

C



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-098035- -00000-0000

Fecha: 2014-05-07 16:34:54 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 76-46

Industria y Comercio
SUPERINTENDENCIA

DELEGATURA DE PROPIEDAD INDUSTRIAL

División de Nuevas Creaciones

SOLICITUD
PATENTE DE INVENCION

21. EXPEDIENTE No. _____

54. TÍTULO _____
APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA
ENCRIPCIÓN Y RECUPERACIÓN DE INFORMACIÓN
LIBRE DE RUIDO

51. CLASIFICACIÓN INTERNACIONAL _____

71. SOLICITANTE _____
UNIVERSIDAD DE ANTIOQUIA

DOMICILIO _____
MEDELLIN, ANTIOQUIA

74. APODERADO _____
LUZ CLEMENCIA DE PAEZ
C.C.35.456.344 de USAQUÉN

22. BOGOTÁ, D.C., _____



Industria y Comercio
SUPERINTENDENCIA

Espacio reservado para el adhesivo de radicación

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-098035- -00000-0000

Fecha: 2014-05-07 16:34:54
Tra. 2 PATENTES
Act. 411 PRESENTACION

Dep. 2020 DIR.NUEVASCR
Eve: 1 REGDEPOSITO
Folios: 26-46

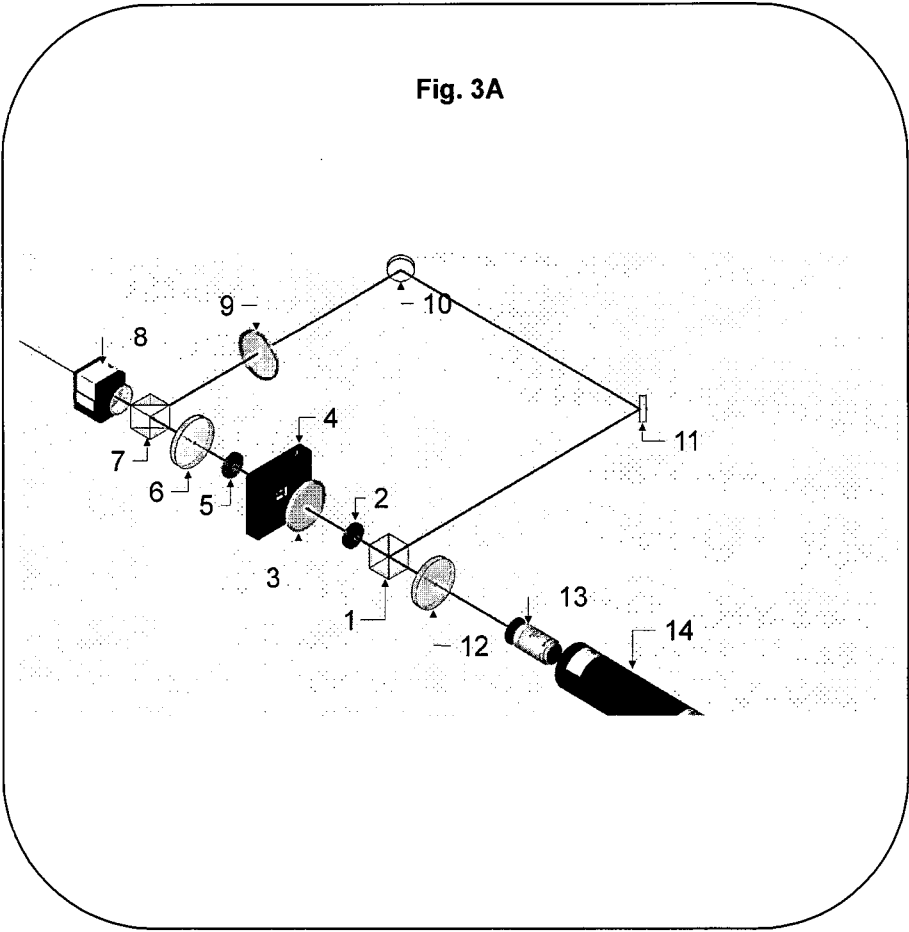
DIRECCIÓN
SOLICITUD

1	TIPO DE SOLICITUD	☒ Patente de invención		☐ Patente de Modelo de Utilidad	
2	TÍTULO DE LA INVENCIÓN			3	CIP Clasificación Internacional de Patentes
APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA ENCRIPTACIÓN Y RECUPERACIÓN DE INFORMACIÓN LIBRE DE RUIDO				G06F G06K	
4	SOLICITANTE (S) ☐ Esta persona también es inventor. Para datos adicionales utilizar hoja de información complementaria				
APELLIDOS O RAZÓN SOCIAL			NOMBRE		IDENTIFICACIÓN
UNIVERSIDAD DE ANTIOQUIA					
5	DATOS DEL SOLICITANTE				
DIRECCIÓN		Calle 67 # 53-108 Medellín, Colombia		No. TELÉFONO	3 47 36 11
CIUDAD		Medellín		CORREO ELECTRÓNICO	clientes@cavelier.com
DEPARTAMENTO/ESTADO				NACIONALIDAD O LUGAR DE CONSTITUCIÓN	
PAÍS DE RESIDENCIA		Colombia			Colombia
6	INVENTOR (ES) Para datos adicionales utilizar hoja de información complementaria				
APELLIDOS		NOMBRES		NACIONALIDAD	
1. BARRERA RAMÍREZ		John Fredy		Colombiano	
2. MIRA AGUDELO		Alejandro		Colombiano	
3. TORROBA		Roberto Daniel		Argentino	
DIRECCIÓN DE CORREO ELECTRÓNICO:					
7	DATOS INVENTOR (ES) Para datos adicionales utilizar hoja de información complementaria				
PAÍS RESIDENCIA		DEPARTAMENTO/ESTADO		CIUDAD	DIRECCIÓN
1. Colombia				Medellín	Calle 67 # 53-108 Medellín, Colombia
2. Colombia				Medellín	Calle 67 # 53-108 Medellín, Colombia
3. Argentina				La Plata	Calle 5 No 1241, La Plata, Argentina
OTRO(S) SOLICITANTE(S) Y/O (OTRO(S)) INVENTOR(ES)					
☐ Los demás solicitantes y/o (demás) inventores se indican en una hoja de información complementaria.					
8	☐ REPRESENTANTE LEGAL ☐ APODERADO				
APELLIDOS		NOMBRES		IDENTIFICACIÓN	
De Páez		Luz Clemencia		C.C. 35.456.34 T.P. 23.555	
DIRECCIÓN		Carrera 4ª No. 72-35		No. TELÉFONO	3 47 36 11
CIUDAD		BOGOTA		CORREO ELECTRÓNICO	cavelier@cavelier.com
PAÍS		COLOMBIA		No. RADICACIÓN O PROTOCOLO DE PODER GENERAL	
9	DECLARACIONES DE PRIORIDAD ☐ SI ☒ NO				
(33) PAÍS DE ORIGEN		CÓDIGO PAÍS		(31) NÚMERO	(32) FECHA (AAAA/MM/DD)

10	DECLARACIÓN SOBRE USO DE RECURSOS GENÉTICOS O BIOLÓGICOS	
<i>Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de recursos genéticos o biológicos de los que cualquiera de los países miembros de la Comunidad Andina es país de origen.</i>		
☐ SI ☐ NO		
Nota: En caso afirmativo deberá anexar copia del contrato de acceso de recursos genéticos o productos derivados, o certificado o número de registro, expedido por la Autoridad competente.		
11	DECLARACIÓN SOBRE USO DE CONOCIMIENTOS TRADICIONALES	
<i>Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de conocimientos tradicionales de comunidades indígenas, afroamericanas o locales de países miembros de la Comunidad Andina.</i>		
☐ SI ☐ NO		
Nota: En caso afirmativo deberá anexar la licencia o autorización de uso de conocimiento tradicional, o certificado o número de registro.		
12	REDUCCIÓN DE TASAS	
<i>Declaro que carezco de medios económicos para presentar la solicitud de patente.</i>		
☐ SI ☐ NO		
Nota: En caso de ser persona natural y carecer de medios económicos, y por lo tanto, aplique la reducción de tasas a que se refiere la resolución vigente en tarifas, debe firmar la presente solicitud bajo la gravedad de juramento.		
Micro, pequeñas y medianas empresas ☐		
Universidades públicas o privadas ☒		
Entidades sin ánimo de lucro ☐		
Debe aportar los documentos que se indican en el numeral 17 de anexos		
13	AUTORIZACIÓN DE NOTIFICACIÓN EN LÍNEA ☐ SI ☐ NO	
Manifiesto que he leído y entendido perfectamente los términos y condiciones de uso de medios electrónicos para las notificaciones en línea a través de Internet de los actos administrativos proferidos por la Superintendencia de Industria y Comercio que deben ser notificados personalmente y, en consecuencia, autorizo el servicio de notificación a través de internet.		
14	PARA PUBLICAR A PARTIR DE LA FECHA DE PRESENTACIÓN O DE LA PRIORIDAD INVOCADA:	15 COMPROBANTE DE PAGO O PAGO ELECTRÓNICO
Si es Patente de Invención ☐ 6 meses ☐ 12 meses ☐ 18 meses ☒ Otro Cual: Inmediata		Si es Patente de Modelo de Utilidad ☐ 6 meses ☐ 12 meses ☐ Otro Cual:
No. 14-0047785 Fecha: 2014/05/07 No. 14-0047781 Fecha: 2014/05/07		
16	FIRMA DEL SOLICITANTE, DEL APODERADO O DEL REPRESENTANTE LEGAL <i>Junto a cada firma, indicar el nombre del firmante y su calidad (si tal calidad no es obvia al leer el petitorio)</i>	
Nombre del Firmante LUZ CLEMENCIA DE PAEZ		Firma <u>LUZ CLEMENCIA DE PAEZ</u> TT#23555
C.C 35.456.344 de Usaquén		Tarjeta Profesional 23.555

17 ANEXOS	
Documentación Técnica 1. ☒ Descripción N° de folios: 19 2. ☒ Reivindicaciones N° Reivindicaciones: 28 3. ☒ Dibujos y/o figuras N° folios: 9 4. ☒ Resumen. 5. ☐ Documento de Prioridad. 6. ☐ Traducción del documento de prioridad. 7. ☐ Certificado de depósito de material biológico si fuera el caso. 8. ☐ Listado de secuencias de nucleótidos y/o aminoácidos en forma digital si fuera el caso. 9. ☒ Arte final 12 x 12. 10. ☐ Anexo formato digital.	Documentación Jurídica 11. ☒ Poder de UNIVERSIDAD DE ANTIOQUIA 12. ☒ (2) Dos documentos que legalmente pruebe la cesión de los inventores al solicitante o a su causante. 13. ☐ Copia del contrato de acceso de recursos genéticos o productos derivados, o certificado o número de registro, si fuera el caso. 14. ☐ Copia de la licencia o autorización de conocimientos tradicionales, o certificado o número de registro, si fuera el caso. 15. Reducción de tasas Micro, pequeñas o medianas empresas ☐ Copia simple de la declaración de renta del año inmediatamente anterior, o en su defecto prueba documental idónea. ☐ Documento de constancia de cumplimiento con lo establecido en la ley 905 de 2004. Universidades públicas o privadas ☒ Copia acto de reconocimiento institucional emitido por el Ministerio de Educación Entidades sin ánimo de lucro ☐ Copia de registro vigente en Cámara de comercio. ☐ Hoja de información complementaria. ☐ Otros, especificar 16. ☒ Comprobante de pago de la tasa de presentación de la solicitud. 17. ☐ Comprobante de pago por reivindicación de prioridad. 18. ☐ Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación. 19. ☒ Comprobante de pago por 18 reivindicaciones adicionales a 10 por \$558.000.

FIGURA CARACTERISTICA



**APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA ENCRIPCIÓN Y
RECUPERACIÓN DE INFORMACIÓN LIBRE DE RUIDO**

Campo técnico:

- 5 La invención se refiere a un montaje óptico-físico junto con un procedimiento que incluye la codificación gráfica de la información para su encriptación y posterior recuperación completamente libre de ruido.

Arte previo:

- 10 Los sistemas de seguridad tienen como objetivo asegurar la protección de la información (privacidad) y bienes (recursos) de los ciudadanos, instituciones y empresas. Estos sistemas ofrecen alternativas fiables para, por ejemplo, proteger las claves de seguridad que se usan para ingresar a las cuentas de correo electrónico, a las cuentas en las redes sociales o para realizar pagos o transacciones electrónicas vía internet. Lo antes
- 15 mencionado evidencia que la seguridad de la información ha entrado a formar un papel primordial en todos los ámbitos del quehacer diario de nuestra sociedad.

Los sistemas que permiten proteger la información, usualmente llamados “sistemas de encriptación” comercialmente disponibles, son algoritmos digitales. Pero se ha

20 demostrado a lo largo del tiempo que los sistemas de seguridad digitales que en un momento se pensaron invulnerables, finalmente fueron quebrantados [3]. A medida que los proveedores de seguridad generan nuevos sistemas digitales de seguridad, en esa misma medida, otras personas trabajan en la búsqueda de una forma de vulnerar esos sistemas. Es por esto, que aunque se busca reforzar los sistemas de encriptación que se

25 comercializan en la actualidad, basados en algoritmos digitales, el área de la seguridad en la información también busca alternativas que permitan aumentar la seguridad en el manejo de la información.

En este contexto, la encriptación óptica aparece como una atractiva y poderosa

30 herramienta para el manejo seguro de la información, debido principalmente a su gran confiabilidad, su gran número de grados de libertad y a la gran velocidad de procesamiento a los que se tiene acceso en el procesamiento óptico de información. Para encriptar información ópticamente los datos se introducen, en forma de haces luminosos, a un sistema óptico; el paso de dichos haces a través de uno o varios elementos logran

35 transformarlos en un grado tal que la información obtenida a la salida del sistema no guarda ninguna semejanza con la original. No obstante, la información se encuentra allí codificada y sólo si se conocen todos los pasos del sistema y los elementos introducidos (llave(s) de encriptación y/o parámetro(s)), el proceso se puede revertir y los datos pueden ser recuperados. Los sistemas ópticos más seguros son los que usan llaves

aleatorias de fase físicas para proteger la información, pues hasta el momento han sido inmunes a ataques.

Las contribuciones presentadas en los últimos 10 años, y en especial los últimos 5, han demostrado la confiabilidad de los sistemas ópticos de encriptación [4]. Pero a pesar de todos los avances, es evidente que existe una limitación que desde el punto de vista práctico no permitía plantear una aplicación real de los sistemas ópticos de encriptación. La limitación está relacionada con el ruido que afecta los datos recuperados y que paradójicamente es debido al elemento que le brinda la seguridad al sistema, la máscara aleatoria de fase física. Se debe tener en cuenta que los usuarios exigen sistemas que posean dos características fundamentales: (a) que le asegure la protección de los datos y (b) que la información recuperada sea fiel a la original. Esto significa que los sistemas de seguridad óptico-físicos solo son una alternativa viable siempre y cuando se elimine el ruido generado sobre los datos recuperados.

Aunque hay varias patentes que presentan sistemas ópticos para la protección de información U.S. 5,903,648, U.S. 6,002,773, U.S. 6,519,340, U.S. 6,907,124, U.S. 7,221,760 y U.S. 7, 684,098, ninguna de ellas se encarga de la eliminación del ruido sobre los datos recuperados. Por otro lado, existen algunas publicaciones donde se presentan algunos métodos digitales para reducir en cierta medida el ruido generado en los datos descriptados, y aunque los métodos permiten obtener alguna mejora sobre los datos recuperados, ningún método permite eliminar completamente el ruido [6-8].

Referencias

- [1] C. Shannon. "Communication Theory of Secrecy Systems". Bell Systems Technical Journal 28, 656-715 (1949).
- [2] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway. "Relations Among Notions Security for Public-Key Encryption Schemes". Lecture Notes in Computer 1492, 26-46 (1998). CRYPTO'98, Proceedings.
- [3] N. Camp-Winget, R. Housley, D. Wagner, J. Walker. "Security flaws data links protocols". Communications of the ACM 46, 35-39 (2003).
- [5] Millán M S and Pérez-Cabrera E 2011 Optical data encryption Optical and Digital Image Processing: Fundamentals and Applications ed G Cristóbal, P Schelkens and H Thienpont (Weinheim: Wiley-VCH Verlag) pp 739-67.
- [6] J.M.Vilardy, M.S.Millan, and E.Perz-Cabre, "Improved decryption quality and security of a joint transform correlator-based encryption system," J.Opt. 15, 025401 (2013).
- [7] Bahram Javidi, Nasser Towghi, Nabíl Maghzi, and Steven C. Verrall, "Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption", Appl. Opt. 39, 4117 (2000).

[8] Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. 30(11), 1306–1308 (2005).

Breve descripción de la invención:

5 La presente invención aborda el problema de recuperación de la información libre de ruido, iniciando con una codificación previa de la información que se quiere proteger transformándola en un código gráfico (CG). Este CG se convierte en la imagen que se encripta mediante el sistema físico de encriptación.

10 Como se acaba de describir, existen aparatos ópticos de encriptación que usan elementos ópticos como lentes, divisores, proyectores, láser, etc. para almacenar y/o transmitir información de manera segura (encriptar); no obstante ninguno de esos sistemas o métodos ópticos permiten recuperar completamente libre de ruido o sin deterioro la información encriptada.

15 El sistema físico de encriptación de la presente invención es un dispositivo óptico que utiliza la propagación de la luz a través de una adecuada combinación de elementos ópticos como lentes, divisores, espejos, proyectores, polarizadores, placas y una máscara aleatoria física (llave de seguridad), para lograr ocultar de manera segura el CG. En este caso, la llave de seguridad es un elemento físico semi-transparente que introduce cambios aleatorios de fase permitiendo la encriptación y posterior recuperación de los CGs.

20 El CG encriptado con el montaje óptico-físico, se almacena digitalmente usando una cámara digital. La misma cámara también se usa para almacenar la información de la llave de seguridad usada para encriptar el CG.

25 El CG encriptado puede ser desencriptado nuevamente usando un sistema óptico virtual que simula los procesos de propagación de la luz a través de un montaje físico de desencriptación, donde la llave de seguridad es una máscara aleatoria de fase. El CG así recuperado contendrá ruido inherente tanto al proceso físico de encriptación como al proceso virtual de desencriptación.

30 Luego el CG desencriptado se procesa por sub-áreas, aplicándole a cada una un procedimiento de binarización, que disminuye el ruido presente en el CG desencriptado.

35 Finalmente el CG desencriptado y binarizado se decodifica para obtener la información originalmente almacenada en él. Esta "lectura" del CG desencriptado y binarizado garantiza la obtención de la información original sin ningún tipo de ruido.

De este modo se tiene un sistema de encriptación que tiene las ventajas de seguridad incorporadas por el sistema óptico-físico y una garantía de recuperación libre de ruido. Esta desenscriptación libre de ruido, hace la diferencia respecto a los demás sistemas ópticos de encriptación, lo cual es fundamental pues además de la alta seguridad lograda con la encriptación óptica, también se logra una alta confiabilidad sobre la recuperación de la información original protegida.

La diferencia fundamental entre la invención aquí reclamada y las patentes U.S. 5,903,648, U.S. 6,002,773, U.S. 6,519,340, U.S. 6,907,124, U.S. 7,221,760 y U.S. 7,684,098 radica en los siguientes dos puntos: (a) en la presente invención el dato a ser encriptado se convierte en un código gráfico; este procedimiento a diferencia de las otras propuestas de encriptación óptica usando dispositivos físicos, permite recuperar la información original sin ningún tipo de ruido y (b) la arquitectura consiste de un arreglo interferómetro tipo Mach Zehnder donde en el brazo objeto aparece un sistema 2f para el cual en el plano de entrada está el código gráfico en contacto con una máscara aleatoria de fase. Mientras que el brazo de referencia contiene la llave de seguridad que es un elemento semi-transparente que introduce cambios aleatorios de fase.

A continuación se relacionan algunas diferencias específicas entre la invención reclamada y el estado del arte existente.

En la patente U.S. 5,903,648 se usa un montaje holográfico diferente al aquí reclamado, principalmente en la disposición de los elementos y en la arquitectura de encriptación usada, la cual es 4f, donde la llave de seguridad está en el primer plano de Fourier. Además la imagen encriptada es registrada en una película holográfica y luego insertada en el sistema óptico para el proceso de recuperación de la información. En la presente invención la imagen encriptada y la llave de seguridad son registradas digitalmente para facilitar los procesos de transmisión y recuperación de la información. La patente U.S. 6,002,773, es una extensión de la anteriormente reseñada y se basa en el mismo procedimiento. En la patente U.S. 6,519,340 la imagen original se divide en una parte real y una parte imaginaria y luego es binarizada antes de ser encriptada; se usa una arquitectura de encriptación 4f y se basa completamente en un sistema óptico virtual. La patente U.S. 6,907,124 enseña un sistema no interferométrico con arquitectura de encriptación 4f basado en el método de contraste de fase; en este método la llave de seguridad es digital. En la patente U.S. 7,221,760, se presenta un sistema interferómetro para encriptar objetos tridimensionales. La luz proveniente directamente del objeto tridimensional se almacena holográficamente y se usa una técnica de levantamiento de fase con dos láminas retardadoras. La patente U.S. 7,684,098 relaciona un sistema

interferométrico para validar información basado en cuatro sub-sistemas y en la convolución de la imagen con un código aleatorio, este sistema emplea una arquitectura de transformada de Fourier conjunta para la verificación.

5 Otros documentos como JP2009099091 no hablan de un sistema de encriptación, pero sí indican el procedimiento de lectura del código QR, es decir al procesamiento para lograr que el CG sea identificable y leído. Este tipo de tecnología sólo representa una parte del sistema aquí reivindicado y no contempla los procesos de encriptación y dsenciptación como aquí se indica.

10

US2006097062 refiere una idea digital, que corresponde a una mezcla y recuperación de códigos. En la presente invención el código QR se emplea solo como un contenedor y ese contenedor se procesa óptica y físicamente.

15 **Descripción de las figuras:**

Fig. 1 Es un diagrama de bloques de los procesos de encriptación óptica-física y recuperación de acuerdo a la presente invención.

Fig. 2A Muestra un Código Gráfico correspondiente a la letra "A".

20

Fig. 2B Muestra un Código Gráfico correspondiente a las palabras "Optical Encryption".

Fig. 2C Muestra el Código Gráfico de la Fig. 2B y la subdivisión en secciones independientes.

25

Fig. 3A Es un diagrama esquemático (vista 3D) de un montaje óptico-físico usado en la técnica de encriptación de la presente invención.

Fig. 3B Es un diagrama esquemático (vista superior) de un montaje óptico-físico usado en la técnica de encriptación de la presente invención.

30

Fig.3C Es un diagrama esquemático (vista lateral) detallando solo el "brazo objeto" dentro del montaje óptico-físico usado en la técnica de encriptación de la presente invención.

35

Fig.3D Es un diagrama esquemático (vista 3D) detallando solo el "brazo de referencia" dentro del montaje óptico-físico usado en la técnica de encriptación de la presente invención.

Fig.4A Es un diagrama esquemático (vista 3D) detallando la proyección de un Código Gráfico dentro del montaje óptico-físico usado en la técnica de encriptación de la presente invención.

5 **Fig.4B** Es un diagrama esquemático (vista 3D) detallando el registro de la intensidad del objeto, usando el montaje óptico-físico de encriptación de la presente invención.

10 **Fig.4C** Es un diagrama esquemático (vista 3D) detallando el registro de la intensidad de la llave de seguridad, usando el montaje óptico-físico de encriptación de la presente invención.

15 **Fig.4D** Es un diagrama esquemático (vista 3D) detallando el registro del holograma de la llave de seguridad, usando el montaje óptico-físico de encriptación de la presente invención.

Fig. 5 Muestra la imagen encriptada del Código Gráfico de la Fig 2B, generada usando la técnica de encriptación de la presente invención.

20 **Fig. 6** Es un diagrama esquemático del proceso óptico virtual usado en la técnica de descryptación de la presente invención.

Fig. 7 Muestra el Código Gráfico de la Fig 5, descryptado usando la técnica de descryptación de la presente invención.

25 **Fig. 8** Muestra el proceso de binarización por sub-áreas sobre un Código Gráfico descryptado usando la técnica de la presente invención.

Fig. 9 Muestra el Código Gráfico descryptado de la Fig 7, binarizado usando la técnica de la presente invención.

30 **Fig. 10** Muestra la decodificación o lectura del Código Gráfico descryptado y binarizado de la Fig 9.

Descripción detallada de la invención:

35 La modalidad preferente de la presente invención se relaciona en la Figura 1, donde se ilustra un diagrama del proceso de encriptación y descryptación. Se inicia con un proceso 100 de codificación de la información que se quiere proteger, transformándola en un código gráfico (CG) 101. A continuación el CG se encripta mediante un sistema físico de encriptación 102, el cual es un montaje óptico-físico que utiliza elementos ópticos y

una máscara aleatoria física (elemento 9 en Fig. 3) que es la llave de seguridad que logra ocultar de manera segura el CG. El CG encriptado 105 y la llave de seguridad 107 se almacenan y/o se transmiten, para lo cual se pueden usar nuevamente mecanismos ópticos o se pueden usar medios digitales. Una vez se requiere recuperar el CG encriptado, se aplica el proceso de desencriptación 108 que se puede implementar físicamente con un montaje óptico experimental, o usando un montaje óptico virtual (Fig. 6) que simula los procesos de propagación de la luz a través de un sistema óptico-físico, donde se usa la imagen encriptada y la llave de seguridad almacenadas en los procesos 104 y 106. El CG recuperado 109, contendrá ruido inherente tanto al proceso 102 de encriptación, como al proceso 108 de desencriptación.

Luego el CG desencriptado se procesa por sub-áreas, aplicándole a cada una un procedimiento 110 de binarización, que disminuye el ruido presente en el CG desencriptado.

Finalmente el CG desencriptado y binarizado 113 se decodifica para obtener la información 115 originalmente almacenada en él. Esta "lectura" 112 del CG desencriptado y binarizado garantiza la obtención 114 de la información original sin ningún tipo de ruido.

Proceso para la encriptación de información

El primer paso del proceso de encriptación es la conversión de la información que se pretende proteger, en un Código Gráfico (CG), siendo dicho CG un "contenedor" de los datos a ser encriptados. El CG es una imagen que se genera con cualquier tipo de código matricial (bidimensional) o incluso un código de barras lineales. El CG como matriz de puntos (o de bloques) o código de barras, se puede generar con diferentes metodologías o codificaciones. En esta realización se usa la codificación empleada por los "Quick Response Code (QR code)" (ISO, IEC 18004: 2006), como los que se muestran en las Fig. 2A y Fig. 2B. Con esto se concluye con el proceso 100 de codificación presentado en la Fig. 1.

El CG generado, es luego proyectado dentro del montaje óptico de encriptación que se muestra en las Fig. 3A y Fig. 3B. El montaje óptico está configurado como un arreglo interferómetro tipo Mach Zehnder, donde la luz de una fuente de iluminación láser 14 es dividida en dos trayectorias por medio del divisor de haz 1, el cual puede ser un cubo divisor, una placa divisora, una película divisora o cualquier otro elemento que permita separar dos porciones de la energía de la luz de la fuente láser 14, de tal modo que se dirija cada porción de la luz dividida en dos caminos distintos. Una de las porciones de la luz dividida recorrerá el camino formado por un polarizador 2, un vidrio despulido (o

difusor, o vidrio esmerilado) 3, un Modulador Espacial de Luz (Spatial Light Modulator - SLM) 4, un segundo polarizador 5 y una lente 6; a este camino se le denomina camino o brazo objeto (Fig. 3C). La segunda porción de la luz dividida en el divisor 1, recorrerá el camino formado por los espejos 10 y 11, y el vidrio despulido (o difusor, o vidrio esmerilado) 9 que corresponde a la llave de seguridad; a este camino se le denomina camino o brazo de referencia (Fig. 3D). Por medio del divisor 7 (que puede ser un cubo divisor, una placa divisora, una película divisora o cualquier otro elemento con características similares al divisor 1), la porción de luz que recorre el brazo de referencia vuelve a combinarse con la porción de luz que recorre el brazo objeto, haciendo que ambas porciones de luz se dirijan, coincidan y se superpongan en un elemento de registro 8.

El haz de la fuente de iluminación láser 14, antes de ser dividida por el divisor 1, se expande por medio de un expansor 13 (que puede ser un filtro espacial, un objetivo o un juego de lentes) y se colima (generar un haz con frente de onda plano) por medio de una lente 12.

Los espejos 10 y 11 que se disponen en el brazo de referencia (Fig. 3D), se ubican de tal modo que la porción de luz que se propaga por dicho brazo, se dirija al divisor 7 que a su vez lo dirige al medio de registro 8 donde se superpondrá con la porción de luz que se propaga por el brazo objeto. El vidrio despulido 9 (llave de seguridad) se ubica entre el espejo 10 y el divisor 7.

Como ya se dijo, los polarizadores 2 y 5 están en el brazo objeto (Fig. 3C). El polarizador 2 se ubica en cualquier punto entre el divisor 1 y el SLM 4. El polarizador 5 se ubica en cualquier punto entre el SLM 4 y el divisor 7. Ambos polarizadores se posicionan en una configuración (ángulo) que permitan modular en amplitud al elemento SLM 4. El vidrio despulido 3 se ubica entre el divisor 1 y el SLM 4. La lente 6 es una lente convergente que se ubica entre el SLM 4 y el divisor 7, de tal suerte que la distancia de separación entre la lente 6 y el medio de registro 8 sea igual al valor de la distancia focal f de la lente 6; igualmente que la distancia de separación entre la lente 6 y el SLM 4 sea igual al valor de la distancia focal de la misma lente 6 (Fig. 3B). De este modo el SLM 4, la lente 6 y el medio de registro 8 forman un *sistema* $2f$, en cuyo plano de entrada queda ubicado el SLM 4 donde se proyecta o presenta el CG, y en cuyo plano de salida queda ubicado el medio de registro 8 donde además queda localizado el Plano de Fourier.

En la Fig. 4A se muestra esquemáticamente el CG 41 proyectado o presentado dentro del montaje óptico de encriptación usando el SLM 4. El CG 41 es la imagen o el objeto que será encriptado por el montaje óptico. Colocando el vidrio despulido 3 en contacto con el

SLM 4, y considerando el haz expandido y colimado de la fuente la iluminación 14, se puede expresar matemáticamente la transmitancia en el plano de entrada del sistema 2f en el "brazo objeto" como,

$$u_l(x_0, y_0) = cg_l(x_0, y_0) \cdot r(x_0, y_0) \quad \text{ecuación (1)}$$

donde $cg_l(x_0, y_0)$ representa el CG 41 proyectado en el SLM 4 y $r(x_0, y_0)$ representa la máscara aleatoria de fase inducida por el vidrio despulido 3 (Figura 3C). El haz expandido y colimado de la fuente de iluminación 14 genera el haz objeto al pasar por el divisor de haz 1. Cuando el haz objeto incide sobre el plano de entrada del sistema 2f y atraviesa la lente 6, a una distancia f delante de la lente 6, es decir en el medio de registro 8, se obtiene una distribución de campo $MG_l(u, v)$, que corresponde a la trasformada de Fourier del plano de entrada del brazo objeto (ecuación (1), Figura 3C).

El haz expandido y colimado de la fuente de iluminación 14 también genera el haz de referencia cuando es dividido por el divisor de haz 1. Dicho haz se refleja en los espejos 11 y 10 y luego incide sobre el vidrio despulido 9 (Figura 3D), donde este vidrio es la llave de seguridad del proceso de encriptación presentado en esta invención. Cuando el haz de referencia pasa a través del vidrio despulido 9, viaja hasta el divisor 7 el cual lo dirige al medio de registro 8. La distribución de luz generada por la llave de seguridad en el medio de registro es $K(u, v)$ (Figura 3D).

Como ya se dijo, en el medio de registro 8 se superponen las porciones de luz que se propagan por el brazo objeto y por el brazo de referencia. De este modo, con el montaje óptico en la disposición descrita, sobre el medio de registro 8 se obtiene la intensidad de la distribución de luz que contiene el CG encriptado,

$$I_l(u, v) = |MG_l(u, v)|^2 + |K(u, v)|^2 + MG_l^*(u, v) K(u, v) \exp[-2\pi i(\alpha v + \beta w)] + MG_l(u, v) K^*(u, v) \exp[2\pi i(\alpha v + \beta w)] \quad \text{ecuación (2)}$$

donde $\exp[2\pi i(\alpha v + \beta w)]$ representa la onda plana que viaja por el brazo de referencia, con α y β siendo los ángulos que ésta forma con el medio de registro 8, y $*$ representando el complejo conjugado. La anterior distribución de intensidad para esta realización, se registra con un dispositivo de captura de imágenes digital, como una cámara CCD o una cámara CMOS monocromática, aunque puede usarse cualquier medio sensible a la intensidad. La ecuación (2) contiene cuatro términos; el primero es la intensidad en el plano de Fourier del plano de entrada $|MG_l(u, v)|^2$, el segundo contiene la intensidad del campo que genera el vidrio despulido 9 (llave de seguridad) sobre el

medio de registro 8 $|K(u, v)|^2$, mientras que los términos tres y cuatro contienen la información del complejo conjugado del CG y el CG, ambos encriptados.

El siguiente paso en el proceso es extraer la información del dato encriptado de la

5 intensidad de la distribución (ecuación (2)). El término $|MG_l(u, v)|^2$ corresponde a la imagen de intensidad de la Transformada de Fourier del plano de entrada del sistema 2f, dicho término se registra directamente con la cámara 8, bloqueando la porción de luz que viaja por el brazo de referencia, como se ilustra en la Fig. 4B usando el elemento 15. El término $|K(u, v)|^2$ se obtiene directamente en el medio de registro 8 cuando se bloquea la

10 porción de luz que viaja por el brazo objeto usando el elemento 16, como se muestra en la Fig. 4C. Una vez capturadas estas dos últimas imágenes de intensidad, se restan de la distribución de intensidad descrita por la ecuación (2),

$$Q_l(u, v) = MG_l^*(u, v) K(u, v) \exp[-2\pi i(\alpha v + \beta w)] + MG_l(u, v) K^*(u, v) \exp[2\pi i(\alpha v + \beta w)] \quad \text{ecuación (3)}$$

El paso posterior es eliminar el primer término de la ecuación (3) para retener solamente la imagen del CG encriptado; con este objetivo se aplica una transformada de Fourier

15 sobre la ecuación (3),

$$n_l(x', y') = u_l^*(x', y_0) \otimes k(x', y') \otimes \delta(x' + \alpha \lambda f, y' + \beta \lambda f) + u_l(x', y_0) \otimes k^*(x', y') \otimes \delta(x' - \alpha \lambda f, y' - \beta \lambda f) \quad \text{ecuación (4)}$$

donde $k(x', y')$ es la transformada de Fourier de $K(u, v)$, λ es la longitud de onda de la fuente de iluminación láser 14 y el símbolo $\otimes$ corresponde a la operación de convolución. En este caso se obtienen dos términos cuya separación espacial depende de los ángulos α y β de la onda de referencia, la longitud de onda de iluminación λ y la longitud focal f

20 de la lente 6. Los parámetros antes mencionados se eligen para que no haya ningún tipo de superposición entre los términos de la ecuación (4), de tal manera que se puede eliminar el primer término en la ecuación (4) sin afectar el segundo término. Luego, el término restante, es reposicionado en unas nuevas coordenadas (x_l, y_l) , que son las que definirán la posición final del CG desencryptado en el plano de recuperación,

$$p_l(x', y') = u_l(x', y_0) \otimes k^*(x', y') \otimes \delta(x' - x_l, y' - y_l) \quad \text{ecuación (5)}$$

25 Nótese que el reposicionado puede ser llevado a cabo controlando la dirección de la onda plana de referencia (ecuaciones (4) y (5)); pero este procedimiento implicaría no solo introducir un elemento mecánico para controlar la dirección, sino además las complicaciones que traería sobre el montaje interferómetro introducir cambios en las direcciones de los haces.

Finalmente, al aplicar una transformada de Fourier inversa sobre la ecuación (5), se obtiene el CG encriptado:

$$E_i(u, v) = MG_i(u, v) K^*(u, v) \exp[2\pi i(x_i v + y_i w)] \quad \text{ecuación (6)}$$

En este punto, ya se tiene la imagen del CG encriptado y esta puede ser almacenada y/o transmitida para un usuario autorizado (proceso 104, Fig. 1). Un ejemplo del CG de la Fig. 2B una vez se ha encriptado con el procedimiento descrito en la presente realización, se puede ver en la Fig. 5. Es decir, en este punto ya se ha logrado el proceso 102 (Fig. 1) de encriptación con el montaje óptico.

Proceso de descriptación

Para el proceso 108 de descriptación (Fig. 1), es necesario obtener una versión digital del conjugado de la transformada de Fourier de la llave de seguridad 9 (Fig. 3A, Fig. 3B, Fig. 3D). Para ello en el montaje óptico-físico se remueve el vidrio despulido 3 (Fig. 3A, Fig. 3B, Fig. 3C) y se borra el CG del SLM 4 (el SLM 4 se deja transparente, sin proyección de imágenes), de tal forma que el montaje óptico-físico queda con la disposición que se puede ver en la Fig. 4D. Con esta configuración del montaje óptico-físico se hace el registro 106 (Fig. 1) del Holograma de la transformada de Fourier de la llave de seguridad 9, el cual se captura directamente con el medio de registro 8, y se puede representar matemáticamente como:

$$H(u, v) = |P_r(u, v)|^2 + |K(u, v)|^2 + P_r^*(u, v) K(u, v) \exp[-2\pi i(\alpha v + \beta w)] + P_r(u, v) K^*(u, v) \exp[2\pi i(\alpha v + \beta w)] \quad \text{ecuación (7)}$$

donde $P_r(u, v) = \exp[2\pi i(\alpha' v + \beta' w)]$ representa la onda plana que se propaga por el brazo objeto, con α' y β' como los ángulos que forma dicha onda con el medio de registro 8. Siguiendo un procedimiento similar al realizado para obtener el CG encriptado de la ecuación (6), se procede a extraer el complejo conjugado de la transformada de Fourier de la llave de seguridad $K^*(u, v)$ contenido en el cuarto término de la ecuación (7). El segundo término de la ecuación (7) ya fue almacenado en el proceso de obtención del CG encriptado. Luego se procede a bloquear el brazo de referencia para obtener en el medio de registro 8 el término $|P_r(u, v)|^2$. Al restar estos dos términos de la ecuación (7) se llega a:

$$T(u, v) = P_r^*(u, v) K(u, v) \exp[-2\pi i(\alpha v + \beta w)] + P_r(u, v) K^*(u, v) \exp[2\pi i(\alpha v + \beta w)] \quad \text{ecuación (8)}$$

Para remover el primer término de la ecuación (8), se aplica una transformada de Fourier,

$$t(x', y') = k(x', y') \otimes \delta(x' + \alpha' \lambda f, y' + \beta' \lambda f) \otimes \delta(x' + \alpha \lambda f, y' + \beta \lambda f) + k^*(x', y') \otimes \delta(x' - \alpha' \lambda f, y' - \beta' \lambda f) \otimes \delta(x' - \alpha \lambda f, y' - \beta \lambda f) \quad \text{ecuación (9)}$$

Los dos términos de esta ecuación poseen una separación que depende de los ángulos α , β , α' y β' de las ondas de referencia y objeto, la longitud de onda de iluminación λ y la longitud focal f de la lente 6. Luego de una elección cuidadosa de dichos parámetros se asegura que no habrá ningún tipo de superposición entre los dos términos de la ecuación (8), y por lo tanto será posible eliminar el primer término en la ecuación (9) sin afectar el segundo término. Luego el término restante, es reposicionado en el origen de coordenadas $(0,0)$, quedando expresado como:

$$h(x', y') = k^*(x', y') \quad \text{ecuación (10)}$$

Al aplicar una transformada de Fourier inversa sobre la ecuación (10), se obtiene finalmente el complejo conjugado de la transformada de Fourier de la llave de seguridad:

$$K^*(u, v) \quad \text{ecuación (11)}$$

Una vez se cuente con el CG encriptado (ecuación (6)) y la información de la llave de seguridad (ecuación (11)), estos datos pueden ser enviados por canales diferentes a un usuario autorizado para que recupere el CG y por tanto la información del CG original.

Para la recuperación del CG encriptado con el montaje y el proceso óptico-físico anterior, se procede a usar un sistema óptico-virtual, como el que se representa esquemáticamente en la Fig. 6, que simula un montaje óptico de recuperación, el cual permite realizar el proceso 108 (Fig. 1) de descryptación y recuperación de la información de manera rápida y cómoda para el usuario destinatario de dicha información. Es importante mencionar que la recuperación puede llevarse a cabo con un montaje óptico-físico o un sistema óptico virtual; la ventaja del sistema óptico-virtual es que es más cómodo para el usuario final.

En este proceso 108 de descryptación (Fig. 1), la imagen del CG encriptado 21 (Fig. 6), representado matemáticamente por $E_i(u, v)$ (ecuación (6)), se multiplica digitalmente con la llave de seguridad digital 22, representada matemáticamente por $K^*(u, v)$ (ecuación 11), obteniendo el campo óptico del plano de entrada O del sistema óptico virtual de la Fig. 6. Paso seguido, se simula una iluminación con onda plana coherente 20 y la propagación 23 de dicho campo óptico a lo largo de una distancia f y a través de una lente convergente virtual 24, cuya distancia focal es también igual a f . Finalmente se simula una nueva propagación 25 del campo óptico por una distancia de nuevo igual a f . Con esto, se simula un sistema $2f$, donde en el plano de salida R se obtiene la Transformada de Fourier del campo óptico presente en el plano de entrada O . De este modo, en el plano de salida R , se obtiene matemáticamente:

$$d(x, y) = cg_i(x, y) \cdot r(x, y) \otimes \delta(x - x_l, y - y_l) \quad \text{ecuación (12)}$$

La ecuación (12) es el CG descriptado, que contiene el CG original multiplicado por una máscara de fase aleatoria; este término corresponde a la transmitancia en el plano de entrada para el "brazo objeto" durante el proceso de encriptación (ecuación (1)). Dicho producto estará posicionado en las coordenadas (x_l, y_l) del plano R . Si las coordenada (x_l, y_l) seleccionadas durante el posicionamiento corresponden a $(0,0)$ y se toma la intensidad de la imagen descriptada (ecuación (12)) se recupera el CG centrado en el plano de reconstrucción:

$$|d(x, y)|^2 = |cg_l(x_0, y_0)|^2 \quad \text{ecuación (13)}$$

Esta última expresión corresponde al CG descriptado (Figura (7)), que se obtiene como "salida" 26 del sistema óptico-virtual descrito (Figura 6).

El éxito de los procesos de encriptación y descriptación depende en gran medida de las características de los elementos involucrados en el proceso. Existen algunas limitaciones del medio de proyección de los CGs (SLM 4), del medio de registro 8 y de la lente 6, que restringen el tipo de CGs que pueden ser encriptados y recuperados adecuadamente con el procedimiento descrito. Estas limitaciones están relacionadas con la resolución y dimensiones físicas del sistema de proyección (SLM 4) y del medio de registro 8, así como de la calidad y las dimensiones físicas de la lente 6.

Para sobrepasar esas limitaciones y procesar CGs con cualquier contenido de información, se debe dividir el CG en varias secciones de igual tamaño; luego cada sección se proyecta en el modulador al mismo tamaño que se proyectaría el CG completo. Siguiendo el procedimiento descrito entre las ecuaciones (1) a (6) para una de las secciones del CG, se puede almacenar dicha sección encriptada del CG $E_l(u, v)$ (ecuación (6)); si se sigue el mismo procedimiento para las secciones restante del CG y luego se suman todas las secciones del CG encriptadas individualmente se obtiene:

$$M(u, v) = \sum_{l=1}^n MG_l(u, v) K^*(u, v) \exp[2\pi i(x_l v + y_l w)] \quad \text{ecuación (14)}$$

Donde n es el número de secciones en que se dividió el CG (en el ejemplo de la Fig 2C, $n = 16$). Esta última ecuación representa el CG encriptado, donde se eligen cuidadosamente las coordenadas (x_l, y_l) durante la encriptación de cada sección del CG para que en la descriptación se pueda recuperar el CG adecuadamente. Para descriptar el CG, se sigue el mismo procedimiento 108 (Fig. 1) que se describió en el caso de la recuperación de un CG que se procesa en un solo paso, es decir, sin el proceso de división en secciones. Por lo tanto, se multiplica el CG encriptado (ecuación (14)) por la información de la llave de seguridad (Ecuación 11), y luego de una transformada de Fourier se obtiene:

$$d(x, y) = \sum_{l=1}^n c g_l(x, y) \cdot r(x, y) \otimes \delta(x - x_l, y - y_l) \quad \text{ecuación (15)}$$

Como se observa en la ecuación (15), se descriptan todas las secciones en un solo paso, en el mismo instante y en el mismo plano $\mathbf{R}$ (Fig. 6). De manera que la elección adecuada de las coordenadas (x_l, y_l) para cada sección del CG, permite la descriptación óptima del código GC. El número de divisiones n en que se debe dividir un CG para que este se pueda encriptar y recuperar adecuadamente, depende de las características de los elementos del montaje experimental y de la cantidad de información contenida en el CG. El procedimiento acá descrito garantiza la adecuada encriptación y descriptación de CGs con cualquier contenido usando equipos comercialmente disponibles de gama baja o media.

En la Fig. 7 se muestra como ejemplo, el CG obtenido al llevar a cabo el proceso de descriptación sobre el CG encriptado que se muestra en la Fig. 5. La imagen del CG descriptado contendrá ruido inherente tanto al proceso óptico-físico de encriptación como al proceso óptico-virtual de descriptación. Este tipo de ruido se aprecia como una estructura granulosa (ruido speckle) y se presenta esencialmente por el uso de una máscara aleatoria de fase como llave de seguridad. La escogencia en esta invención de un CG como contenedor de la información encriptada, permite precisamente resolver el problema del impacto del ruido sobre la información recuperada luego del proceso de descriptación, permitiendo que aunque el CG descriptado presente ruido, la decodificación o lectura de dicho CG entregue la información original sin ningún tipo de deterioro. De este modo se tiene un sistema de encriptación que tiene las ventajas de seguridad incorporadas por el sistema óptico-físico y con una llave de seguridad física y aleatoria, y una garantía de recuperación de la información libre de ruido.

Para mejorar el procedimiento 112 (Fig. 1) de lectura o decodificación del CG descriptado, al CG con ruido se le aplica un proceso 110 de binarización (Fig. 1), con la cual se logra una adecuada y rápida lectura del CG. Este proceso de binarización se aplica por sub-áreas sobre el CG descriptado, aprovechando la estructura del CG, que como ya se dijo consiste de bloques cuadrados blancos y negros, organizados en una rejilla cuadrada. De este modo, el CG descriptado se divide en sub-áreas (31, Fig. 8) que coinciden con cada bloque de la estructura del CG. Luego, para cada sub-área se calcula el promedio de todos los valores de pixel que se encuentran dentro de dicha región del CG descriptado y a continuación, todos estos pixeles de la sub-área procesada se reemplazan por el valor promedio de pixel calculado. Esto se repite de manera independiente para cada sub-área, con lo que se obtiene un CG cuyos bloques 32 (Fig. 8) contendrán píxeles homogéneos y por tanto ya no presentan la estructura

granulosa del ruido descrito anteriormente. Finalmente este CG procesado por sub-áreas, se binariza para obtener un CG cuyos bloques 33 (Fig. 8) son blancos o negros.

En la Fig. 9 se presenta un ejemplo del CG descryptado de la Fig. 7, una vez se ha hecho el proceso 110 (Fig. 1) de binarización por sub-áreas.

Una vez se tiene el CG descryptado, homogéneo y binarizado, se realiza el proceso de decodificación 112 para recuperar 114 la información 115 originalmente almacenada en él (Fig. 1). Esta "lectura" del CG descryptado, homogéneo y binarizado garantiza la obtención de la información original sin ningún tipo de ruido.

Para esta realización, en la que se emplea como CG los códigos QR, el procedimiento 112 (Fig. 1) de "lectura" del código QR se realiza con la metodología descrita en el estándar que define dicha codificación (ISO, IEC 18004: 2006, "Information technology - Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification," International Organization for Standardization, Geneva, Switzerland (2006)).

En la Fig. 10 se muestra un ejemplo del resultado de la "lectura" del CG descryptado y binarizado de la Fig. 9, mostrando la perfecta recuperación de la información original con la que se inició el proceso de encriptación descrito en la presente invención.

Se destaca que todo el proceso de recuperación de la información encriptada se puede realizar usando un único dispositivo, en el que se hacen los procesos 108 de descryptación, 110 de binarización y 112 de lectura del CG.

Ventajas técnicas

Tal como se describió anteriormente, según esta realización se tiene un montaje óptico-físico y una metodología de encriptación que posee dos características fundamentales en un sistema de encriptación: se asegura una alta protección de los datos contra el acceso de usuarios no autorizados y se garantiza que la información recuperada es completamente fiel a la original.

La seguridad de la información encriptada respecto al acceso de usuarios no autorizados, se logra por el proceso óptico-físico en el cual un CG es proyectado en un SLM 4 y por medio de la propagación de campos ópticos a través de diferentes elementos ópticos, se encripta usando una llave de seguridad, en forma de una máscara aleatoria de fase producida por un vidrio despulido 9.

En esta realización el CG encriptado y la llave de seguridad son registrados y almacenados como imágenes en el medio de registro 8, lo cual facilita el proceso de envío de la información encriptada y la llave de seguridad, usando distintos canales de transmisión para cada uno.

80

El proceso de recuperación de la información que emplea un sistema óptico-virtual de descryptación, un proceso de binarización y la lectura final del CG descryptado, se puede implementar en un único sistema para el usuario autorizado final receptor de dicha información.

La recuperación de la información descryptada libre de ruido y fiel a la original, se logra en esta realización al emplear un CG que codifica la información en forma de código QR, que garantiza una inmunidad sobre el ruido introducido por el proceso óptico de encriptación y descryptación, de modo que la lectura del CG descryptado entrega la información completamente fiel a la original.

De este modo se tiene un sistema de encriptación que tiene las ventajas de seguridad incorporadas por el sistema óptico-físico y una garantía de recuperación de la información encriptada totalmente libre de ruido.

Variantes

La invención actual puede ser implementada usando muchas variantes de sistemas de encriptación que son conocidas ampliamente en la literatura ya que han sido publicadas en revistas internacionales; dichas variantes no aportan o modifican el impacto de la presente invención. Pero la idea presente en esta invención se puede unir fácilmente con estas variantes para crear sistemas alternativos de seguridad. Las variantes pueden corresponder a diferentes formas de obtener los códigos gráficos, cambiar la ubicación de los elementos físicos que conforman el dispositivo óptico o incluir elementos físicos nuevos en el instrumento óptico. Además, tanto la invención presente como sus posibles variantes pueden implementarse en el dominio de sistemas ópticos virtuales, que son simulaciones digitales del montaje óptico-físico; Asimismo se puede presentar adaptaciones híbridas en los cuales se usa un montaje óptico-físico para el proceso de encriptación y un sistema óptico virtual para la recuperación, o viceversa. En lo que sigue, se mostrarán las diferentes posibilidades de implementación de la invención presente en las diferentes variantes.

La invención presente puede ser implementada usando una arquitectura de encriptación $4f$. La denominación $4f$ se debe a que utiliza dos lentes de longitud focal f , una ubicada a una distancia f del plano de entrada y la segunda a una distancia $2f$ de la primera, de esta

forma el plano de salida se ubica a una distancia f de la segunda lente para que la distancia entre el plano de entrada y el plano de salida se $4f$. Este dispositivo de encriptación posee dos máscaras aleatorias de fase, una en el plano de entrada y la segunda ubicada a una distancia f delante de la primera lente; esta segunda máscara es la llave de seguridad. Esta variación puede servir para encriptar múltiples datos, donde el dato encriptado de uno de los objetos es la llave del otro o donde se pueden encriptar múltiples datos complejos; además junto con una técnica de modulación theta se pueden encriptar videos en tonos de gris o a color. Asimismo, implementando la invención actual en esta arquitectura es posible encriptar múltiples datos cambiando la longitud de onda de iluminación, usando múltiples pupilas, cambiando la polarización del sistema, realizando desplazamientos sobre la llave de seguridad, modificando la pupila del sistema, combinando máscaras de amplitud y fase, escalando la llave de seguridad, incluyendo fibras ópticas para el procesamiento, insertando máscaras de seguridad estructuradas, iluminando incoherentemente, con un potencial inducido ópticamente, empleando conteo de fotones, introduciendo elementos ópticos difractivos, por medio de modulación de amplitud, con encriptación de fase pura, utilizando ptychography, con proyecciones a tiempo real o usando encriptación por polarización.

La variantes a la presente invención también incluyen la arquitectura óptica de correlador de transformada conjunta, donde el dato a encriptar y la llave de seguridad están en el plano de entrada de un sistema que contiene solo una lente. Este sistema es inherentemente holográfico y por lo tanto el dato encriptado se obtiene a través de la intensidad de la transformada de Fourier del plano de entrada. Al cambiar la posición de la llave de seguridad y luego mediante desplazamientos controlados de la misma se pueden encriptar múltiples datos. Aplicando un procedimiento de posicionamiento durante la encriptación es posible encriptar múltiples datos y luego recuperarlos sin la influencia de los otros datos involucrados. Implementado la presente invención en esta técnica se puede: encriptar múltiples datos y recupera solo uno de ellos evitando la superposición de la información proveniente de los objetos no descriptados, incluir una llave maestra para evitar el uso de la onda de referencia externa, encriptar videos, multiplexar datos encriptados rotando la llave de seguridad, multiplexar secciones de un dato estructurado para lograr su correcta recuperación, proteger datos de cualquier longitud, usar fractales para encriptar uno o múltiples datos, y usar desplazamiento de fase para proteger información.

Algunos procesos de protección de datos puede generarse en sistemas interferométricos utilizando como base la invención aquí descrita. Implementado la presente invención es posible proteger información: de pura fase, empleando dos máscaras aleatorias, con eliminación de silueta, considerando cada punto del objeto como una partícula, en un

interferómetro de Michelson, por medio de llaves asimétricas y planos fraccionales, incluyendo múltiples llaves, manipulando la polarización de la iluminación, empleando hologramas generados por computador o insertando desplazamientos de fase.

- 5 Otras variantes incluyen dominios fraccionales de Fourier: con múltiples canales, y desplazamientos aleatorios, incluyendo múltiples parámetros, o multiplexado de máscara aleatoria, además se puede implementar una técnica en dominios multi-fraccionales de Fourier. Respecto a la disposición de elementos en el sistema óptico-físico u óptico virtual, la idea presente en la actual patente permite generar un sistema de seguridad empleando
- 10 las arquitecturas de Fresnel o las transformadas afines; asimismo se pueden utilizar arquitecturas que incluyen la transformada: Hartley, de rotación, jigsaw, Arnold, Mellin o coseno discreta. Otros sistemas pueden incluir simultáneamente transformadas de Fourier y Fresnel.
- 15 Otras variantes pueden incluir sistemas de seguridad basados en formación computacional de imágenes fantasmas, procesos térmicos, elementos difractivos, procesamiento asimétrico con modulación aleatoria o sensado de frente de onda, holografía de compresión o máscaras caóticas. En la línea de compresión de información se puede usar la idea presente en la patente actual para recuperar información libre de
- 20 ruido en procesos de compresión de información usando procesadores ópticos, máscaras aleatorias y modulación theta, o en procedimientos que mezclan encriptación y compresión usando posicionamiento o modulación theta.

Diferentes realizaciones

- 25 El proceso 100 (Fig. 1) de codificación de la información en un CG, según la realización 2 se genera empleando metodologías o codificaciones distintas a los códigos QR. Pueden usarse los "Datamatrix" o "Semacode" (ISO/IEC16022 - International Symbology Specification), los "PDF417" (ISO/IEC 15438), los códigos de barras lineales que permiten codificar datos alfanuméricos como "Code 128", "Code 39", "Code 93", o en general
- 30 cualquier otro tipo de codificación que permita de manera sistemática y controlada, la conversión de información alfanumérica en una imagen o código gráfico bidimensional.

En esta realización, los procesos subsiguientes de encriptación 102 (Fig. 1), de almacenamiento del CG encriptado 104 y de la llave de seguridad 106, de desencriptación

35 108 y binarización 110 del CG recuperado, se realizan de manera idéntica a la descrita en la realización 1.

23
53

El proceso de lectura 112 y recuperación final de la información 114, se debe realizar con la metodología indicada por el sistema de codificación particular que se emplee en el proceso inicial de codificación 100.

5 Los efectos de esta realización son los mismos que los descritos en la realización 1.

Realización 3

El sistema de proyección de los CG en el montaje óptico

10 El Modulador Espacial de Luz 4, puede reemplazarse por un sistema de proyección de imágenes dinámico, ya sea por transmisión o por reflexión, moduladas en fase o en intensidad. También se podrían emplear dispositivos como espejos segmentados.

Realización 4

El Sistema 2f

15 La distancia entre el SLM 4 y la lente 6 puede configurarse con un valor distinto a la distancia focal de la lente 6. En tal caso, el plano de salida del sistema en el medio de registro 8, contendrá la Transformada de Fourier del objeto proyectado en el SLM y adicionalmente contendrá un factor de fase cuadrático que depende de la distancia entre el SLM 4 y la lente 6.

20

Realización 5

El sistema de iluminación

25 El sistema de iluminación colimado logrado con la fuente de iluminación láser 14, el expensor 13 y la lente 12, puede modificarse o cambiarse por cualquier sistema de iluminación coherente colimado. También se puede emplear un sistema de iluminación coherente divergente o convergente

Realización 6

Proceso de descryptación

30 El sistema de encriptación es un sistema físico que permite proveerle seguridad a la información que se oculta. En la realización 1, la recuperación se lleva a cabo con un sistema óptico-virtual que simula un montaje óptico de recuperación. La recuperación también puede hacerse mediante un montaje óptico-físico.

24
~~54~~

REIVINDICACIONES

1. Un método de encriptación de datos que comprende los pasos de:
 - a) convertir la información que se desea proteger en un código gráfico (41);
 - b) proyectar el código gráfico (41) sobre un modulador espacial de luz (4);
 - c) dividir el haz de luz de una fuente de iluminación láser (14) en dos trayectorias: un camino objeto y un camino de referencia;
 - d) hacer pasar el camino objeto por el modulador espacial de luz;
 - e) desviar el camino de referencia mediante espejos (10, 11) de tal forma que este no pase por el modulador espacial de luz (4);
 - f) hacer pasar el camino de referencia por un vidrio difusor (9);
 - g) volver a unir los caminos de objeto y referencia;
 - h) dirigir el nuevo haz de luz combinado a un elemento de registro (8);
 - i) registrar la luz recibida, que corresponde a la superposición de ambos caminos, este registro corresponde al código encriptado;
 - j) bloquear el camino objeto;
 - k) registrar, en el elemento de registro, la luz recibida, que corresponde únicamente al camino de referencia, este registro corresponde a la llave de seguridad.
2. El método según la reivindicación 1, en donde el código gráfico (41) es seleccionado entre el grupo que consiste de un código de barras lineales, un código matricial bidimensional y un código QR.
3. El método según cualquiera de las reivindicaciones anteriores, en donde el camino objeto se hace pasar, antes del modulador espacial de luz (4) por un vidrio difusor (3).
4. El método según la reivindicación 3, en donde el camino objeto se hace pasar, después del modulador espacial de luz (4), por una lente convergente (6).
5. El método de la reivindicación 4, en donde el camino objeto se hace pasar, antes del vidrio difusor (3), por un polarizador (2), y, después del modulador espacial de luz (4), por un segundo polarizador (5).
6. El método según la reivindicación 4 ó 5, en donde la lente convergente (6) se ubica de forma equidistante al modulador espacial de luz (4) y al elemento de registro (8), y en donde la distancia desde la lente convergente (6) hasta cualquiera de dichos elementos (4, 8) es igual a la distancia focal (f) de dicha lente (6).
7. El método según cualquiera de las reivindicaciones anteriores, en donde, antes de ser dividido, el haz de luz se hace pasar por un expansor (13).

25
85

8. El método según la reivindicación 7, en donde, después de pasar por el expansor (13), el haz de luz se colima mediante un lente (12).
9. Un método para descryptar datos, encriptados mediante el método de cualquiera de las reivindicaciones anteriores, que comprende los pasos de:
 - a) transmitir la información del código encriptado y de la llave de seguridad a un usuario autorizado;
 - b) mediante un sistema óptico, poner en contacto el código encriptado con la llave de seguridad ¿conjugado de la llave? para recuperar el código gráfico (41);
 - c) obtener, del código gráfico (41), los datos originalmente encriptados.
10. El método según la reivindicación 9, en donde el código de seguridad y la llave de seguridad se transmiten al usuario autorizado por canales diferentes.
11. El método según la reivindicación 9 ó 10, en donde el paso b) se realiza mediante un montaje óptico-físico.
12. El método según la reivindicación 9 ó 10, en donde el paso b) se realiza mediante un montaje óptico-virtual.
13. Un montaje para encriptar datos caracterizado porque comprende:
 - Una fuente de iluminación láser (14);
 - un divisor de haz (1) que divide el haz de la fuente de iluminación láser (14) en dos haces: uno de objeto y uno de referencia;
 - un modulador espacial de luz (4) en la trayectoria del haz de objeto;
 - espejos (10, 11) para desviar el haz de referencia;
 - un vidrio difusor (9) ubicado en la trayectoria del haz de referencia;
 - un divisor (7), en el cual se unen los haces de objeto y de referencia;
 - un elemento de registro (8);
 - un elemento de bloqueo de luz (15) para bloquear selectivamente el haz de referencia.
14. El montaje según la reivindicación 13, en donde el divisor de haz se selecciona del grupo que consiste de un cubo divisor, una placa divisora o una película divisora.
15. El montaje según la reivindicación 13 ó 14, que comprende además un vidrio difusor (3) entre el divisor de haz (1) y el modulador espacial de luz (4).
16. El montaje según la reivindicación 15, en donde el vidrio difusor (3) es un vidrio despolido o un vidrio esmerilado.

17. El montaje según cualquiera de las reivindicaciones 13 a 16, que comprende además una lente convergente (6) entre el modulador espacial de luz (4) y el divisor (7).
18. El montaje según la reivindicación 17, que comprende además un polarizador (2) antes del vidrio difusor (3) y un segundo polarizador (5) después del modulador espacial de luz (4).
19. El montaje según cualquiera de las reivindicaciones 13 a 18, en donde el divisor (7) se selecciona del grupo que consiste de un cubo divisor, una placa divisora o una película divisora.
20. El montaje según cualquiera de las reivindicaciones 13 a 19, que comprende además un expansor (13) entre la fuente de iluminación láser (14) y el divisor de haz (1).
21. El montaje según la reivindicación 20, que comprende además un lente (12) entre el expansor (13) y el divisor de haz (1) para colimar el haz de luz.
22. El montaje según cualquiera de las reivindicaciones 13 a 21, en donde el vidrio difusor (9) está ubicado entre el espejo (10) y el divisor (7).
23. El montaje según cualquiera de las reivindicaciones 13 a 22, en donde el elemento de registro (8) se selecciona del grupo que consta de una cámara CCD y una cámara CMOS monocromática.
24. El montaje según cualquiera de las reivindicaciones 17 a 23, en donde la lente convergente (6) se ubica de forma equidistante al modulador espacial de luz (4) y al elemento de registro (8), y en donde la distancia desde la lente convergente (6) hasta cualquiera de dichos elementos (4, 8) es igual a la distancia focal (f) de dicha lente (6).
25. El método según cualquiera de las reivindicaciones 1 a 8, en donde el modulador espacial de luz (4) se reemplaza por un sistema de proyección de imágenes dinámico.
26. El método según cualquiera de las reivindicaciones 1 a 8, en donde el modulador espacial de luz (4) se reemplaza por espejos segmentados.
27. El montaje según cualquiera de las reivindicaciones 13 a 23, en donde el modulador espacial de luz (4) se reemplaza por un sistema de proyección de imágenes dinámico.
28. El montaje según cualquiera de las reivindicaciones 13 a 23, en donde el modulador espacial de luz (4) se reemplaza por espejos segmentados.

RESUMEN

La presente invención proporciona un sistema físico de encriptación en el cual un haz de luz pasa por un código gráfico (CG) y otro haz de luz pasa por una máscara aleatoria física (llave de seguridad), ambos haces se juntan para ocultar de manera segura el CG. En este caso, la llave de seguridad es un elemento físico semi-transparente que introduce cambios aleatorios de fase permitiendo la encriptación y posterior recuperación de un CG. El CG encriptado con el montaje óptico-físico, se almacena digitalmente usando una cámara digital. La misma cámara también se usa para almacenar la información de la llave de seguridad usada para encriptar el CG. El CG encriptado puede ser desencriptado nuevamente usando un sistema óptico virtual que simula los procesos de propagación de la luz a través de un montaje físico de desencriptación, donde la llave de seguridad es una máscara aleatoria de fase.

FIGURAS

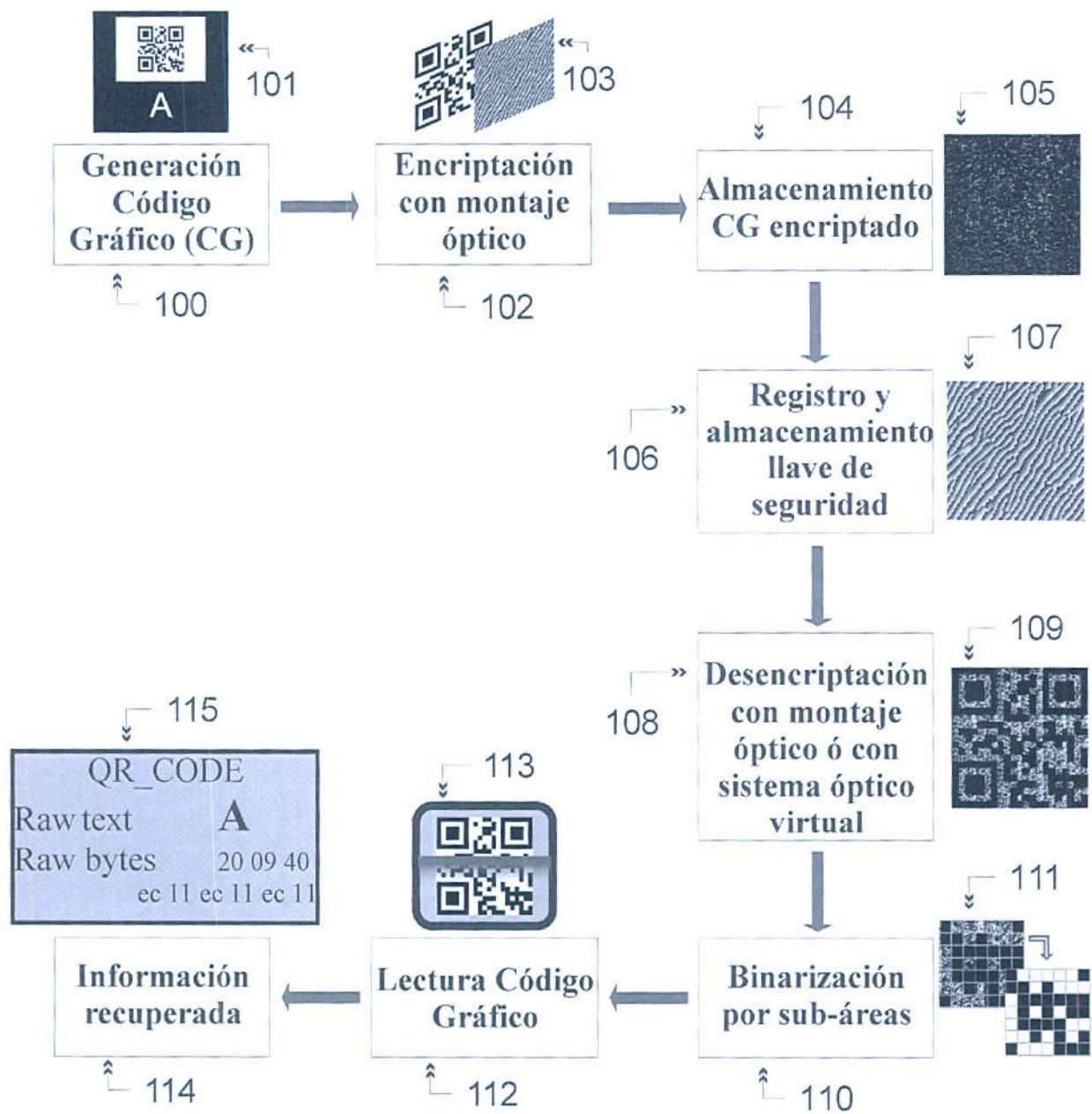


Fig. 1

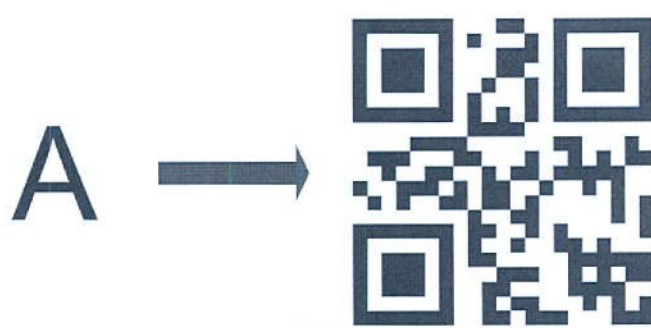


Fig. 2A

Optical
Encryption

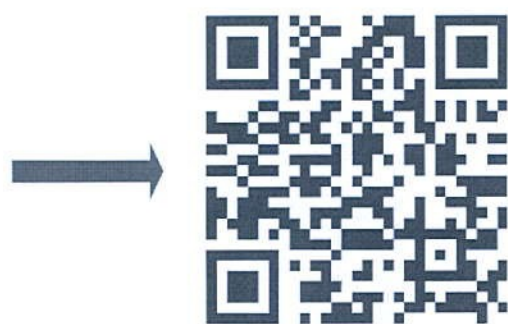


Fig. 2B

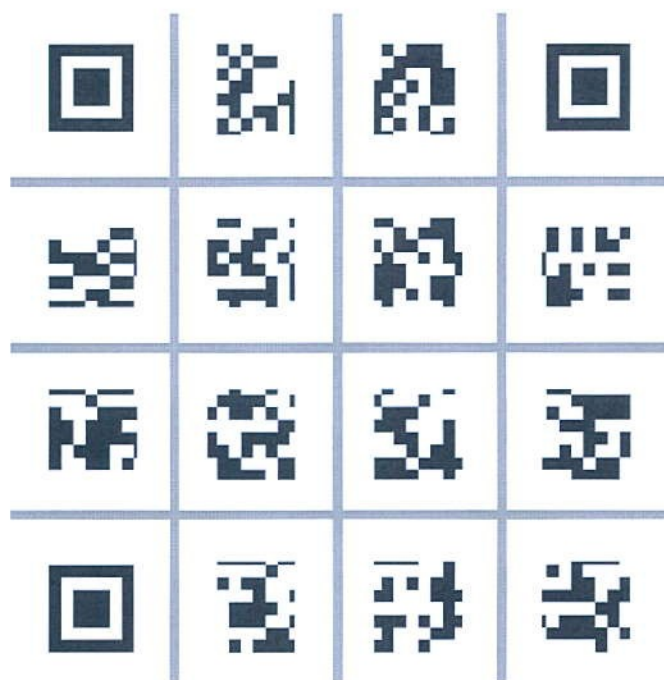


Fig. 2C

30
60

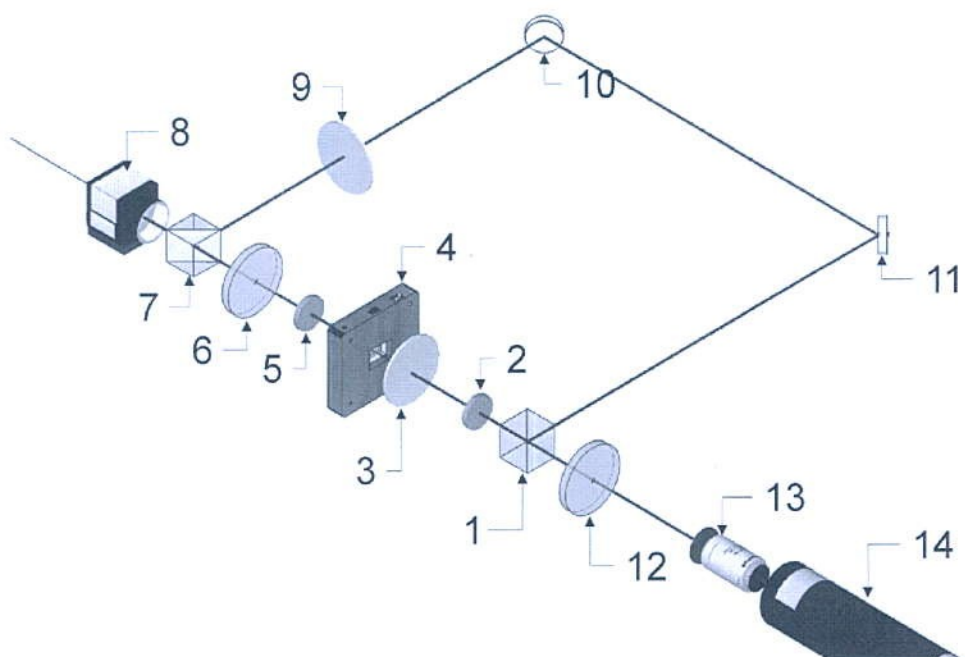


Fig. 3A

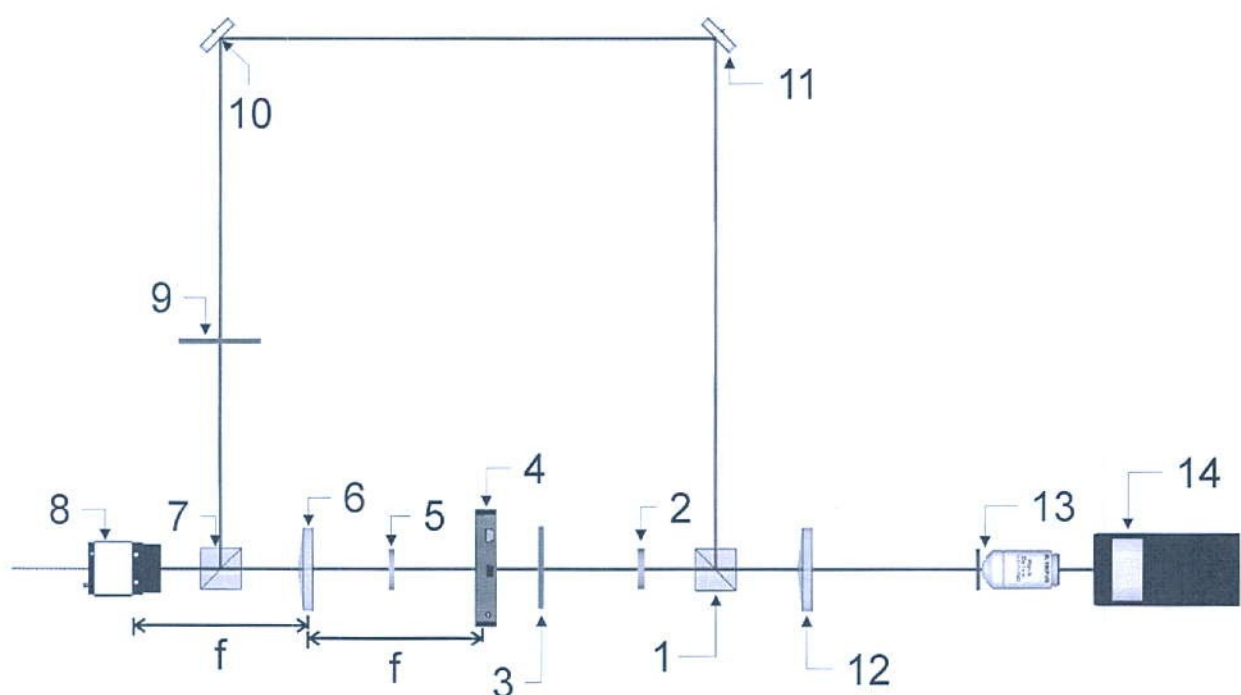


Fig. 3B

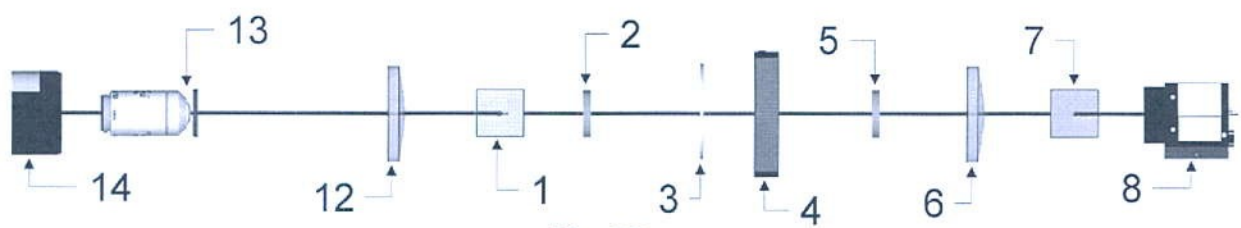


Fig. 3C

31
61

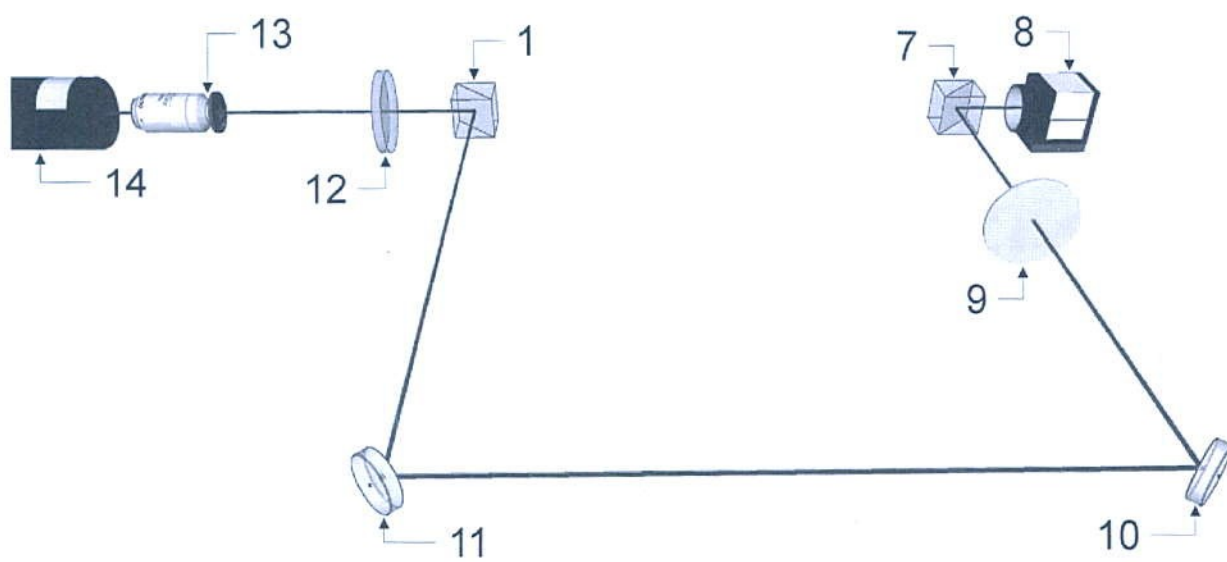


Fig. 3D

32
~~62~~

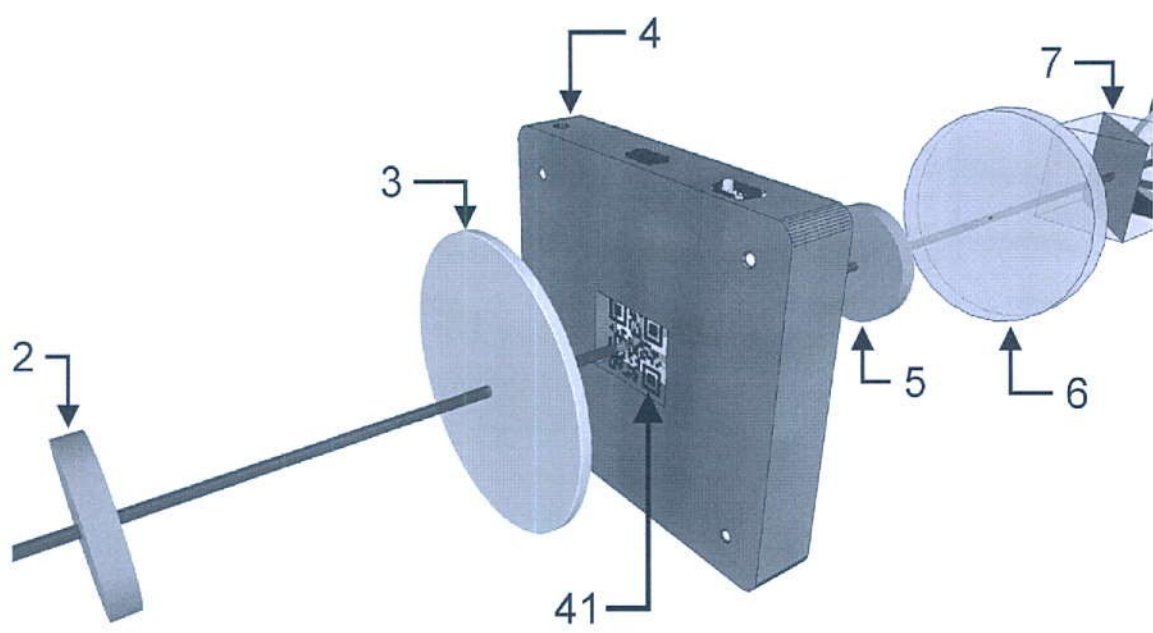


Fig. 4A

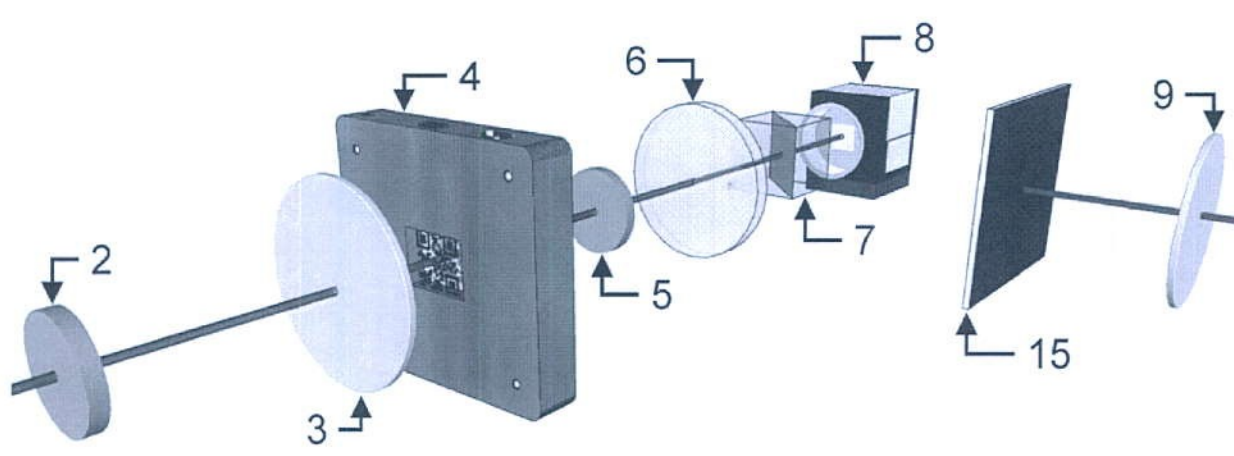


Fig. 4B

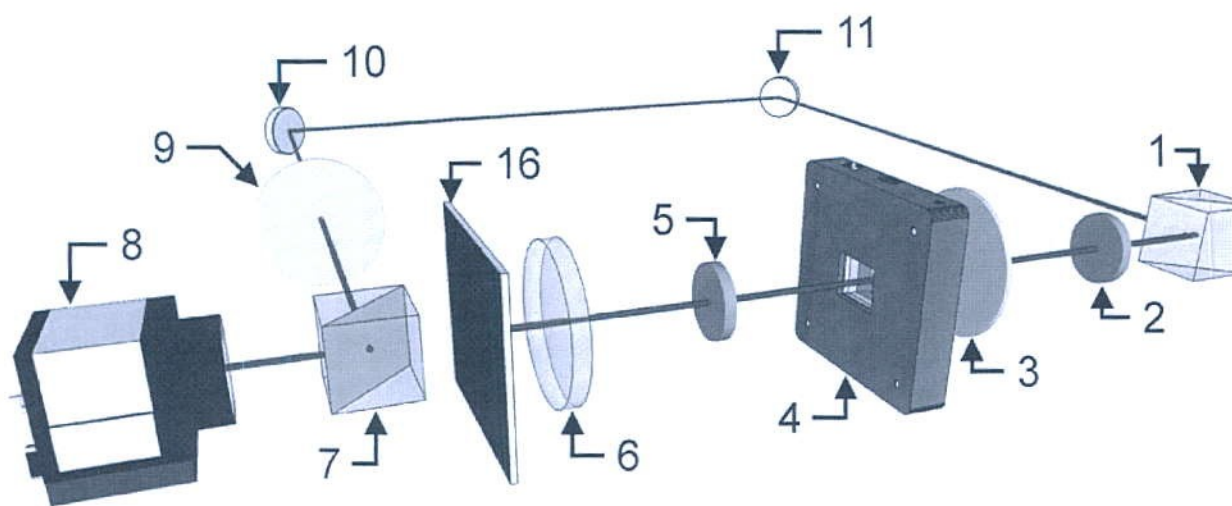


Fig. 4C

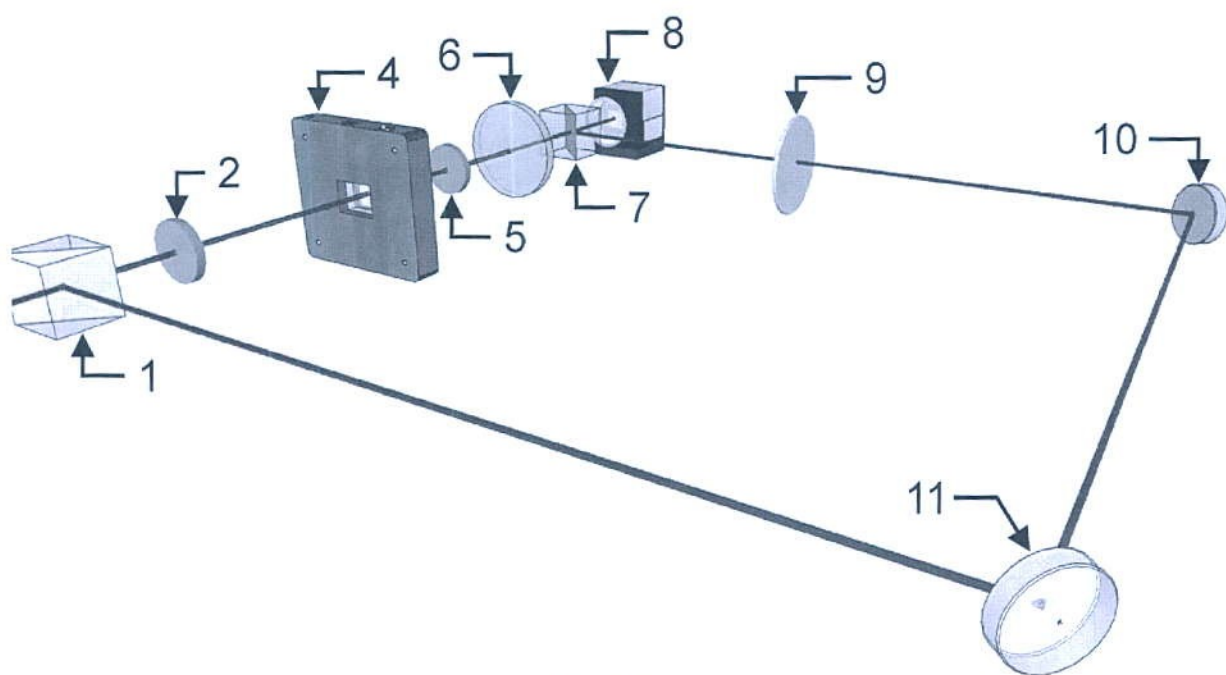


Fig. 4D



Fig. 5

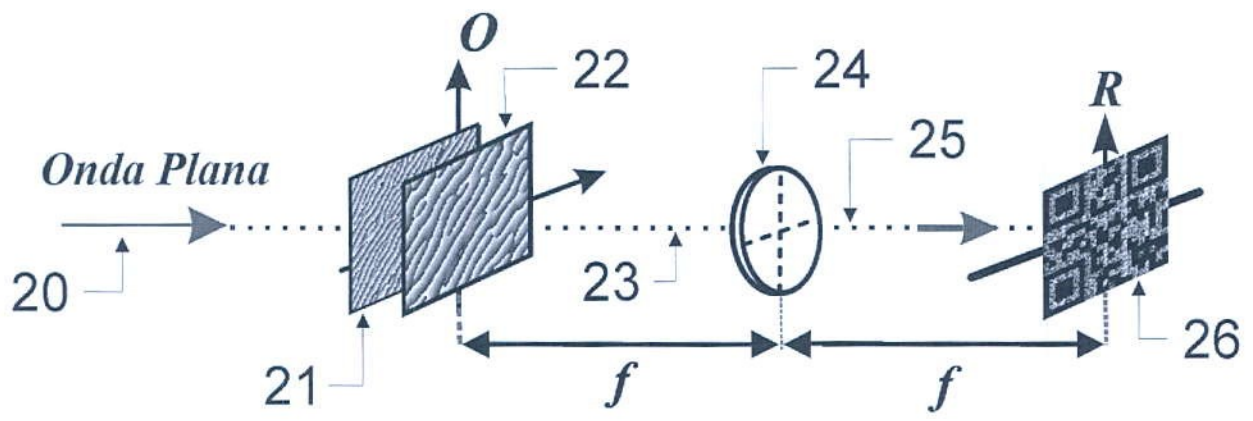


Fig. 6

35
65

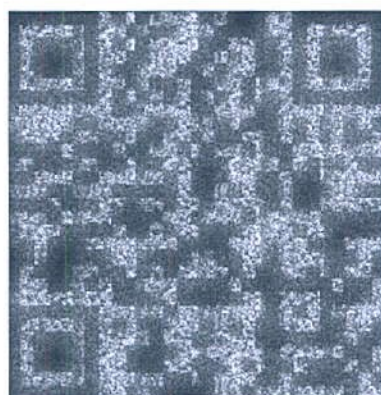


Fig. 7

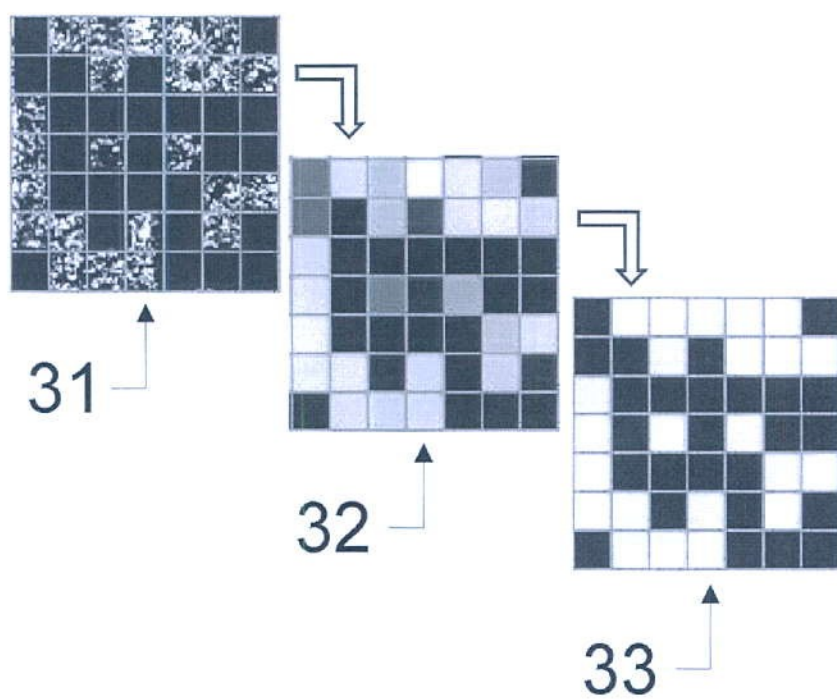


Fig. 8



Fig. 9

36
66

QR_CODE

Raw text **Optical**

Encryption

Raw bytes

41 24 f7 07 46 96 36 16 c0

a4 56 e6 37 27 97 07 46 96

f6 e0 ec 11 ec 11 ec 11

Fig. 10

37
~~67~~

CAVELIER

ABOGADOS
EDIFICIO SISKI
CARRERA 4ª N° 72-35
BOGOTÁ, 8 - COLOMBIA

213

Poder especial para uso en Colombia
para Propiedad Industrial (persona
jurídica)

Señor Director

DIRECCION DE NUEVAS CREACIONES

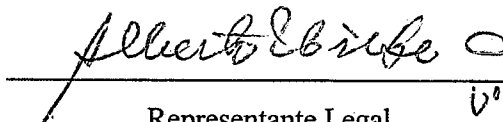
Superintendencia de Industria y Comercio

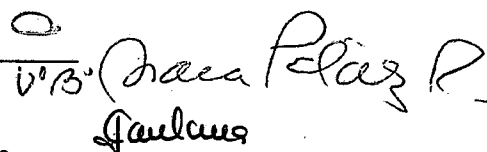
E. S. D.

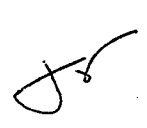
Yo, ALBERTO URIBE CORREA, Representante Legal de la UNIVERSIDAD DE ANTIOQUIA, domiciliada en la Calle 67 # 53-108 en Medellín, confiero poder a los doctores **LUZ CLEMENCIA DE PAEZ**, T.P.A. No. 23.555, identificada con cédula de ciudadanía número 35.456.344 de Usaquén, **JORGE CHÁVARRO ARISTIZABAL**, T.P.A. No. 40.119, identificado con cédula de ciudadanía número 16.209.380 de Cartago (Valle), **OSCAR FERNANDO CORREA BARBOSA**, T.P.A. No. 71.027 identificado con cédula de ciudadanía número 79.524.634 de Bogotá, **EDNA DARMELY SARMIENTO CHARRY**, T.P.A. 65.794 identificada con cédula de ciudadanía número 52.006.265 de Bogotá, para solicitar y obtener Patente de Invención para “**APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA ENCRIPCIÓN Y RECUPERACIÓN DE INFORMACIÓN LIBRE DE RUIDO**”.

Los apoderados quedan facultados para interponer recursos, transigir, conciliar, desistir, cancelar, recibir, renunciar, sustituir y revocar las sustituciones, y ratificar los actos de agentes oficiosos.

Señor Director,


Representante Legal
C.C. No. 8.346.555 de Envigado


Oscar Fernando Correa Barbosa



EL SUBDIRECTOR DE INSPECCION Y VIGILANCIA DEL
VICEMINISTERIO DE EDUCACIÓN SUPERIOR EN
CUMPLIMIENTO DE LAS FUNCIONES ATRIBUIDAS POR EL
DECRETO 5012 DE 2009 Y LA RESOLUCIÓN 7245 DE 2011

RL-0003509-2012

CERTIFICA:

Que el(la) UNIVERSIDAD DE ANTIOQUIA (Código:1201), con domicilio en MEDELLIN, es una institución de educación superior, OFICIAL, y su carácter académico es el de Universidad, creada mediante Ley 71 de 4 de Diciembre de 1878, expedido(a) por el(la) la Asamblea Legislativa del Estado Soberano de Antioquia..

Que mediante Resolución 2087 del 5 de septiembre de 2003, expedida por el Ministerio de Educación Nacional, le fue otorgada Acreditación Institucional. Que mediante Decreto 1297 del 30 de mayo de 1964, expedido por el Gobierno Nacional, la Universidad de Antioquia obtuvo reconocimiento como Universidad. De conformidad con los Artículos 46 y 47 del Acuerdo Superior No. 1 de 1994, el Rector es reemplazado por el Vicerrector General en caso de faltas temporales y ejerce, además, las funciones que el Rector, los estatutos y los reglamentos de la Universidad le asignen.

Que la mencionada institución cuenta con seccional(es) en:

- 1219 CARMEN DE VIBORAL
- 1220 ANDES
- 1221 CAUCASIA
- 1222 PUERTO BERRIO
- 1223 TURBO
- 9125 SANTAFE DE ANTIOQUIA

Que al folio 531 distinguido con el registro 525 del libro de rectores y representantes legales de las instituciones de educación superior aparece inscrito(a) el(la) Doctor ALBERTO DE JESUS URIBE CORREA, identificado(a) con cédula de ciudadanía No 8346555 expedida en Envigado como RECTOR , por un periodo comprendido entre el 7 de Abril de 2012 y el 6 de Abril de 2015, que dicha inscripción se efectuó el 19 de Abril de 2012 de conformidad con lo dispuesto en el(la) RESOLUCIÓN 1763, del 13 de Marzo de 2012, expedido(a) por el(la) CONSEJO SUPERIOR.

Que al folio 539 distinguido con el registro 533 del libro de rectores y representantes legales de las instituciones de educación superior aparece inscrito(a) el(la) Doctor MARTINIANO JAIME CONTRERAS, identificado(a) con cédula de ciudadanía No 70064464 expedida en Medellín como RECTOR ENCARGADO , por un periodo comprendido entre el 1 de Septiembre de 2009 y el 31 de Agosto de 2012, que dicha inscripción se efectuó el 24 de Mayo de 2012 de conformidad con lo dispuesto en el(la) RESOLUCIÓN 28617, del 31 de Agosto de 2009, expedido(a) por el(la) RECTORIA.

Que al folio 531 distinguido con el registro 525 del libro de rectores y representantes legales de las instituciones de educación superior aparece inscrito(a) el(la) Doctor ALBERTO DE JESUS URIBE CORREA, identificado(a) con cédula de ciudadanía No 8346555 expedida en Envigado como REPRESENTANTE LEGAL , por un periodo comprendido entre el 7 de Abril de 2012 y el 6 de Abril de 2015, que dicha inscripción se efectuó el 19 de Abril de 2012 de conformidad con lo dispuesto en el(la) RESOLUCIÓN 1763, del 13 de Marzo de 2012, expedido(a) por el(la) CONSEJO SUPERIOR.

Que al folio 539 distinguido con el registro 533 del libro de rectores y representantes legales de las instituciones de educación superior aparece inscrito(a) el(la) Doctor MARTINIANO JAIME CONTRERAS, identificado(a) con cédula de ciudadanía No 70064464 expedida en Medellín como REPRESENTANTE LEGAL ENCARGADO , por un periodo comprendido entre el 1 de Septiembre de 2009 y el 31 de Agosto de 2012, que dicha inscripción se efectuó el 24 de Mayo de 2012 de conformidad con lo dispuesto en el(la) RESOLUCIÓN 28167, del 31 de Agosto de 2009, expedido(a)

39
69

por el(la) RECTORIA.
La información consignada en este certificado corresponde a la última reportada por parte de la institución.
De conformidad con lo establecido por la ley 962 de 2005, los actos de registro aquí certificados quedan en firme cinco (5) días hábiles después de la fecha de inscripción, siempre que no sean objeto del recursos en la vía gubernativa.
El presente documento electrónico tiene validez por cumplir los requisitos de que trata la Ley 527 de 1999, el Decreto Reglamentario 1747 de 2000 y las demás normas que los complementen, modifiquen o reemplacen. Para verificar la autenticidad del presente certificado o ver el documento electrónico, deberá ingresar a www.mineduccion.gov.co, menú de Trámites, opción de Consulta de Certificados e ingresar el número de radicado.
Se expide la presente certificación en Bogotá D.C. a los 11 días del mes de Septiembre de 2012, por solicitud de UNIVERSIDAD DE ANTIOQUIA UNIVERSIDAD DE ANTIOQUIA.

Certificado	JUAN GUILLERMO PLATA PLATA		
Propietario	T=SUBDIRECCION DE INSPECCION Y VIGILANCIA, SN=PLATA PLATA, STREET=CALLE 43 NO. 57 14 CAN, S=BOGOTA D.C., OU=MINISTERIO DE EDUCACION, SERIALNUMBER=204818, OID.1.3.6.1.4.1.23267.2.3=89999990017, OID.1.3.6.1.4.1.23267.2.2=91298420, OID.1.3.6.1.4.1.23267.2.1=52, O=MINISTERIO DE EDUCACION NACIONAL, L=BOGOTA D.C., G=JUAN, E=JPLATA@MINEDUCACION.GOV.CO, C=CO, CN=JUAN GUILLERMO PLATA PLATA		
Fecha Firma	2012-09-11T16:30:56.180	Emisor	CN=AC Subordinada Certicámara S.A., O=Sociedad Cameral de Certificación Digital - Certicámara S.A., C=CO



UNIVERSIDAD DE ANTIOQUIA
1803

EL SECRETARIO GENERAL DE LA UNIVERSIDAD DE ANTIOQUIA,

INFORMA QUE:

La Universidad de Antioquia es una Institución de educación superior creada mediante la Ley 71 de 1878 del extinguido Estado Soberano de Antioquia, y cuya Personería Jurídica deriva de la ley 153 de 1887; aprobada por el Decreto 1297 del 30 de mayo de 1964, código ICFES 1201, Registro de Alta Calidad, Acreditación Institucional del Ministerio de Educación Nacional Resolución 2087 del 5 de septiembre de 2003, NIT 890.980.040.8.

Su autonomía como Universidad Departamental fue reiterada y confirmada por la Ley 30 del 28 de diciembre de 1992.

De conformidad con los artículos 66 de la Ley 30 de 1992, y 40 del Estatuto General de la Universidad, el Rector es el representante legal y su primera autoridad ejecutiva, cargo que en la actualidad desempeña el doctor ALBERTO URIBE CORREA, con cédula 8.346.555 de Envigado, designado mediante la Resolución Superior 1763 del 13 de marzo de 2012.

El Rector como representante legal de la Universidad, está facultado según el Estatuto General de Contratación, artículo 11 del Acuerdo Superior 095 del 21 de octubre de 1996, para suscribir contratos.

El Rector sólo requiere autorización del Consejo Superior Universitario para suscribir contratos cuya cuantía supere el valor de mil quinientos (1.500) salarios mínimos legales mensuales vigentes en el país, siempre y cuando los mismos signifiquen egresos para la Universidad.

Medellín, 24 OCT. 2012

LUQUEGI GIL NEIRA

SECRETARÍA GENERAL

Ciudad Universitaria: Calle 67 N.º 53-108 ■ Recepción de correspondencia: Calle 70 N.º 52-21
Teléfono: 219 50 20 ■ Fax: 219 50 38 ■ Apartado: 1226
Correo electrónico: secretar@quimbaya.udea.edu.co ■ Medellín, Colombia

41

71

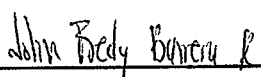
©CAVELIER
ABOGADOS

CESION DE DERECHOS DE PROPIEDAD INDUSTRIAL

Los suscritos, **John Fredy Barrera Ramírez** y **Alejandro Mira Agudelo**, mayores de edad, identificados como aparece al pie de sus firmas, domiciliados en la Calle 67 No. 53 - 108, Medellín, Colombia, declaramos bajo juramento ser inventores de la invención: **"APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA ENCRIPCIÓN Y RECUPERACIÓN DE INFORMACIÓN LIBRE DE RUIDO"**, y declaramos así mismo que cedemos y transferimos, sin limitación, a favor de la **UNIVERSIDAD DE ANTIOQUIA**, constituida y existente de conformidad con las leyes de la República de Colombia y domiciliada en Medellín, Antioquia, Colombia, todos los derechos inherentes a dicha invención y que la citada Universidad queda facultada para solicitar en su nombre la patente de invención correspondiente en la República de Colombia.

El presente documento se suscribe para ser presentado por la **Universidad de Antioquia**, en el trámite de la solicitud de patente ante la Superintendencia de Industria y Comercio.

Dado y firmado hoy 22 de abril de 2014 en Medellín, Antioquia.



JOHN FREDY BARRERA RAMÍREZ
C.C. N° 71'769.124 de Medellín

Dado y firmado hoy 22 de abril de 2014 en Medellín, Antioquia.



ALEJANDRO MIRA AGUDELO
C.C. N° 71'337.736 de Medellín

42
72

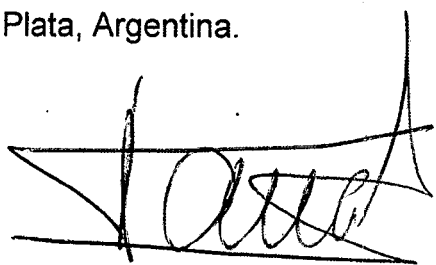
©CAVELIER
ABOGADOS

CESION DE DERECHOS DE PROPIEDAD INDUSTRIAL

El suscrito, **Roberto Daniel Torroba**, mayor de edad, identificado como aparece al pie de su firma, domiciliado en Calle 5 Nro. 1241, La Plata, Argentina, declaro bajo juramento ser inventor de la invención: **"APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA ENCRIPCIÓN Y RECUPERACIÓN DE INFORMACIÓN LIBRE DE RUIDO"**, y declaro así mismo que cedo y transfiero, sin limitación, a favor de la **UNIVERSIDAD DE ANTIOQUIA**, constituida y existente de conformidad con las leyes de la República de Colombia y domiciliada en Medellín, Antioquia, Colombia, todos los derechos inherentes a dicha invención y que la citada Universidad queda facultada para solicitar en su nombre la patente de invención correspondiente en la República de Colombia.

El presente documento se suscribe para ser presentado por la **Universidad de Antioquia**, en el trámite de la solicitud de patente ante la Superintendencia de Industria y Comercio.

Dado y firmado hoy 22 de Abril de 2014 en La Plata, Argentina.



ROBERTO DANIEL TORROBA
D.N.I. N° 11.231.720 de Argentina.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

-/-

43

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 0047785

Bogotá D.C., Mayo 07 de 2014 - 11:41:10

RECIBIDO DE : CAVELIER ABOGADOS

NI 860.041.367

RE

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
RECIBO DE CA	999999999	41374	16/04/2014		1.000.00
RECIBO DE CA	999999999	45521	29/04/2014		52.000.00
RECIBO DE CA	999999999	45522	29/04/2014		52.000.00
RECIBO DE CA	999999999	45534	29/04/2014		128.000.00
RECIBO DE CA	999999999	45570	29/04/2014		1.000.00
RECIBO DE CA	999999999	45583	29/04/2014		5.000.00
RECIBO DE CA	999999999	47535	06/05/2014		21.000.00
RECIBO DE CA	999999999	47553	06/05/2014		128.000.00
RECIBO DE CA	999999999	47557	06/05/2014		278.000.00

*** Conceptos Pagados ***

CANT. RENTISTICO

1 50005-01-01 SOLICITUDES

CONCEPTO

2249 DTO 25% PCT SOLICITUD DE PATENTE
DE INVENCIÓN

Vr.UNDITARIO Vr.CONCEPTO

386.250.00

386.250.00

\$386.250.00

=====

SON: **TRESCIENTOS OCHENTA Y SEIS MIL DOSCIENTOS CINCUENTA PESOS MONEDA CORRIENTE***

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-098035- 00000-0000

Fecha: 2014-05-07 16:34:54 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 26-46

0000005895-802-002-5

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia

Web: www.sic.gov.co e-mail: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

Mayo 7 de 2014 - 11:41:11

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

-/-

44

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 0047781

Bogotá D.C., Mayo 07 de 2014 - 11:36:49

RECIBIDO DE : CAVELIER ABOGADOS

NI 860.041.367

RE

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
RECIBO DE CA	999999999	41375	16/04/2014		1.000.00
RECIBO DE CA	999999999	44688	29/04/2014		13.000.00
RECIBO DE CA	999999999	45524	29/04/2014		106.000.00
RECIBO DE CA	999999999	45533	29/04/2014		128.000.00
RECIBO DE CA	999999999	45567	29/04/2014		62.000.00
RECIBO DE CA	999999999	45569	29/04/2014		1.000.00
RECIBO DE CA	999999999	47561	06/05/2014		464.000.00
RECIBO DE CA	999999999	47575	06/05/2014		93.000.00

*** Conceptos Pagados ***

CANT. RENTISTICO

CONCEPTO

Vr.UNDITARIO

Vr.CONCEPTO

18 50005-01-01 SOLICITUDES

1607 REIVINDICACION PATENTE UNITARIA
ADICIONAL A LAS 10 INIC

31.000.00

558.000.00

\$558.000.00

SON: **QUINIENTOS CINCUENTA Y OCHO MIL PESOS MONEDA CORRIENTE***

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-098035- -00000-0000

Fecha: 2014-05-07 16:34:54

Dep. 2020 DIR.NUEVASCR

Tra. 2 PATENTES

Eve: 1 REGDEPOSITO

Act. 411 PRESENTACION

Folios: 70-46

C.C.O. 05895-802-0025

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia

Web: www.sic.gov.co e-mail: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

Mayo 7 de 2014 - 11:36:50

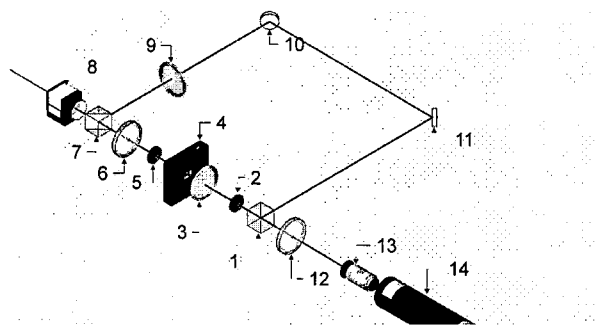
45-78

 Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISION DE NUEVAS CREACIONES EXTRACTO PARA PUBLICACIÓN SOLICITUD DE PATENTE DE INVENCION	
(21) N° de solicitud: (22) Fecha de solicitud: (30) Prioridad (31) <i>No. Prioridad</i> (32) <i>Fecha</i> (33) <i>País</i>		(51) Int Cl: (71) Solicitante(s) UNIVERSIDAD DE ANTIOQUIA (72) Inventor(es) JOHN FREDY BARRERA RAMIREZ Y OTROS (74) Apoderado: LUZ CLEMENCIA DE PAEZ	
(54) Titulo: APARATO ÓPTICO-FÍSICO Y PROCEDIMIENTOS PARA LA ENCRIPCIÓN Y RECUPERACIÓN DE INFORMACIÓN LIBRE DE RUIDO			

Resumen:

La presente invención proporciona un sistema físico de encriptación en el cual un haz de luz pasa por un código gráfico (CG) y otro haz de luz pasa por una máscara aleatoria física (llave de seguridad), ambos haces se juntan para ocultar de manera segura el CG. En este caso, la llave de seguridad es un elemento físico semi-transparente que introduce cambios aleatorios de fase permitiendo la encriptación y posterior recuperación de un CG. El CG encriptado con el montaje óptico-físico, se almacena digitalmente usando una cámara digital. La misma cámara también se usa para almacenar la información de la llave de seguridad usada para encriptar el CG. El CG encriptado puede ser descryptado nuevamente usando un sistema óptico virtual que simula los procesos de propagación de la luz a través de un montaje físico de descryptación, donde la llave de seguridad es una máscara aleatoria de fase.

Fig. 3ª





No. 14-098035- -00000-0000

Fecha: 2014-05-07 16:34:54 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 76 46

S

10

PATENTE DE INVENCION ☐

MODEL

☐	Indicación que se solicita una patente.
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Descripción de la invención
☐	Dibujos de ser estos pertinentes
☐	Comprobante de pago de las tasas establecidas (De ser el caso formato de descuento)
Completa ☐	Incompleta ☐

PATENTE DE INVENCION PCT ☐ MODELO DE UTILIDAD PCT ☐ Art.33 Decisión 486/00, Circular Única

☐	Indicación que se solicita una PCT
☐	Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)
☐	Dibujos de ser estos pertinentes
☐	Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)
Completa ☐	Incompleta ☐

DISEÑO INDUSTRIAL ☐

(Art. 119 Decisión 486/00)

☐	Indicación que se solicita Diseño industrial
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Representación gráfica y fotográfica del Diseño industrial o muestra del material que incorpora el diseño
☐	Comprobante de pago de las tasas establecidas
Completa ☐	Incompleta ☐

ESQUEMA DE TRAZADO ☐

(Art. 92 Decisión 486/00)

☐	Indicación que se solicita un esquema de trazado
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Representación gráfica de un esquema de trazado
☐	Comprobante de pago de las tasas establecidas
Completa ☐	Incompleta ☐