

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

Señor(a)
BANCO DE MÉXICO
patentessic@castellanosyco.com.co

Asunto: PATENTE DE INVENCION - PCT

Patente de Invención	PT	Patente de Modelo de Utilidad			
Vía Nacional					
Vía PCT (Fase Nacional)	PCT	Capítulo I	X	Capítulo II	
No. Solicitud Internacional	PCT/IB2014/002906				
Fecha de Presentación Internacional	24 de diciembre de 2014				

Como resultado del examen de fondo realizado, con fundamento en el Artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se comunica:

1. Documentos estudiados

Descripción	NC2017/0007331	24 de julio de 2017
Reivindicaciones:	NC2017/0007331	24 de julio de 2017
Dibujos:	NC2017/0007331	24 de julio de 2017

2. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del capítulo primero del Título X de la Circular Única para efectos del examen de patentabilidad, se tendrá en cuenta la tasa pagada por la solicitante al momento de comenzar el examen para las reivindicaciones adicionales; esto es que cuando la solicitud contenga más de diez

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

(10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada. Por lo tanto, se estudiarán las reivindicaciones 1 a 18 del capítulo reivindicatorio (Radicado N° NC2017/0007331 del 24 de julio de 2017).

Título de la solicitud: “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” (Ver página 1 del radicado bajo el N° NC2017/0007331 del 24 de julio de 2017).

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.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): G07D 7/20.

3. De la solicitud de patente

Reivindicaciones (Art. 30 D 486, Art. 22 PCT)

- 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. Estos términos se describen a continuación: “(...) *odcumento*

Página 2 de 16

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

(...)” (reiv. 9); “(...) *lámina* (...)” (reiv. 14); “(...) *ventana transparente* (...)” (reiv. 14); “(...) *equipo de procesamiento de dinero en efectivo* (...)” (reiv. 18). Se sugiere hacer la aclaración respectiva.

- Las reivindicaciones 1, 9, 14 y 15 no son claras porque los términos: “*uno o mas*” (reivs. 1 y 9); “*tales como*” (reiv. 1); “*al menos*” (reivs. 14 y 15)”; son imprecisos, por lo cual no permiten distinguir la invención del estado de la técnica. Se sugiere sustituirlos por un término preciso o un rango concreto.
- Se sugiere al solicitante incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin de hacer más fácil y sencilla la comprensión de la materia reivindicada.

4. 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**

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

El documento D1¹ 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).

El documento D2² 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).

El documento D3³ 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).

5. Examen de Patentabilidad (Art. 14 D486)

Nivel inventivo (Art 18 D486)

La reivindicación 1 consiste en: *“Un método para certificar un documento de seguridad, comprendiendo (...)”* (Ver página 1 del radicado N° NC2017/0007331 del 24 de julio de 2017).

Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Seleccionar un conjunto de características	Este medio se serializa y se registra una descripción de las características	No se menciona

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

únicas, en donde las características únicas están relacionadas a las variaciones en el proceso de fabricación y los suministros para manufacturar documentos de seguridad.	aparentemente no determinísticos. El medio, que en este caso es papel, por ejemplo stock de 16-32 lb., que tiene un patrón aparentemente poco determinístico de bajo contraste resultante de los procesos de fabricación, con la descripción registrada como una descripción de un patrón no determinístico, o un código estenangiográfico oculto en el patrón no determinístico de los medios (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).	
Obtener una imagen digital de un documento de seguridad y obtener los datos de un conjunto de características únicas tales como la posición relativa entre uno o más elementos.	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). Las fibras fluorescentes proporcionan un mecanismo de autenticación de diferentes niveles de capacidad. La firma de	No se menciona

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

	autenticación depende de cuatro parámetros; la posición x, y, el dicroísmo y el entorno local (Pág. 20, Fl. 21).	
Construir un mensaje midiendo el registro de los elementos seleccionados del documento e incorporando los datos de la ID del documento.	El contenido se autoriza entonces para impresión, y se transmite un mensaje al usuario desde el proveedor del servicio que incluye una imagen del contenido del documento, que incluye opcionalmente una copia del identificador único, opcionalmente un patrón de puntos correspondiente a los puntos de color en el medio de grabación. Opcionalmente, la clave pública previamente definida para el medio de grabación, opcionalmente una firma digital para el contenido del documento y el identificador único, y opcionalmente una segunda contraseña generada aleatoriamente (Pág. 64, Fl. 65).	No se menciona
Construir un mensaje con una función de hash, en donde el mensaje de hash es el mensaje obtenido después de ser codificado por medio de una función de hash 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 utilizando un sistema criptográfico de clave pública para obtener un certificado digital por medio de una clave privada.	En primer lugar, el contenido del documento y el identificador del medio 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).	No se menciona

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

	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, un sistema para leer la característica aparentemente no determinística, y un procesador para comparar la característica aparentemente no determinística de lectura del certificado de autenticación y el contenido del mismo con el código de seguridad asociado para determinar la autenticidad del certificado de autenticación, la autenticidad está asociado con una confiabilidad de los mismos, basada en variaciones estocásticas en la característica aparentemente no determinística, y variaciones estocásticas en la entrada recibida utilizada para la generación del código de seguridad asociado. El código de seguridad es, por ejemplo, un código de autenticación de clave pública/clave privada (Pág. 53, Fl. 54 a Pág. 54, Fl. 55).	
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).

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

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.

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

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

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).

La reivindicación 9 consiste en: “*Un método de autenticación de un documento de seguridad (...)*” (Ver página 2 del radicado N° NC2017/0007331 del 24 de julio de 2017).

Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D3
Proporcionar un documento de seguridad a ser autenticado.	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).	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. El documento personal (1) en la Figura 8 es una tarjeta de identificación hecha de material plástico como Teslin, PVC, PET, policarbonato o cualquier otro material utilizado en la industria de las tarjetas plásticas (Pág. 6, Fl. 7).
Verificar que las materias primas de seguridad y los procesos de fabricación	Este medio se serializa y se registra una descripción de las características aparentemente no determinísticos. El medio, que en este caso es papel, por	No se menciona

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

estén presentes en el documento de seguridad.	ejemplo stock de 16-32 lb., que tiene un patrón aparentemente poco determinístico de bajo contraste resultante de los procesos de fabricación, con la descripción registrada como una descripción de un patrón no determinístico, o un código estenangiográfico oculto en el patrón no determinístico de los medios (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).	
Obtener una imagen digital de un documento de seguridad, y obtener los datos de un conjunto de características únicas, como la posición relativa entre uno o más elementos.	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). Las fibras fluorescentes proporcionan un mecanismo de autenticación de diferentes niveles de capacidad. La firma de autenticación depende de cuatro	No se menciona

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

	parámetros; la posición x, y, el dicroísmo y el entorno local (Pág. 20, Fl. 21).	
Construir un mensaje midiendo el registro de uno o mas elementos del documento y los datos de la ID del documento.	El contenido se autoriza entonces para impresión, y se transmite un mensaje al usuario desde el proveedor del servicio que incluye una imagen del contenido del documento, que incluye opcionalmente una copia del identificador único, opcionalmente un patrón de puntos correspondiente a los puntos de color en el medio de grabación. Opcionalmente, la clave pública previamente definida para el medio de grabación, opcionalmente una firma digital para el contenido del documento y el identificador único, y opcionalmente una segunda contraseña generada aleatoriamente (Pág. 64, Fl. 65).	No se menciona
Aplicar una función de hash para obtener un mensaje de hash 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).
Obtener y descifrar un mensaje certificado con una función de hash almacenado, para el	El destinatario del mensaje descifra 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	No se menciona

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

documento de seguridad certificado.	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).	
Autenticar el documento comparando el mensaje certificado con una función de hash y el mensaje con una función de hash 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 y el mensaje con una función de hash para la verificación es una coincidencia, el documento se considera como genuino, si el mensaje certificado con una función de hash y el mensaje con una función de hash para la	No se menciona	

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

verificación coinciden, documento considera como una falsificación.	no el se una		
---	-----------------------	--	--

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 comparar el mensaje certificado con una función de hash y el mensaje con una función de hash.

El efecto que logra el incluir el comparar el mensaje certificado con una función de hash y el mensaje con una función de hash es poder identificar si el documento 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 es genuino o es una falsificación?”.

Sin embargo, la utilización del comparar el mensaje certificado con una función de hash y el mensaje con una función de hash, 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

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

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). 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 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 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

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

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

(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).

6. Conclusión

Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	WO 0191007	1, 6, 7, 9, 12 a 14 y 16	Nivel Inventivo
D2	US 2006/021065	1	Nivel inventivo
D3	WO 2009/150622	9	Nivel inventivo

En cumplimiento del artículo 45, de la Decisión 486 de la Comisión de la Comunidad Andina, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento la solicitante llegara a modificar: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presente un nuevo capítulo reivindicatorio, y desee que se realice un nuevo examen de patentabilidad a esta modificación, no deberá pagar la tasa de modificación voluntaria pero sí la correspondiente a la tasa de examen de patentabilidad. En todo caso, el número de requerimientos por no patentabilidad estará supeditado a que el término del estudio

Página 15 de 16

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 5489

Ref. Expediente N° NC2017/0007331

de patentabilidad no sea superior a 18 meses, contados desde la publicación de la solicitud de patente de invención. Adicionalmente, se le recuerda a la solicitante que si como respuesta a este requerimiento llegara a modificar el capítulo reivindicatorio y éste contenga más de diez (10) reivindicaciones deberá pagar la tasa por reivindicación adicional.

Se invita a la solicitante se sirva indicar, si así lo considera, su renuncia al término faltante para los sesenta (60) días.

Notifíquese el presente oficio conforme a lo dispuesto en el Título I, Actuaciones ante la Superintendencia de Industria y Comercio; Capítulo sexto, publicación, comunicación, notificación y ejecutoria de las decisiones de la Superintendencia de Industria y Comercio, informándoles que contra el mismo no procede el recurso de la vía gubernativa.

Atentamente,



[DirectorName]

DIRECTOR DE NUEVAS CREACIONES

Elaborado: FERNANDO NICOLÁS VARGAS PLAZAS

Revisado: FERNANDO NICOLÁS VARGAS PLAZAS

Aprobado: JOSÉ LUIS SALAZAR LÓPEZ