

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

Por la cual se deniega una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 26
del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO:

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 24 de julio de 2017, con el N° NC2017/0007331, por el BANCO DE MÉXICO, entró a fase nacional la solicitud de patente de invención titulada "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", que corresponde a la solicitud internacional PCT/IB2014/002906 del 24 de diciembre de 2014.

SEGUNDO: Que el extracto de esta solicitud fue publicado en la Gaceta de la Propiedad Industrial N° 800 el 28 de julio de 2017, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 5489, notificado el 04 de mayo de 2018, se requirió a la solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2017/0007331 el 03 de agosto de 2018, respondió oportunamente el requerimiento formulado y presentan nuevas reivindicaciones 1 a 18 que reemplazan las originalmente presentadas, atendiendo de esta manera las observaciones efectuadas en el examen de fondo. Se acepta este último capítulo reivindicatorio presentado, comoquiera que se ajusta a las prescripciones contenidas en el artículo 34 de la Decisión 486.

QUINTO: Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina "Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial."

SEXTO: Que en el presente caso las reivindicaciones 1 a 18 incluidas en el radicado bajo el N° NC2017/0007331 del 03 de agosto de 2018, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

6.1. Objeto de la invención

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, se 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.

6.2. Determinación del estado de la técnica

El estado de la técnica se determinó con base en la fecha de presentación internacional: diciembre 24 de 2014 y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	WO 0191007	"System And Method For Production And Authentication Of Original Documents"	29/noviembre/2001
D2	US 2006/021065	"Method and device for authorizing content operations"	26/enero/2006
D3	WO 2009/150622	"Encrypted Marking And Method For Securing And Certifying The Authenticity Of A Product"	17/diciembre/2009

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

El documento D1¹ enseña 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 documento D2² enseña 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).

El documento D3³ enseña 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).

6.3. Examen de Patentabilidad (Art. 14 D486)

Nivel inventivo (Art 18 D486)

Según lo dispuesto en el artículo 18 de la Decisión 486: "*Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica*".

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 1 se refiere a: "*Un método implementado por computadora (...)*" (Ver página 1 del radicado N° NC2017/0007331 del 03 de agosto de 2018).

¹https://worldwide.espacenet.com/publicationDetails/biblio?CC=WO&NR=0191007A1&KC=A1&FT=D&ND=3&date=20011129&DB=&locale=en_EP

²https://worldwide.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20060126&CC=US&NR=2006021065A1&KC=A1

³https://worldwide.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20091217&CC=WO&NR=2009150622A2&KC=A2

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 1, y las reveladas en los documentos D1 y D2 que representan el estado de la técnica:

Tabla 1

Características esenciales	D1	D2
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.	En el caso de los documentos de autenticación automática, para cada documento impreso, la aplicación de software imprime en el documento un código cifrado que describe las características aparentemente no deterministas del medio, así como una firma digital del contenido del documento (Pág. 56, Fl. 57). El tercer nivel de precisión de autenticación implica generar un patrón x-y pregrabado de las fibras fluorescentes en el artículo (por ejemplo, registrando el patrón aleatorio particular de las fibras presentes en una tarjeta de crédito particular cuando se fabrica la tarjeta (Pág. 21, Fl. 22).	No se menciona
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.	Como se muestra en la figura 1, se proporciona un documento de autoverificación que tiene un stock (1), un contenido de documento impreso (2), una región de autenticación (3) y una región codificada de codificación (4) (Pág. 61, Fl. 62). La fuente en bruto (1) es escaneada (101) por el escáner (10) para determinar un patrón no determinista de las fibras (6) dentro de la región de autenticación (3). Estos datos se almacenan (102), por ejemplo en la memoria temporal (11) bajo control de un procesador (15), o en asociación con un identificador de la acción (1) (Pág. 61, Fl. 62).	No se menciona
Obtener una imagen digital de un documento de seguridad (10).	La información devuelta puede ser una imagen o descripción expresa del patrón del documento capturado durante el	No se menciona

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

	proceso de producción, una firma digital (hash) del patrón, o una descripción de un método de autenticación, que puede variar aleatoriamente, de acuerdo con un programa de costos u otro patrón (Pág. 35, Fl. 36 a Pág. 36, Fl. 37).	
Obtener los datos (20) del conjunto de elementos de la área determinada del documento que tiene características únicas de registro.	La fuente en bruto (1) es escaneada (101) por el escáner (10) para determinar un patrón no determinista de las fibras (6) dentro de la región de autenticación (3). Estos datos se almacenan (102), por ejemplo en la memoria temporal (11) bajo control de un procesador (15), o en asociación con un identificador de la acción (1) (Pág. 61, Fl. 62).	No se menciona
Obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos (20) de la ID del documento.	Con el fin de detectar dicroísmo, por ejemplo de fibras dicroicas incrustadas en un medio, una realización de la invención proporciona el uso de al menos dos fuentes de luz o un sistema de fuente de luz variable en el tiempo, o al menos dos detectores o un sistema de detección variable en el tiempo, para iluminar las fibras dicroicas, midiendo selectivamente el patrón de la característica, que en este caso es el anisotropismo óptico (Pág. 44, Fl. 45). Para autenticar un documento de este tipo, el stock en sí se examina para verificar su autenticidad. Luego se examina la información criptográfica para determinar si el contenido ha sido alterado y la identificación coincide con la identificación impresa en el documento (Pág. 41, Fl. 42).	No se menciona
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.	Se produce una imagen de mapa de bits, como escanear un documento impreso. Preferiblemente, el mapa de bits se comprime en una cadena de datos y se procesa en hash. El archivo hash está firmado por una autoridad de certificación, como el USPS, que utiliza un esquema de firma existencialmente imposible de descifrar (Pág. 28, Fl. 29).	No se menciona
Encriptar el mensaje de hash (50) utilizando una	En primer lugar, el contenido del documento y el identificador del medio	No se menciona

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

clave privada (70) en un sistema criptográfico de clave pública (60) para obtener un certificado digital (80).	pueden transmitirse a un servidor remoto, para su procesamiento en una firma digital, hash (proceso irreversible) con la descripción de las características aparentemente no deterministas del medio, y encriptado, utilizando una clave pública y un algoritmo de clave privada (Pág. 56, Fl. 57). Otro objeto de la invención es proporcionar un sistema de autenticación que comprenda un certificado de autenticación que tenga un elemento resistente a la falsificación y un contenido de documento, un código de seguridad asociado con el certificado de autenticación que defina una característica aparentemente no determinístico del elemento resistente a la falsificación y una firma digital del contenido del documento (Pág. 53, Fl. 54).	
Almacenar el certificado digital en una base de datos externa.	No se menciona	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).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque 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).

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.

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.

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

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).

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.

Asimismo, el documento D1 divulga las características de las siguientes reivindicaciones dependientes así:

- Reivindicación 6: Los problemas de autenticación y disuasión de falsificaciones pueden ser importantes en muchos contextos. Billetes de divisas, certificados de acciones y bonos, tarjetas de crédito, pasaportes, conocimientos de embarque, así como muchos otros documentos legales (por ejemplo, escrituras, testamentos, etc. (Pág. 1, Fl. 2). Por lo tanto, los certificados originales como certificados de nacimiento, testamentos, licencias, derechos de autor y similares pueden imprimirse en lugares distribuidos bajo la autoridad directa de la autoridad competente, con la contabilidad y la responsabilidad proporcionadas (Pág. 38, Fl. 39).
- Reivindicación 7: Sin embargo, durante la producción, se puede escanear todo el stock, con una autenticación normal basada en un subconjunto de los datos escaneados (Pág. 35, Fl. 36).

En conclusión, las reivindicaciones dependientes 2 a 8 no tienen características adicionales que le proporcionen un efecto sorprendente a la materia de la reivindicación 1, por lo tanto, tampoco tienen nivel inventivo.

Por otra parte, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 9 se refiere a: “*Un método de autenticación de un documento de seguridad (...)*” (Ver página 2 del radicado N° NC2017/0007331 del 03 de agosto de 2018).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 9, y las reveladas en los documentos D1 y D3 que representan el estado de la técnica:

Tabla 2

Características esenciales	D1	D3
Documento de seguridad (10) documento de seguridad (10).	Posteriormente, el documento puede autenticarse utilizando una técnica en línea, en el que el identificador del documento se emplea para recuperar una representación almacenada remotamente del documento, incluido el patrón de fibra, para la autenticación (Pág. 35, Fl. 36).	El siguiente ejemplo ilustra la protección de seguridad de los documentos de identificación personal mediante una marca encriptada multinivel única protegida por el código del material donde los datos biométricos personales del titular del documento están integrados en dicha marca (Pág. 6, Fl. 7).
Recibir por parte de un usuario, 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	La información devuelta puede ser una imagen o descripción expresa del patrón del documento capturado durante el proceso de producción, una firma digital (hash) del patrón, o una descripción de un método de autenticación, que puede variar aleatoriamente, de acuerdo con un programa de costos u otro patrón (Pág. 35, Fl. 36 a Pág. 36, Fl. 37). En el caso de los documentos de autenticación automática, para cada documento impreso, la aplicación de software imprime en el documento un código cifrado que describe las características aparentemente no deterministas del medio, así como una firma digital del contenido del documento (Pág. 56, Fl. 57). El tercer nivel de precisión de autenticación implica generar un patrón x-y pregrabado de las fibras fluorescentes en el artículo (por ejemplo, registrando el patrón aleatorio particular de las fibras presentes en una tarjeta de crédito	No se menciona

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

	particular cuando se fabrica la tarjeta (Pág. 21, Fl. 22).	
Obtener datos (20) de un conjunto de elementos de una área determinada del documento que tiene características únicas de registro.	La fuente en bruto (1) es escaneada (101) por el escáner (10) para determinar un patrón no determinista de las fibras (6) dentro de la región de autenticación (3). Estos datos se almacenan (102), por ejemplo en la memoria temporal (11) bajo control de un procesador (15), o en asociación con un identificador de la acción (1) (Pág. 61, Fl. 62).	No se menciona
Obtener una medida del registro del conjunto determinado de elementos del documento y los datos (20) de la ID del documento.	Con el fin de detectar dicroísmo, por ejemplo de fibras dicroicas incrustadas en un medio, una realización de la invención proporciona el uso de al menos dos fuentes de luz o un sistema de fuente de luz variable en el tiempo, o al menos dos detectores o un sistema de detección variable en el tiempo, para iluminar las fibras dicroicas, midiendo selectivamente el patrón de la característica, que en este caso es el anisotropismo óptico (Pág. 44, Fl. 45). Para autenticar un documento de este tipo, el stock en sí se examina para verificar su autenticidad. Luego se examina la información criptográfica para determinar si el contenido ha sido alterado y la identificación coincide con la identificación impresa en el documento (Pág. 41, Fl. 42).	No se menciona
Aplicar una función de hash (40) para obtener un mensaje de hash (50) para la verificación.	Se produce una imagen de mapa de bits, como escanear un documento impreso. Preferiblemente, el mapa de bits se comprime en una cadena de datos y se procesa en hash. El archivo hash está firmado por una autoridad de certificación, como el USPS, que utiliza un esquema de firma existencialmente imposible de descifrar (Pág. 28, Fl. 29).	El valor hash de la información almacenada en el chip de contacto se calcula bajo la función hash matemática. Una característica distintiva de la función hash es que un cambio de incluso un bit de información de entrada da como resultado un valor calculado diferente. La función hash calculada se integra luego en la marca cifrada (3) mediante la alteración de algunos elementos de la marca (Pág. 7, Fl. 8).



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

Obtener y descryptar un mensaje certificado con una función de hash (40) almacenado, para el documento de seguridad (10) certificado.	El destinatario del mensaje descrypta el mensaje utilizando su clave privada. Como solo el destinatario tiene acceso a la clave privada (a través de la protección con contraseña o de seguridad física), solo el destinatario puede leer el mensaje. Para crear una firma digital, la computadora del remitente realiza un cálculo que involucra tanto la clave privada del remitente como el mensaje. El resultado del cálculo es una firma digital, que luego se incluye como un archivo adjunto al mensaje original. El destinatario del mensaje realiza un cálculo similar que incluye el mensaje, la firma digital del remitente y la clave pública del remitente. Según el resultado del cálculo del destinatario, conocido como hash, se puede determinar si la firma es auténtica (o es fraudulenta) y si el mensaje fue interceptado y/o alterado en algún momento entre el remitente y el destinatario (Pág. 22, Fl. 23 a Pág. 23, Fl. 24).	No se menciona
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.	No se menciona	El valor de hash de los datos almacenados en ese chip se calcula e integra en la marca cifrada multinivel única (5), que se presenta en forma de una perforación de una imagen en el documento. El proceso de verificación incluye la lectura de una marca encriptada y los datos integrados en ella. Se calcula el valor hash de los datos almacenados en el chip y el valor del marcado se compara con el valor hash calculado. Si ambos valores coinciden, los datos del chip son auténticos. Si no coinciden, es una señal segura de que los datos han sido manipulados y alterados (Pág. 7, Fl. 8).
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	No se menciona	

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

función de hash (40) para la verificación no coinciden, el documento se considera como una falsificación.		
---	--	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 9 porque 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).

La diferencia entre la invención, definida en la reivindicación 9 y el sistema de D1 consiste en que el método de la reivindicación 9 compara el mensaje certificado con una función de hash (40) y el mensaje con una función de hash (40) para la verificación y 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.

El efecto que logra el incluir el comparar el mensaje certificado con una función de hash (40) y el mensaje con una función de hash (40) para la verificación y 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 es poder identificar si el documento de seguridad es genuino o es una falsificación.

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 identificar si el documento de seguridad es genuino o es una falsificación?”.

Sin embargo, la utilización del comparar el mensaje certificado con una función de hash (40) y el mensaje con una función de hash (40) para la verificación y 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



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

falsificación, ya está divulgada en el documento D3 que se refiere a que el valor de hash de los datos almacenados en ese chip se calcula e integra en la marca cifrada multinivel única (5), que se presenta en forma de una perforación de una imagen en el documento. El proceso de verificación incluye la lectura de una marca encriptada y los datos integrados en ella. Se calcula el valor hash de los datos almacenados en el chip y el valor del marcado se compara con el valor hash calculado. Si ambos valores coinciden, los datos del chip son auténticos. Si no coinciden, es una señal segura de que los datos han sido manipulados y alterados (Pág. 7, Fl. 8).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la comparación de los datos con la función de hash del documento D3 en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 9 de la solicitud. Por lo cual se considera obvia.

Asimismo, el documento D1 divulga las características de las siguientes reivindicaciones dependientes así:

- Reivindicación 12: Posteriormente, el documento puede autenticarse utilizando una técnica en línea, en el que el identificador del documento se emplea para recuperar una representación almacenada remotamente del documento, incluido el patrón de fibra, para la autenticación. La información devuelta puede ser una imagen o descripción expresa del patrón del documento capturado durante el proceso de producción, una firma digital (hash) del patrón, o una descripción de un método de autenticación, que puede variar aleatoriamente, de acuerdo con un programa de costos u otro patrón (Pág. 35, Fl. 36 a Pág. 36, Fl. 37). La capacidad de análisis de imágenes generalmente se ajustará o adaptará para los tipos de codificación empleados, reduciendo el análisis a detalles relevantes del marcado (Pág. 47, Fl. 48). U. S. Pat. No. 3.942.154 (Akami, et al., 2 de marzo de 1976), que se incorpora aquí como referencia, describe un método y aparato para reconocer patrones coloreados (Pág. 16, Fl. 17).
- Reivindicación 13: Los problemas de autenticación y disuasión de falsificaciones pueden ser importantes en muchos contextos. Billetes de divisas, certificados de acciones y bonos, tarjetas de crédito, pasaportes, conocimientos de embarque, así como muchos otros documentos legales (por ejemplo, escrituras, testamentos, etc. (Pág. 1, Fl. 2).
- Reivindicación 14: Las fibras fluorescentes proporcionan un mecanismo de autenticación de diferentes niveles de capacidad. La firma de autenticación depende de cuatro parámetros; la posición x, y, el dicroísmo y el entorno local. La

Página 12 de 16

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

disponibilidad de tantas variables no determinísticas dificulta la falsificación. Esencialmente, las fibras que tienen una característica de espacio de color no RGB fácilmente detectable, por ejemplo, dicroísmo fluorescente, se incrustan aleatoriamente dentro de un sustrato fibroso (Pág. 20, Fl. 21). El propio medio de grabación puede incluir características que son difíciles de reproducir, tales como marcas de agua, fibras incrustadas, hilos de seguridad, hologramas o similares (Pág. 37, Fl. 38). El documento JP 61-41397 divulga un método para hacer transparente el papel y un método para su fabricación para sobres de ventana transparente (Pág. 6, Fl. 7).

- Reivindicación 16: Ventajosamente, el escáner (16) se proporciona como parte de una bandeja de papel para una impresora (13), con una conexión universal de bus serie (USB) (14) a una computadora central (15), o se comunica a través de una interfaz de impresora o interfaz de servidor de impresión (Pág. 62, Fl. 63). La autenticación automática de documentos es soportada por un aparato que comprende una pantalla maestra, un medio de adquisición de imágenes tal como una cámara CCD y un procesador de comparación cuya tarea es comparar el perfil de intensidad de moiré adquirido con una imagen de referencia prealmacenada (Pág. 12, Fl. 13).

En conclusión, las reivindicaciones dependientes 10 a 18 no tienen características adicionales que le proporcionen un efecto sorprendente a la materia de la reivindicación 1, por lo tanto, tampoco tienen nivel inventivo.

En referencia al argumento de la solicitante, según el cual afirma que a diferencia del arte previo citado, la presente invención no incluye agregar marcas al documento, es pertinente aclarar que esta diferencia no está especificada dentro del capítulo reivindicatorio NC2017/0007331 del 03 de agosto de 2018, por lo tanto, no hacen parte del estudio de novedad realizado. Resulta del caso señalar que, el artículo 30 de la Decisión 486 señala que las reivindicaciones deben ser claras y concisas y contener todas las características técnicas esenciales de la invención.

Por otra parte, en referencia al argumento de la solicitante, según el cual afirma que el documento D1 y el documento 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 (...)*”, cabe indicar que el capítulo reivindicatorio no menciona de manera explícita esta característica, sino que hace referencia a “(...) *teniendo tal documento de seguridad (10) una variación en el registro de elementos única con respecto de otros documentos*

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

de seguridad también manufacturados con los mismos procesos (...), la cual es afectada por el documento D1 al mencionar que el tercer nivel de precisión de autenticación implica generar un patrón x-y pregrabado de las fibras fluorescentes en el artículo (por ejemplo, registrando el patrón aleatorio particular de las fibras presentes en una tarjeta de crédito particular cuando se fabrica la tarjeta (Pág. 21, Fl. 22). De este párrafo es posible evidenciar que en el documento D1, el patrón pregrabado en las fibras presentes en la tarjeta de crédito (documento de seguridad), es aleatorio y particular en cada tarjeta en el momento de su fabricación, por lo que el documento D1 es claro en divulgar una variación única del registro de los elementos presentes de un documento de seguridad respecto a otras tarjetas fabricadas igualmente, tal como lo menciona el capítulo reivindicatorio estudiado. Por lo tanto, esta característica es anticipada en su totalidad por el documento D1.

Por otro lado, en referencia al argumento de la solicitante, según el cual afirma que el documento D1 no menciona 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 (...)*”, es pertinente aclarar primero que el documento D1 hace referencia a la primera característica mencionada por la solicitante al referirse que, como se muestra en la figura 1, se proporciona un documento de autoverificación que tiene un stock (1), un contenido de documento impreso (2), una región de autenticación (3) y una región codificada de codificación (4) (Pág. 61, Fl. 62). La fuente en bruto (1) es escaneada (101) por el escáner (10) para determinar un patrón no determinista de las fibras (6) dentro de la región de autenticación (3). Estos datos se almacenan (102), por ejemplo en la memoria temporal (11) bajo control de un procesador (15), o en asociación con un identificador de la acción (1) (Pág. 61, Fl. 62). De este párrafo es posible evidenciar que a partir de una región (área) de autenticación del documento, se determinan ciertos patrones de las fibras con las cuales se fabrica el documento, lo cual corresponde a las características únicas de registro de cada uno de los documentos de seguridad, siendo realizado este proceso por un procesador.

Por otra parte, el documento D1 hace referencia a la captura de una imagen digital a partir del documento de seguridad al mencionar que la información devuelta puede ser una imagen o descripción expresa del patrón del documento capturado durante el proceso de producción, una firma digital (hash) del patrón, o una descripción de un

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

método de autenticación, que puede variar aleatoriamente, de acuerdo con un programa de costos u otro patrón (Pág. 35, Fl. 36 a Pág. 36, Fl. 37).

Adicionalmente, el documento D1 menciona que la fuente en bruto (1) es escaneada (101) por el escáner (10) para determinar un patrón no determinista de las fibras (6) dentro de la región de autenticación (3). Estos datos se almacenan (102), por ejemplo en la memoria temporal (11) bajo control de un procesador (15), o en asociación con un identificador de la acción (1) (Pág. 61, Fl. 62), lo cual anticipa la característica de la reivindicación D1 “(...) *obtener los datos del conjunto de elementos de la área determinada del documento que tiene características únicas de registro (...)*”, al determinar los patrones de las fibras de la región (área) de autenticación del documento y almacenarlos en una memoria.

Por último, el documento D1 anticipa la característica “(...) *obtener una medida del registro del conjunto determinado de elementos del documento e incorporando los datos de la ID del documento (...)*”, al referirse que con el fin de detectar dicroísmo, por ejemplo de fibras dicroicas incrustadas en un medio, una realización de la invención proporciona el uso de al menos dos fuentes de luz o un sistema de fuente de luz variable en el tiempo, o al menos dos detectores o un sistema de detección variable en el tiempo, para iluminar las fibras dicroicas, midiendo selectivamente el patrón de la característica, que en este caso es el anisotropismo óptico (Pág. 44, Fl. 45). Para autenticar un documento de este tipo, el stock en sí se examina para verificar su autenticidad. Luego se examina la información criptográfica para determinar si el contenido ha sido alterado y la identificación coincide con la identificación impresa en el documento (Pág. 41, Fl. 42). De estos párrafos se puede evidenciar primero que por medio de dos fuentes de luz se realiza una medición de ciertos patrones de las fibras incrustadas en el documento de seguridad, además que se incorporan los datos de identificación (ID) de forma impresa en el documento, por lo cual el documento D1 hace mención a esta característica, tal como se evidencia en el análisis de nivel inventivo del presente Oficio.

En consecuencia, el documento D1 divulga todas las características esenciales objetadas por la solicitante y junto con la combinación de enseñanzas de los documentos D1, D2 y D3, se anticipa en su totalidad las características esenciales de la invención, tal y como se ilustra en el presente Oficio.

En conclusión, teniendo en cuenta que los argumentos de la solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentada, el Superintendente de Industria y Comercio,

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 69473

Ref. Expediente N° NC2017/0007331

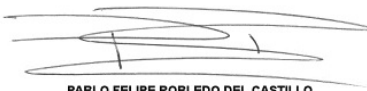
RESUELVE

ARTÍCULO PRIMERO: Denegar la patente de invención a la creación titulada “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”.

ARTÍCULO SEGUNDO: Notificar el contenido de la presente resolución al BANCO DE MÉXICO, advirtiéndole(s) que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 18 de septiembre de 2018


PABLO FELIPE ROBLEDO DEL CASTILLO
Superintendente de Industria y Comercio