos de fabricación. Durante la fabricación de un documento de seguridad (10), la posición relativa entre la variedad de imágenes o caracteres o elementos de seguridad de diferentes procesos, varía de documento a documento, haciendo al documento único e irrepetible, debido a tales variaciones.

Función métrica - Una métrica en un conjunto X es una función (llamada la *función de distancia* o distancia simplemente)

$d: X \times X \rightarrow \mathbb{R}$, en donde $\mathbb{R}$ es el conjunto de números reales). Para toda x, y, z en X , se requiere que esta función satisfaga las siguientes condiciones:

1. $d(x, y) \geq 0$
2. $d(x, y) = 0$ si y sólo si $x = y$

$$3. \quad d(x, y) = d(y, x)$$

$$4. \quad d(x, z) \leq d(x, y) + d(y, z).$$

5 **Función métrica generalizada** - Una métrica generalizada en un conjunto X es como una función métrica, pero de una manera que relaja sus axiomas (por ejemplo, tal vez sólo satisface los axiomas 1 y 3).

10 **Datos (20) de ID del documento** – son los datos (20) que actúan como un identificador para un documento particular. Puede ser una palabra, número, letra, símbolo o cualquier combinación de éstos. Un identificador es un nombre que identifica (esto es, califica la identidad de), ya sea un documento único o un conjunto de documentos. La abreviatura ID se refiere al identificador (esto es, un ejemplo de identificación). En el caso de billetes, contiene el número de serie.

15 **El mensaje** – es la concatenación del resultado de aplicar algunas métricas, métricas generalizadas u otras funciones, a los puntos en un subconjunto previamente seleccionado de características únicas (del documento de seguridad (10)); y su ID del documento.

El mensaje de hash (50) – es el mensaje codificado por medio de una función de hash (40) criptográfica unidireccional.

20 **Certificado digital (80)** – el certificado digital (80) del documento es el mensaje de hash (50) encriptado, almacenado en el proceso de certificación (encriptado utilizando una clave privada (70)).

25 El término “**características únicas**” está en uso para todas aquellas variaciones naturales del documento, que surgen en el proceso de fabricación y que son medibles, en particular, aquéllas proporcionadas por el proceso de impresión de seguridad para la fabricación de un documento de seguridad (10). Un ejemplo de una característica única es el registro.

De acuerdo con la presente invención, los elementos de seguridad son aquellas partes o componentes que están presentes en un documento de seguridad (10), que tienen el propósito de facilitar a los diferentes usuarios del documento, la autenticación del documento por medio del control del proceso de fabricación, distribución y comercialización, a modo de evitar la adquisición del elemento de seguridad y/o la falsificación por parte de un individuo o entidad no autorizado.

De acuerdo con la presente invención, las características únicas, son aquellas variaciones naturales que son medibles a lo largo del proceso de fabricación.

También se describe un método para certificar digitalmente un documento de seguridad (10) a través de los datos (20) obtenidos de las características únicas, en particular, el registro.

En un aspecto de la invención, se proporciona un método para certificar de manera digital los documentos de seguridad, utilizando elementos de seguridad y características únicas, que ya están presentes en el documento mencionado.

Particularmente, el documento se digitalizará, lo que puede hacerse a través de un escáner o fotografía digital utilizando diferentes fuentes y clases de iluminación, así como cualquier otra medición de las propiedades físicas, químicas o fisicoquímicas del documento, de las que pueden obtenerse las características únicas. Particularmente, utilizando luz con una longitud de onda entre 200 y 1500 nanómetros, o luz visible y un dispositivo para digitalizar la imagen del documento, puede medirse el registro.

De acuerdo con la presente invención, por “tomar una imagen”, debe entenderse la exploración y digitalización asociada con el equipo de medición de los elementos, tales como:

- reflexión, transmisión, absorción, propiedades de emisión, en cualquier longitud de onda del espectro electromagnético, o una combinación de las mismas, ya sea con iluminación estacionaria o con un estado pulsátil;
- propiedades magnéticas y/o eléctricas, por ejemplo, huella digital electromagnética de los materiales que constituyen el documento de seguridad (10);
- propiedades acústicas; el papel cuando se somete a ciclos de estrés de una magnitud particular, produce niveles medibles particulares de sonido;
- propiedades en respuesta a los estímulos mecánicos y/o químicos y/o eléctricos del papel o los elementos de seguridad.

Los elementos a ser medidos dependen en gran medida de la naturaleza del proceso de fabricación empleado durante la fabricación del documento de seguridad (10), así como el uso que se le dará al documento.

- 15 Un mensaje se construirá utilizando algunos elementos, así como la correlación matemática entre ellos. De acuerdo con la presente invención, se utiliza una función Métrica, que es una función de distancia entre dos puntos.

El mensaje es construido utilizando esos elementos que no pueden degradarse, o cuya degradación es conocida y/o predecible:

- múltiples zonas de diferentes tamaños y/o todo el documento;
- los elementos a ser medidos dependen del documento y el proceso de fabricación para obtener el mismo.
- los elementos que dependen de la interacción entre al menos dos procesos diferentes.

En el caso particular de obtener los datos (20) de los elementos de imágenes digitales, bajo cualquier iluminación, la imagen se toma enfatizando aquellas partes que pretenden ser certificadas. Por ejemplo, podría ser de interés certificar sólo la mitad o un cuarto del tamaño del documento de seguridad (10), o crear múltiples certificaciones utilizando diferentes mensajes para un solo documento.

El sistema de certificación y autenticación de la presente invención se describe con referencia a las Figuras.

El proceso de fabricación del documento de seguridad (10) de acuerdo con la presente invención comprende:

- a) Proporcionar suministros adecuados (paso 11a), que incluyen el sustrato, tintas, elementos de seguridad tales como marcas de agua, hilos, ventanas transparentes, fibras coloreadas, láminas o parches, etc.
- b) Realizar el proceso de fabricación del documento de seguridad (10) (paso 13a), que involucra la integración de todos los suministros. El proceso comprende colocar una variedad de elementos, caracteres o imágenes en el sustrato, utilizando al menos dos diferentes procesos de fabricación; y marcar o colocar el número de serie del documento o cualquier otro dato de ID del documento; y
- c) certificar el documento de seguridad (10) mediante:
 - i. La obtención de una imagen digital del documento (paso 10) y la obtención de los datos (20) (20) que corresponden a un grupo seleccionado de características únicas para cada documento, y los datos (20) del ID del documento. Estas características únicas son un resultado de las variaciones del proceso de fabricación y los suministros utilizados;

ii. La construcción de un mensaje (30) utilizando una función métrica para determinar la posición relativa de los puntos de un grupo seleccionado previamente de características únicas, así como los datos (20) de la ID del documento;

5 iii. La construcción de un mensaje de hash (50), aplicando una función de hash (40) (40), el mensaje de hash (50) (50) es el mensaje obtenido por medio de la aplicación de una función de hash (40) criptográfica unidireccional;

10 iv. La encriptación por medio de un sistema de criptografía de clave pública (60) del mensaje de hash (50) utilizando una clave privada (70) (70), para obtener un certificado digital (80) (80), y

 v. Almacenando el certificado digital (80) en una base de datos (20) (90) y/o,

15 vi. Marcando o imprimiendo (97) el certificado digital (80) en el documento de seguridad (10) (10).

En la Figura 2, se describe un documento de seguridad (10) de acuerdo con la invención. Para la fabricación del documento de seguridad (10), algunos procesos están involucrados, por ejemplo, se muestran cuatro procesos (A, B, C, E). El documento de seguridad (10) incluye una variedad de imágenes y
20 caracteres que pertenecen a diferentes procesos de fabricación. En el caso de la Figura 2, el Proceso A, proporciona el sustrato inicial para un documento de seguridad (10). El sustrato incluye algunos elementos de seguridad, tales como un hilo o parche (ai) y una marca de agua y/o imagen de electrotipo (aii). El Proceso B proporciona un conjunto de imágenes (bi), por ejemplo, en la forma
25 de impresión en offset. El Proceso C proporciona al documento de seguridad (10) una imagen (ci) y también caracteres (ciii) en el ejemplo, que se refieren a la denominación, y el carácter (cii) podría ser un proceso de grabado. De igual

manera, el Proceso E proporciona el número de serie del documento de seguridad (10) (e1), ejemplificado como un billete. En una modalidad de la invención, el documento de seguridad (10) se certifica de acuerdo con el proceso descrito en la Figura 1, como resultado, el certificado digital (80) obtenido por el proceso de certificación puede opcionalmente, imprimirse en el documento de seguridad (10) como el elemento (fi).

De acuerdo con la presente invención, al menos una de las siguientes características únicas del documento se considera para certificar el documento y se obtiene de:

- 10 – Respuesta electromagnética (IR, Visible, UV),
- Registro
- Número y posición de las fibras fluorescentes
- Errores de impresión o variaciones de impresión: manchas aleatorias de tinta, líneas sin llenar, color, etc.
- 15 – Propiedades físicas:
 - Propiedades acústicas,
 - Propiedades eléctricas,
 - Propiedades magnéticas,
 - etc.
- 20 – y requiere al menos un dato de la ID del documento:
 - número de serie,
 - denominación del documento,

- nombres,
- fechas, etc.

La Figura 1 describe el proceso de certificación de acuerdo con la presente invención, un documento de seguridad (10) se fabrica de acuerdo con los procesos bien conocidos de la técnica previa (Paso 10). Incluyendo un paso de proporcionar suministros especiales 11a, fabricar un sustrato 13a y realizar un proceso de fabricación que comprende una variedad de pasos (13a).

El documento así fabricado, se somete a continuación a la obtención de datos (20) (paso 20), Figura 1 con el fin de obtener los datos (20) particulares de cada artículo fabricado y en particular, la información con respecto a las posiciones relativas entre la variedad de caracteres o imágenes presentes en un documento de seguridad (10).

Los datos (20) de la posición relativa de las imágenes y caracteres en un documento de seguridad (10) se utilizan para construir un mensaje numérico. La Figura 3 describe la manera de obtener los datos (20) del documento de seguridad (10). El mensaje (30) obtenido en el paso (20) consiste de datos (20) con respecto a las posiciones relativas entre las imágenes y caracteres, cuya posición depende del proceso mediante el cual todas las imágenes y caracteres se colocan en el documento de seguridad (10). Por ejemplo, en la Figura 3, se representa un documento de seguridad (10) que contiene imágenes producidas mediante una secuencia de los procesos A, B, C y E. Como se indicó, hay un conjunto definido de puntos de referencia (A1, A2, ..., AN), (B1, B2, ..., BN), (C1, C2, ..., CN), (E1, E2, ..., EN) etc., (para cada imagen o proceso, en una posición aleatoria definida que proporciona un fácil acceso o identificación, por ejemplo, ciertas esquinas de una imagen, algunos puntos marcados, etc., y a continuación se calcula una primera posición relativa $[D1(A1,A2)]$ de un primer punto relativo (A2) en la imagen A, con respecto al punto de referencia A1; una

segunda posición relativa $[D2(A1,B1)]$ del punto relativo B1 en la imagen B con respecto al punto de referencia A1. De la misma manera, se calcula una tercera posición relativa $[D3(A1,C1)]$ del punto relativo C1 en la imagen C; y opcionalmente, una cuarta posición relativa $[D4(A1,E1)]$ de un punto relativo (E1) en la imagen D. En una modalidad de la presente invención, también se calculan otras posiciones relativas, tomando como referencia un segundo punto de referencia en la imagen B (B2), un tercer punto de referencia en el carácter C (C2) o una cuarta posición de referencia en el carácter E (E2). La métrica también se calcula para cada posición relativa de cada punto de referencia, así como otros valores trigonométricos y otras cantidades matemáticas asociadas con la distancia entre los puntos. Así, pueden definirse una variedad de puntos de referencia y una variedad de mediciones.

Los datos (20) del documento de seguridad (10) se asocian a continuación mediante una función matemática, tal como una matriz como la descrita en la Figura 4, que forma parte del “Mensaje” del documento de seguridad (10) en conjunto con los datos (20) de ID. Como se indicó, es posible construir un mensaje de seguridad general M_D para todos los elementos medidos, o también es posible construir una variedad de mensajes que vienen de partes específicas del documento de seguridad (10), por ejemplo, los Mensajes M_{DA} que se refieren a la posición relativa del punto A con respecto a los puntos A, B, C y E restantes, o un Mensaje M_{DCB} que se relaciona con la posición relativa entre los puntos C y B, o el Mensaje M_{DEC} que se relaciona con la posición relativa de los puntos de las figuras C y E. Esto es particularmente útil cuando es deseable autenticar un documento, en donde sólo una parte del documento está disponible, por ejemplo, en el caso de fracciones de documentos, o documentos de seguridad desgarrados.

Existen algunos métodos matemáticos en la técnica previa para obtener un mensaje de la información recolectada. Por ejemplo, un algoritmo que

devuelva el valor de las posiciones relativas o una regresión matemática, por ejemplo, una regresión lineal, una regresión logarítmica u otra clase de regresión matemática. Para los propósitos de la presente invención, se prefiere una función métrica.

5 Con el fin de obtener una variedad de los puntos de referencia y las posiciones relativas, se realiza un proceso de digitalización o captura de una imagen, que puede llevarse a cabo por ejemplo, con fotografía digital o un escáner; así como cualquier otra medición física y/o química de las características únicas para cada documento, por ejemplo, tipo de papel, peso
10 del papel, textura del papel, color del papel, tipo de tinta, color de la tinta, etc. El paso de digitalización podría realizarse en un módulo de digitalización subsiguiente a la fabricación (13a).

Como un ejemplo, cuando un subconjunto de características únicas surge del registro entre los diferentes procesos involucrados en la fabricación
15 del documento de seguridad (10), entonces las variaciones entre las imágenes y los caracteres que resultan de considerar los procesos A, B, C y E, resultarán en el orden de algunos quintillones, dependiendo de la resolución de la imagen digital del documento.

	Número mínimo de Combinaciones en:		
	100 dpi	200 dpi	600 dpi
Variaciones del Proceso	8.3E+08	2.1E+11	1.4E+15
Total incluyendo la ID del documento	1.7E+17	4.3E+19	2.8E+23

20 Como se indicó, el nivel de variación proporciona una manera única e irrepetible para identificar documentos, cuya reproducción exacta es extremadamente compleja, incluso para el fabricante original.

Además, si no sólo se utiliza el registro, sino también otras características únicas tales como el número y posición de fibras coloreadas o fluorescentes, el número de variaciones se incrementará por algunos cientos de órdenes de magnitud.

5 Al seleccionar los puntos de acuerdo con la presente invención, es posible obtener algunos quintillones de posibles combinaciones, así, es extremadamente improbable que un falsificador obtenga un documento con las mismas características únicas que aquéllas contenidas en un certificado digital (80) producido de acuerdo con la presente invención.

10 En el caso particular de los billetes, incluso si el fabricante original quisiera falsificar y copiar exactamente un documento, tendría que fabricar muchos documentos (en el orden de quintillones), y a continuación seleccionar uno que tuviera la misma variación, y a continuación poner los datos (20) de la ID del documento junto con el mismo certificado del original. Por lo tanto,
15 particularmente para billetes, este método que utiliza el registro, hace imposible la falsificación, a través de hacerla económicamente inviable, ya que será un proceso muy complejo e ineficiente y en el caso de los billetes no habría lugar para una ganancia monetaria.

 Sin embargo, para evitar que un falsificador estudie estadísticamente las
20 variaciones del fabricante oficial, el mensaje obtenido en el paso (30) se transforma a continuación en el paso 40 a través del uso de una función matemática de hash que es irreversible y después se encripta en el paso 60 para proporcionar un certificado digital (80) único.

 En el paso 40 de la Figura 1, el mensaje obtenido en el paso (30), se
25 transforma a continuación utilizando una función matemática, tal como una función de hash (40), con el fin de obtener un Mensaje con una función de hash (40), que consiste en al menos una cadena de caracteres en el paso 50 de la

Figura 1. Existen algunos métodos matemáticos para correr una función de hash (40), por ejemplo, por medio de un proceso o algoritmo matemático unidireccional, que suministre una cadena de caracteres.

La función de hash (40) se encripta a continuación en el paso (60) para proporcionar un mensaje encriptado o certificado digital (80) con una función de hash (40). Con el fin de encriptar el Mensaje de hash (50), se utiliza un algoritmo de encriptación asimétrica, que requiere una clave privada (70) (70), con el fin de generar un certificado digital (80) (80), en la forma de una cadena alfanumérica encriptada.

Como se muestra en la Figura 1, el certificado digital (80) se almacena a su vez en una base de datos (20) (90), que puede mantenerse en un servidor colocado en instalaciones seguras, y/o puede imprimirse o marcarse (97) nuevamente en el documento (10), de una manera legible por el mismo mecanismo para obtener los datos (20) (20), tal como un código de barras, código o texto sin formato (fi). Cuando se utiliza una base de datos (20) (90), además de almacenar el certificado digital (80) (80), también puede ser útil asociar ese certificado digital (80) en la base de datos (20) con otro ID de información de datos (20), tal como el número de serie del documento de seguridad (10), una copia escaneada del documento, detalles del lugar y la hora de fabricación del documento, etc.

El certificado digital (80) es entonces un elemento de validación asociado con los datos (20) de la ID del documento de seguridad (10), y se refiere a una relación particular entre las imágenes y caracteres que están presentes de una manera única para cada documento de seguridad (10).

El certificado digital (80) 80 actúa como una barrera para que una tercera parte no autorizada con un lector, que quiera leer los documentos o billetes falsificados, e imprimir en ellos una etiqueta que represente la exploración del

lector de acuerdo con el esquema de encriptación. Típicamente, el certificado digital (80) (por ejemplo, una etiqueta de código de barras u otra marca), representaría un criptograma descifrable por una clave pública, y la clave privada (70) se reservaría para la parte o autoridad certificante autorizada. Sin embargo, como se mencionó, el certificado digital (80) puede no incluirse nuevamente en el documento de seguridad (10). El certificado digital (80) mencionado anteriormente, representa las características físicas únicas e irrepetibles de las imágenes y caracteres presentes en un documento de seguridad (10), y no describirá información adicional sobre cómo falsificar una copia.

La información encriptada se coloca a continuación como una marca o se imprime nuevamente en el paso 97 de la Figura 1. El certificado digital (80) 80 y el mensaje de hash (50) 50, así como los mensajes parciales de hash y los datos (20) de la ID del documento de seguridad (10), se almacenan en una base de datos (20) 90, se coloca en un servidor disponible para el acceso público. El certificado digital (80) en la forma de un elemento (fi), puede opcionalmente, insertarse en el documento de seguridad (10) 10.

En una modalidad de la invención, el certificado digital (80) puede seleccionarse de un código de barras o de un elemento de un código de barras bidimensional o de una serie de caracteres (f1).

Así, el certificado digital (80) 80 es el resultado de la relación única e irrepetible entre la variedad de imágenes y caracteres. Que son así debido a su proceso de fabricación presente en un documento de seguridad (10).

25 **Proceso de autenticación**

Los documentos de seguridad que se han certificado, se someten a una autenticación adicional. El proceso de autenticación de un documento de seguridad (10) en circulación, se describe en las Figuras 5 y 6. La autenticación de un documento de seguridad (10) es una tarea realizada por una autoridad de autenticación, por ejemplo, la autoridad de autenticación de una institución emisora, pero también puede realizarse por un usuario del documento y la autoridad de autenticación, cuando un usuario desea autenticar un documento. De acuerdo con la Figura 5, un usuario o autoridad de autenticación, que desea conocer si un documento emitido (110) es auténtico o no, debe primero (paso 120) verificar la autenticidad de los suministros y la existencia de los elementos de seguridad (marcas de agua, hilos de seguridad, tintas de seguridad, procesos de seguridad, etc.), que deben estar presentes en un documento auténtico, las fotocopias simples y las copias burdas se discriminan en el paso 120 en la Figura 5 y el paso 121 en la Figura 6, y se consideran como una falsificación de baja calidad (122, Figura 6).

A continuación, si las materias primas y los procesos de impresión presentes en el documento sometido a la autenticación se consideran como auténticos (paso 123, Figura 6), debe generarse un mensaje de hash (50) de acuerdo con los elementos del documento del usuario. Para tal propósito, el usuario/autoridad de autenticación debe obtener los datos (20) de los documentos de seguridad (paso 130), por medio de cualquier dispositivo capaz de tomar la imagen digital requerida, después construir un mensaje a través del uso de una función métrica y los datos (20) de la ID del documento (paso 140), y aplicar una función de hash (40) (150) para obtener un mensaje de hash (50) (160) para la verificación.

Como siguiente paso, se proporciona al usuario un teléfono inteligente, tableta o un dispositivo de procesamiento diferente con una aplicación capaz de obtener los datos (20) (130) y construir de manera automática el mensaje (140)

a través de la función métrica, así como aplicar la función de hash (40) (150) al mensaje, con el fin de obtener un mensaje de hash (50) (160) para la verificación.

Con el fin de autenticar el documento de seguridad (10), el mensaje de hash (50) de la verificación (160), se compara con un mensaje de hash (50) descriptado (260). El certificado digital (80) (80, Figura 1) para obtener el mensaje de hash (50) descriptado (260), necesita recuperarse de alguna manera. Una fuente de certificados digitales (80, Figura 1) para la verificación es la base de datos (20) (280), creada durante la certificación. Considerando que el módulo de adquisición y procesamiento de datos (20) puede tener acceso a la base de datos (20) administrada por la autoridad de autenticación, el certificado digital (80) puede descriptarse (250) por medio de una clave pública (230), con el fin de obtener un mensaje de hash (50) descriptado (260). La base de datos (20) puede ser parte de un dispositivo de almacenamiento masivo que forma parte del aparato lector, o puede estar en una ubicación remota y accesarse por el lector a través de un enlace de telecomunicaciones. El enlace de telecomunicaciones puede tomar cualquier forma convencional, incluyendo enlaces inalámbricos y fijos, y puede o no estar disponible en Internet. El módulo de adquisición y procesamiento de datos (20) puede ser operable, al menos en algunos modos de operación, para permitir que una firma se agregue a la base de datos (20) si no se encuentra una coincidencia. Esta función usualmente sólo se permitiría a las personas autorizadas por obvias razones. Deberá notarse que el mal uso de la clave pública no facilita la falsificación del documento, puesto que la clave pública es útil para descriptar el certificado digital (80), pero es inútil para encriptar un mensaje de hash (50).

En una modalidad de la invención, el mensaje de hash (50) de la verificación (160) del documento de seguridad (10), se proporciona a la

autoridad de autenticación, quien está autorizada para obtener el mensaje de hash (50) descriptado (260) correspondiente a la base de datos (20) (280), como se describió anteriormente, y realizar una comparación para establecer si el mensaje de hash (50) de la verificación (160) coincide con el mensaje de hash (50) descriptado (260).

Otra fuente para recuperar el certificado digital (80) (80, Figura 1), es el código de barras o un elemento del código de barras bidimensional o una serie de caracteres (f1, en la Figura 2) marcado/impreso en el documento de seguridad (10).

En otra modalidad de la invención, el certificado digital (80) puede descriptarse (250) por medio de una clave pública (230), para obtener un mensaje de hash (50) descriptado (260), y con el fin de realizar la comparación para establecer si el mensaje de hash (50) de la verificación (160) coincide con el mensaje de hash (50) descriptado (260), que puede realizarse localmente por el usuario.

Finalmente, si el mensaje de hash (50) de la verificación (160) y el mensaje de hash (50) descriptado (260) coinciden, el documento es entonces calificado como un documento auténtico (400 en la Figura 6). Por otra parte, si el mensaje de hash (50) de la verificación (160) no coincide con el mensaje de hash (50) descriptado correspondiente (260), el documento se considera como una falsificación de alta calidad (305). La incidencia de tal falsificación puede proporcionar elementos/evidencia para investigar patrones criminales.

Como se describe en la Figura 6, el usuario debe realizar primero un paso de verificación 121 para la presencia de materias primas auténticas y los procesos de fabricación de seguridad originales presentes en los documentos de seguridad, tales como un billete. Si tales materiales y procesos no están presentes, entonces el documento se considera como una falsificación de baja

calidad (122). Si los materiales y procesos esperados que están en el documento se consideran como auténticos, entonces el usuario debe realizar un paso de obtención de los datos (20) (130).

5 En una modalidad de la invención, el proceso de autenticación se realiza a través del uso de una aplicación para un dispositivo inteligente, tal como un teléfono inteligente o tableta. La aplicación guía al usuario para obtener una imagen exacta y proporciona los medios para conectarse con la Autoridad de Autenticación. Después de la autenticación, por medio de la Autoridad de Autenticación, el resultado del proceso de comparación se
10 entrega.

El método de la invención proporciona la posibilidad de clasificar las falsificaciones por sus características de fabricación, para tales propósitos, se requiere un equipo para la clasificación y registro automático (ID) de las falsificaciones, que está a cargo de registrar los elementos de todas las
15 falsificaciones que llegan a la institución emisora, con el fin de crear una base de datos (20) con toda la información extraída de las falsificaciones, con el fin de enlazar estadísticamente las piezas a los “Falsificadores” (no necesariamente una persona), y detectar incluso las ligeras mejoras. Tal información es útil para investigar y perseguir los crímenes de falsificación.

20 Para la certificación se necesitan: Sistemas de adquisición de imágenes (cámara digital, escáner), equipo de procesamiento de imágenes (tales como CPU, GPU, FPGA), y sistemas de almacenamiento (servidores de datos (20)). En el caso de 97, para el dispositivo de Marcado/Impresión, este puede ser una impresora de inyección, máquina numeradora, dispositivos de marcado con
25 láser, dispositivos de etiquetado, etc.

Para la autenticación se necesitan: sistemas de adquisición de imágenes (cámaras digitales, cámaras de teléfono celular, escáner, etc.),

sistemas de procesamiento de imágenes (tales como CPU [PC, Servidores, Tableta, Teléfonos Inteligentes, etc.], GPU, FPGA). En el caso de 280: el acceso a la base de datos (20) (Internet, SMS, LAN, WAN, VPN, etc.) es requerido.

- 5 Siendo la invención así descrita, será obvio que la misma puede variarse de muchas formas. Tales variaciones no deben considerarse como que se apartan del espíritu y alcance de la invención, y todas estas modificaciones como sería obvio para alguien con experiencia en la técnica, están incluidas dentro del alcance de las siguientes reivindicaciones.

10

Agradecimientos:

El autor está agradecido con Mario Hernández Téllez y Uriel Mancebo del Castillo por las útiles y numerosas discusiones.

RESUMEN DE LA INVENCION

La invención se relaciona con métodos para certificar y autenticar documentos de seguridad. La certificación comprende las etapas de : a) seleccionar un conjunto de características únicas, obtenidas como resultado de las variaciones en el proceso de fabricación y los suministros, b) obtener una imagen digital de un documento de seguridad (10) y obtener los datos (20) de la posición relativa entre los elementos seleccionados de diferentes procesos de fabricación (registro), c) construir un mensaje midiendo el registro de los elementos seleccionados del documento y los datos (20) de la ID del documento, d) construir un mensaje de hash (50), siendo este el mensaje obtenido después de ser codificado por medio de una función de hash (40) criptográfica unidireccional, e) encriptar el mensaje de hash (50) utilizando un sistema criptográfico de clave pública (60) para obtener un certificado digital (80), por medio de una clave privada (70), y f) almacenar el certificado digital (80) en una base de datos (90) externa.