

DISPOSITIVO, MÉTODO Y SISTEMA ÓPTICO DE ENCRIPCIÓN DE INFORMACIÓN

DISPOSITIVO, MÉTODO Y SISTEMA ÓPTICO DE ENCRIPCIÓN DE INFORMACIÓN

Campo de la Invención

La presente invención se relaciona con los dispositivos y procesos de encriptación y desencriptación de información usando fenómenos ópticos.

Antecedentes de la invención

En la actualidad, la protección de la información privada es una necesidad prioritaria tanto para individuos como para organizaciones e instituciones. Los métodos tradicionales de encriptación digital, aunque ampliamente utilizados, han demostrado ser vulnerables ante ataques cada vez más sofisticados. En respuesta a estas limitaciones, se han desarrollado sistemas ópticos de encriptación como una alternativa viable para resguardar información sensible. Estos sistemas ofrecen ventajas significativas frente a los digitales al aprovechar múltiples parámetros físicos (grados de libertad) para codificar la información, lo que incrementa notablemente su nivel de seguridad.

Los sistemas de encriptación transforman la información original en un formato cifrado, llamado información encriptada, que es ininteligible hasta que se usa una llave de seguridad específica. Esta llave permite tanto el proceso de encriptación como el de desencriptación, asegurando que solo quienes posean la llave puedan acceder a los datos originales. Entre las técnicas más avanzadas de encriptación óptica se destaca el uso de dos máscaras aleatorias de fase. Sin embargo, esta tecnología presenta desafíos prácticos que limitan su implementación fuera del entorno controlado de un laboratorio.

Por otro lado, los sistemas ópticos tradicionales dependen de montajes complejos que requieren numerosos elementos como espejos, divisores de haz y polarizadores, además de condiciones de alta estabilidad y precisión en la alineación. Los primeros prototipos empleaban materiales de registro físico, como cristales fotorrefractivos o películas

holográficas, que dificultaban la transferencia de la información encriptada al usuario final. Esto hacía que estos sistemas fueran poco prácticos para aplicaciones fuera del laboratorio.

Para solucionar algunas de estas limitaciones, surgieron los sistemas óptico-digitales, que combinan componentes ópticos con medios de registro digitales (como cámaras). Estos medios permiten digitalizar las salidas de los sistemas de encriptación y enviar la información a través de canales como Internet. Sin embargo, estos avances aún presentan retos, particularmente en cuanto a la complejidad del proceso de desencriptación. En estos sistemas, la información relacionada con la llave de seguridad —que contiene datos complejos de fase y amplitud— suele ser registrada mediante montajes interferométricos que requieren un brazo de referencia. Esta configuración es sensible a perturbaciones, lo que limita su viabilidad fuera del entorno experimental.

Otra de las principales dificultades que enfrentan los sistemas ópticos de encriptación es el ruido aleatorio en los datos recuperados. Este problema surge debido al uso de elementos difusores y fuentes de iluminación coherente como láseres, que introducen ruido a la información recuperada tras el proceso de encriptación-desencriptación. Los usuarios esperan que los sistemas de encriptación no solo protejan sus datos, sino que también garanticen su recuperación precisa. Además, algunos sistemas óptico-digitales requieren al menos dos registros (uno para la información encriptada y otro para la llave de seguridad). Este proceso puede generar errores debido a variaciones en el montaje entre cada registro, lo que incrementa el ruido. Para mitigar estos problemas, se han propuesto diversas estrategias, como el uso de códigos gráficos (códigos QR y de barras) para garantizar la recuperación de información libre de ruido, pero aún quedan desafíos por resolver.

Dada la creciente demanda de sistemas seguros y eficientes para la protección de la información, resulta fundamental desarrollar una tecnología de encriptación óptica que supere algunas de las limitaciones actuales.

Descripción breve de la invención

La presente invención busca solucionar los problemas ya mencionados de la encriptación óptica de datos, simplificando el sistema, con la eliminación del brazo de referencia requerido en montajes interferométricos, lo cual reduce los requerimientos de estabilidad y alineación, minimizando el número de elementos ópticos necesarios. Asimismo, tiene como objetivo disminuir la degradación del dato recuperado causado por el proceso de encriptación- desencriptación mediante técnicas avanzadas de reducción de ruido. Esta nueva solución pretende no solo facilitar la implementación de sistemas ópticos de encriptación a gran escala, sino también asegurar que los datos protegidos puedan ser

recuperados con fidelidad por el usuario final, manteniendo la integridad de la información en todo momento.

De esta forma, la presente divulgación busca proporcionar un dispositivo, un método y un sistema óptico capaz de encriptar y desencriptar información de manera confiable y eficiente.

El dispositivo óptico de encriptación de información aquí divulgado proyecta la información a encriptar en forma de imagen y la encripta a partir de la propagación de la luz y el uso de una máscara aleatoria de fase, que es usada como llave de seguridad. Este dispositivo comprende un único brazo de iluminación que incluye una fuente de iluminación que produce un haz de luz coherente; un expansor de haz, que aumenta el área de iluminación del haz de luz producido por la fuente de iluminación, un elemento difusor, que introduce una fase aleatoria al haz proveniente del expansor; un elemento de proyección, en donde se ubican simultáneamente la información a encriptar, la ventana de la llave de seguridad y la ventana auxiliar, las cuales son iluminadas por medio del haz proveniente del elemento difusor; y un elemento de adquisición de luz que registra la intensidad de la luz proveniente del elemento de proyección, donde este registro contiene la información encriptada y la llave de seguridad.

El método óptico de encriptación-desencriptación de información aquí revelado es realizado gracias al dispositivo óptico de encriptación y se caracteriza porque comprende las etapas de: ubicar simultáneamente la información a encriptar, una ventana de la llave de seguridad y una ventana auxiliar en un elemento de proyección; iniciar un haz de luz coherente, usando una fuente de iluminación; aumentar el área de iluminación del haz de luz proveniente de la fuente de iluminación por medio de un expansor de haz; introducir una fase aleatoria al haz de luz proveniente del expansor de haz, por medio de un elemento difusor; iluminar en el elemento de proyección la información a encriptar, la ventana de llave de seguridad y la ventana auxiliar, por medio del haz con la fase aleatoria proveniente del difusor; registrar la intensidad de la luz propagada proveniente del elemento de proyección, por medio de un elemento de adquisición de luz; almacenar la información registrada, por medio de un computador; recuperar la información original, por medio de la información encriptada, la llave de seguridad y un sistema óptico virtual de desencriptación.

Otro objeto de la presente divulgación es un sistema óptico de encriptación - desencriptación de información que comprende: un dispositivo óptico de encriptación de información de acuerdo con una realización de la invención, y un dispositivo de computación conectados entre sí, en donde el dispositivo de computación controla el elemento que

proyecta la información a encriptar, la ventana de la llave de seguridad y la ventana auxiliar, además procesa y almacena la información encriptada y la llave de seguridad a partir de la información que registra el sistema de adquisición de luz, y recupera la información original, usando un sistema óptico virtual de desencriptación.

La información encriptada y la llave de seguridad son enviadas a un usuario autorizado, el cual usa un sistema óptico virtual que reproduce los procesos del montaje físico para el proceso de desencriptación. Debido a los procesos físicos involucrados durante la encriptación y la desencriptación, el objeto recuperado contiene ruido. A pesar de lo anterior, el contenido de la información recuperada se puede identificar.

Además, con el objetivo de obtener una lectura de la información libre de ruido, se incluyen modalidades para la encriptación y recuperación de la información usando un código gráfico como contenedor de la información. En estas, la información a encriptar se codifica en un código diseñado para el procesamiento óptico (CDPO), el cual se somete al proceso de encriptación y desencriptación, recuperándose un CDPO con ruido. De ese modo, al aplicar un proceso de filtrado y lectura a este CDPO, se recupera la información contenida en él completamente libre de ruido.

De manera ventajosa, el dispositivo, método y sistema de encriptación aquí descritos permiten que no se requiera el uso de un montaje óptico interferométrico con brazo de referencia para el registro de la llave de seguridad, lo cual reduce el tamaño, el número de elementos y los requerimientos de estabilidad y alineación. Sumado a esto, con un solo registro se obtiene tanto la información encriptada como la llave de seguridad, lo que agiliza la captura de la información y evita el ruido que puede aparecer al realizar múltiples registros. Adicionalmente, la presente divulgación emplea los códigos diseñados para el procesamiento óptico (CDPO) en lugar de códigos QR para una desencriptación libre de ruido. Esto permite encriptar y desencriptar más información, ya que, a diferencia de los códigos QR, los CDPO tienen una estructura más simple que facilita el procesamiento y la recuperación satisfactoria de una mayor cantidad de datos.

Descripción de las figuras

La Figura 1 muestra un diagrama esquemático con los elementos que conforman el dispositivo óptico de encriptación de información aquí revelado.

La Figura 2 muestra una fotografía de una realización del dispositivo óptico de encriptación de información de acuerdo con la presente invención.

La Figura 3 muestra un diagrama de bloques ilustrando los procesos de encriptación y desencriptación del método según una realización de la presente invención.

La Figura 4 muestra un ejemplo de una imagen proyectada en el dispositivo óptico aquí revelado con la información a encriptar, la ventana llave seguridad, la ventana auxiliar y las coordenadas de posicionamiento de cada ventana.

La Figura 5 muestra un ejemplo de una imagen con información a encriptar.

La Figura 6 muestra un ejemplo de una imagen del proceso de filtrado de la distribución conjunta de potencias (DCP) con base en la imagen de la Figura 5 al ser procesada por el dispositivo, método y sistema aquí revelados.

La Figura 7 muestra una imagen de la información de la imagen de la Figura 5 encriptada mediante el dispositivo, método y sistemas de la presente invención.

La Figura 8 muestra un diagrama que ejemplifica el montaje óptico físico o el proceso simulado por el sistema óptico virtual para llevar a cabo la desencriptación de acuerdo con la presente invención.

La Figura 9 muestra un ejemplo de la información de la Figura 5 recuperada mediante el sistema de la presente invención.

La Figura 10 muestra el código diseñado para el procesamiento óptico (CDPO) para la letra “o” según la presente invención.

La Figura 11 muestra el CDPO del mensaje “Hola” de acuerdo con las realizaciones de la invención.

La Figura 12 muestra el diagrama del proceso que sigue un CDPO para encriptar y desencriptar un mensaje libre de ruido en el sistema aquí revelado.

Descripción detallada de la invención

La presente invención proporciona un dispositivo, un método y un sistema óptico capaz de encriptar y desencriptar información de manera confiable y eficiente.

Dispositivo óptico de encriptación

En una realización de las modalidades preferidas de la presente invención se revela aquí un dispositivo óptico de encriptación de información (1) caracterizado porque comprende un único brazo de iluminación (100). Dicho Brazo de iluminación (100) incluye una fuente de iluminación (101) que produce un haz de luz coherente; un expansor de haz (102), ubicado

después de la fuente de iluminación (101), que aumenta el área de iluminación del haz de luz producido por la fuente de iluminación (101); un elemento difusor (103), ubicado después del expansor de haz (102), que introduce una fase aleatoria al haz proveniente del expansor (102); un elemento de proyección (104), en donde se ubican simultáneamente la información a encriptar (200), la ventana de la llave de seguridad (201) y la ventana auxiliar (202), las cuales son iluminadas por medio del haz proveniente del elemento difusor (103) del único brazo de iluminación (100); y un elemento de adquisición de luz (105) que registra la intensidad de la luz proveniente del elemento de proyección (104), donde este registro contiene la información encriptada y la llave de seguridad.

Tal como se muestra en las Figuras 1 y 2 en una realización de la invención el dispositivo óptico de encriptación posee un brazo único de iluminación (100), una fuente de iluminación láser (101), el expansor de haz (102), el elemento difusor (103), el elemento de proyección (104) y el elemento de adquisición de luz (105). En algunas realizaciones, el dispositivo óptico (1) incluye un filtro neutro (106) entre el elemento difusor (103) y el elemento de proyección (104). La Figura 2 evidencia que en una realización preferida el dispositivo óptico aquí revelado es compacto lo que lo hace más conveniente para su utilización en distintos tipos de aplicaciones.

De acuerdo con realizaciones de la invención la fuente de iluminación (101) es un láser que genera luz coherente; también podría usarse una fuente de iluminación parcialmente coherente, tal como un led.

De manera preferida, el elemento difusor (103) que introduce cambios de fase aleatorios puede ser de vidrio, de plástico o de resina. Otras modalidades pueden usar un elemento semitransparente, como un polímero, con espesores determinados que pueden dar origen a cambios de fase no aleatorios que pueden ser caóticos, fractales, entre otros. Así mismo, dicho elemento difusor puede sustituirse por elementos como máscaras estructuradas o elementos ópticos difractivos.

En una de las modalidades preferidas, el elemento de proyección (104) es un dispositivo digital de microespejos (DDM), y el elemento de adquisición de luz (105) se selecciona de un grupo que comprende una cámara CCD o una cámara CMOS. En otro tipo de realizaciones, dicho elemento de adquisición de luz (105) puede ser una película fotográfica, película holográfica o cristal fotorrefractivo.

De acuerdo con algunas realizaciones de la invención el elemento de adquisición de luz (105) y el elemento de proyección (104) se encuentran separados entre sí, y no existe ningún componente adicional entre ellos.

En realizaciones de la invención, durante el funcionamiento del dispositivo óptico de encriptación (1) la fuente de iluminación láser (101) produce un haz de luz coherente, el cual pasa por el expansor de haz (102) para aumentar el área de iluminación. Este haz de luz expandido pasa por el elemento difusor (103) seguido en algunas modalidades por un filtro neutro (106); el elemento difusor (103) es el encargado de introducir una fase aleatoria al haz de luz y el filtro neutro (106) controla su intensidad. Posteriormente, este haz de luz interactúa con el elemento de proyección (104), en donde se ubica la información a encriptar (200), la ventana llave de seguridad (201) y la ventana auxiliar (202). Como el haz de luz tiene una fase aleatoria, este introduce máscaras aleatorias de fase a la información que se va a encriptar y a la ventana auxiliar, y genera la llave de seguridad por medio de la ventana de la llave de seguridad (201). Finalmente, la luz reflejada por el elemento de proyección (104) se propaga libremente por el espacio hasta alcanzar el elemento de adquisición de luz (105) (preferiblemente una cámara); la cual registra una imagen con la intensidad de la luz propagada, también denominada distribución conjunta de potencias (DCP) (203).

En otras modalidades, el elemento de proyección (104) puede ser un modulador espacial de luz de cristal líquido, sea de amplitud o fase, moduladores ferroeléctricos de fase, filminas prediseñadas o un sistema de proyección de imágenes dinámico ya sea por reflexión o transmisión, moduladas en amplitud.

En otras modalidades del dispositivo, un sistema de dos lentes o un filtro espacial de luz (pinhole y objetivo de microscopio) en conjunto con una lente colimadora, puede reemplazar el expansor de haz (102).

De la misma forma, la función del filtro neutro (106) puede ser desempeñada por uno o dos polarizadores según el estado de polarización de la fuente de iluminación (101).

Método óptico de encriptación-desencriptación de información

En otra modalidad preferida de la presente invención se revela aquí un método óptico de encriptación-desencriptación de información caracterizado porque comprende las etapas de: ubicar simultáneamente la información a encriptar (200), la ventana de la llave de seguridad (201) y la ventana auxiliar (202) en un elemento de proyección (104); emitir con un haz de luz coherente, usando una fuente de iluminación (101); aumentar el área de iluminación del haz de luz proveniente de la fuente de iluminación (101), por medio de un expansor de haz (102); introducir una fase aleatoria al haz de luz proveniente del expansor de haz (102), por medio de un elemento difusor (103); iluminar en el elemento de proyección (104) la información a encriptar (200), la ventana de llave de seguridad (201) y

la ventana auxiliar (202), por medio del haz con la fase aleatoria proveniente del difusor (103); registrar la intensidad de la luz propagada proveniente del elemento de proyección (104), por medio de un elemento de adquisición de luz (105); almacenar la información registrada, por medio de un computador (110); recuperar la información original, por medio de la información encriptada, la llave de seguridad y un sistema óptico virtual de descryptación (120).

La Figura 3 ilustra los procedimientos de encriptación, almacenamiento y descryptación de acuerdo con una realización de método óptico de encriptación-descryptación de acuerdo con la invención. Como se muestra en dicha Figura 3, en el proceso de encriptación, la información a encriptar (200) se proyecta en el dispositivo (1). El dispositivo (1) lleva a cabo el proceso óptico de encriptación y la imagen de salida de este se registra y almacena digitalmente. A esta imagen se le conoce como distribución conjunta de potencias (DCP) (203).

Usando procesos de filtrado individuales para la información encriptada y para la llave de seguridad, junto con la aplicación de transformadas de Fourier (TF), se extraen la información encriptada (300), y la llave de seguridad (301) de la distribución conjunta de potencias DCP (203a y 203b).

El proceso de descryptación se puede hacer a través de un sistema óptico virtual (120) o con un montaje físico, utilizando la información encriptada (300) y la llave de seguridad (301). El resultado es una imagen cuya intensidad es la información recuperada (400), la cual presenta ruido inherente a los procesos físicos involucrados.

En una realización preferida, el proceso de encriptación aquí revelado es realizado de la siguiente manera:

En el elemento de proyección (104) (preferiblemente un DDM) del dispositivo (1), una imagen, como la mostrada en la Figura 4, es proyectada como entrada al sistema. Dicha imagen comprende tres elementos: la información a encriptar (200), la ventana llave de seguridad (201) y la ventana auxiliar (202). En particular, la información a encriptar (200) consiste en una imagen binaria, como por ejemplo los caracteres "JTC" mostrados en la Figura 5. La ventana auxiliar (202) se usa para registrar la información de la llave de seguridad.

Matemáticamente, el proceso de encriptación por propagación en espacio libre se puede describir usando el formalismo de transformada fraccional de Fourier (TFRF). El orden fraccional α se puede estimar con la siguiente expresión:

$$\tan \alpha = A^2 \lambda d \quad (\text{Ecuación I})$$

Donde λ es la longitud de onda de la luz emitida por la fuente de iluminación (101), d la distancia de propagación entre el elemento de proyección (104) y el elemento de registro (105), y A una constante para cancelar las dimensiones de λd , si las longitudes se miden en mm , $A = 1 \text{ mm}^{-1}$.

Como se indicó previamente, en una realización de la invención la información a encriptar (200), definida matemáticamente como $(o(x, y))$, y ventanas llave de seguridad (201) y auxiliar (202) se proyectan en una sola imagen (Figura 4) a través del elemento de proyección (104) del dispositivo (1). Definiendo como origen del sistema de referencia el centro de la imagen de entrada con eje horizontal positivo hacia la derecha y eje vertical positivo hacia abajo (Figura 4), se obtiene que el centro de la información a encriptar (200) corresponde a la posición $(-a, -b)$, el centro de la ventana llave de seguridad (201) está en $(a, -b)$, y la ventana llave auxiliar (202) tiene como centro $(-a, c)$.

En esta realización, la imagen proyectada en el elemento de proyección (104) se ilumina con luz colimada que previamente ha pasado a través del elemento difusor (103), la cual se asume como constante en amplitud y con una fase distribuida aleatoriamente en el rango $(0, 2\pi)$. De este modo, la información a ser encriptada $o(x, y)$ estará multiplicada por una máscara aleatoria de fase $(f(x, y) = o(x, y)r(x, y))$, la llave de seguridad será también una máscara aleatoria de fase $(k(x, y))$ y la ventana auxiliar también tendrá una distribución aleatoria de fase $(k_{aux}(x, y))$. El campo de entrada al proceso óptico de encriptación se puede expresar en términos de los operadores de traslación fraccionales $(\tau_{x_d, y_d; \alpha})$, con x_d y y_d los desplazamientos en las direcciones horizontal y vertical, respectivamente) como:

$$e(x, y) = \tau_{-a, -b; \alpha} \{f(x, y)\} + \tau_{a, -b; \alpha} \{k(x, y)\} + \tau_{-a, c; \alpha} \{k_{aux}(x, y)\} \quad (\text{Ecuación II})$$

El campo presente en la Ecuación II se propaga por el espacio libre una distancia d hasta el elemento de adquisición de luz (105), donde se realiza el registro de la intensidad del campo resultante. Esta información viene dada por:

$$E(u, v) = F_\alpha(u, v) \exp[2\pi i(au + vb) \csc \alpha] + K_\alpha(u, v) \exp[-2\pi i(au - vb) \csc \alpha] + K_{aux, \alpha}(u, v) \exp[2\pi i(au - vc) \csc \alpha] \quad (\text{Ecuación III})$$

donde $F_\alpha(u, v)$, $K_\alpha(u, v)$ y $K_{aux, \alpha}(u, v)$ son las transformadas fraccionales de Fourier (TFRF) de $f(x, y)$, $k(x, y)$ y $k_{aux}(x, y)$, respectivamente, asociadas con la propagación libre. El elemento de adquisición de luz registra la intensidad asociada a este campo o la distribución conjunta de potencias (DCP) (203) definida matemáticamente por:

$$\begin{aligned}
I_{DCP}(u, v) &= E(u, v)E^*(u, v) \\
&= |F_\alpha(u, v)|^2 + |K_\alpha(u, v)|^2 + |K_{aux, \alpha}(u, v)|^2 \\
&\quad + F_\alpha(u, v)K_\alpha^*(u, v) \exp[4\pi i a u \csc \alpha] \\
&\quad + F_\alpha^*(u, v)K_\alpha(u, v) \exp[-4\pi i a u \csc \alpha] \\
&\quad + F_\alpha(u, v)K_{aux, \alpha}^*(u, v) \exp[2\pi i (b + c)v \csc \alpha] \\
&\quad + F_\alpha^*(u, v)K_{aux, \alpha}(u, v) \exp[-2\pi i (b + c)v \csc \alpha] \\
&\quad + K_\alpha(u, v)K_{aux, \alpha}^*(u, v) \exp[-2\pi i (2au - (b + c)v \csc \alpha)] \\
&\quad + K_\alpha^*(u, v)K_{aux, \alpha}(u, v) \exp[2\pi i (2au - (b + c)v \csc \alpha)]
\end{aligned}$$

(Ecuación IV)

En total se tienen nueve términos, entre los cuales hay términos relacionados con la información a encriptar (200) y con la llave de seguridad (201). Esto hace necesario un proceso de filtrado para extraer la información encriptada definida por $(F_\alpha(u, v)K_\alpha^*(u, v))$, correspondiente al cuarto término de la Ecuación IV, y para extraer la llave de seguridad definida por $(K_\alpha(u, v)K_{aux, \alpha}^*(u, v))$, asociada al octavo término de la Ecuación IV.

Una vez extraídas la información encriptada y la llave de seguridad, se envían a un destinatario final. Este proceso de filtrado se inicia con la aplicación de una TF a $I_{DCP}(u, v)$ Ecuación IV obteniéndose:

$$\begin{aligned}
\mathbf{TF}\{I_{DCP}(u, v)\} &= f_\alpha(x, y) \otimes f_\alpha^*(x, y) \\
&\quad + k_\alpha(x, y) \otimes k_\alpha^*(x, y) \\
&\quad + k_{aux, \alpha}(x, y) \otimes k_{aux, \alpha}^*(x, y) \\
&\quad + f_\alpha(x, y) \otimes k_\alpha^*(x, y) \otimes \delta(x + 2a \csc \alpha, y) \\
&\quad + f_\alpha^*(x, y) \otimes k_\alpha(x, y) \otimes \delta(x - 2a \csc \alpha, y) \\
&\quad + f_\alpha(x, y) \otimes k_{aux, \alpha}^*(x, y) \otimes \delta[x, y + (b + c) \csc \alpha] \\
&\quad + f_\alpha^*(x, y) \otimes k_{aux, \alpha}(x, y) \otimes \delta[x, y - (b + c) \csc \alpha] \\
&\quad + k_\alpha(x, y) \otimes k_{aux, \alpha}^*(x, y) \otimes \delta[x + 2a \csc \alpha, y - (b + c) \csc \alpha] \\
&\quad + k_\alpha^*(x, y) \otimes k_{aux, \alpha}(x, y) \otimes \delta[x - 2a \csc \alpha, y + (b + c) \csc \alpha]
\end{aligned}$$

(Ecuación V)

donde $\otimes$ simboliza la operación de convolución, $f_\alpha(x, y) = \mathbf{TF}\{F_\alpha(u, v)\}$, $k_\alpha(x, y) = \mathbf{TF}\{K_\alpha(u, v)\}$ y $k_{aux, \alpha}(x, y) = \mathbf{TF}\{K_{aux, \alpha}(u, v)\}$; y $\delta(x, y)$ es la función delta de Dirac. Nótese que el argumento de la función delta de Dirac, contiene la información de la posición del término respectivo en el plano de la transformada, como se ilustra en la Figura 6. Además, la Ecuación V contiene información compleja (parte real e imaginaria); por tanto, en la Figura 6 se muestra el módulo cuadrado de dicha Ecuación V.

En la Figura 6, la región (10) de la imagen contiene información superpuesta de la información a encriptar, la llave de seguridad y la ventana auxiliar, la cual está ubicada en el centro del plano de la transformada. La región (11) está relacionada con la información a encriptar y la llave de seguridad (asociada a la información encriptada (300)), y está ubicada

en la posición $(-2a \csc \alpha, 0)$, mientras que la región (12) es su complejo conjugado y se ubica en la posición $(2a \csc \alpha, 0)$. La región (13) está relacionada con la información a encriptar y la ventana auxiliar, y se ubica en la posición $(0, -(b+c)\csc \alpha)$, mientras que su complejo conjugado corresponde a la región (14) y se posiciona en $(0, (b+c)\csc \alpha)$. Finalmente, la región (15) está relacionada con las llaves de seguridad y auxiliar (asociada con la llave de seguridad (301)), y se ubica en la posición $(2a \csc \alpha, -(b+c)\csc \alpha)$, mientras que su complejo conjugado corresponde a la región (16) y está ubicado en la posición $(-2a \csc \alpha, (b+c)\csc \alpha)$.

Durante el proceso de filtrado, se extrae la región (11) de la figura 6 correspondiente al cuarto término de la Ecuación V, el cual se ubica en el centro de una nueva matriz $(oe(x, y) = f_\alpha(x, y) \otimes k_\alpha^*(x, y))$, y se realiza una TF inversa para obtener la información encriptada (41):

$$OE(u, v) = F_\alpha(u, v)K_\alpha^*(u, v) \quad (\text{Ecuación VI})$$

En la Figura 7 se muestra la amplitud de la información encriptada de acuerdo con esta realización del método de la presente invención, evidenciando que la dicha información encriptada corresponde a una distribución aleatoria (ruido), y no guarda ninguna relación con la información original mostrada en la Figura 5; lo que demuestra la encriptación efectiva de la información original.

De manera similar al proceso de filtrado para obtener la información encriptada, se extrae la región (15) de la figura 6 correspondiente al octavo término de la Ecuación V, el cual se ubica en el centro de una nueva matriz $(k_f(x, y) = k_\alpha(x, y) \otimes k_{aux, \alpha}^*(x, y))$ y se le aplica una TF inversa para obtener la llave de seguridad (42):

$$K_f(u, v) = K_\alpha(u, v)K_{aux, \alpha}^*(u, v) \quad (\text{Ecuación VII})$$

Según una realización del método de la invención, para llevar a cabo el proceso de descryptación, un usuario autorizado debe tener la información encriptada (41) (Ecuación VI) y la llave de seguridad (42) (Ecuación VII). Este proceso se hace a través de un montaje óptico físico inverso en el orden fraccional al usado durante el proceso de encriptación, como el mostrado en la Figura 8, o también puede ser implementado numéricamente por medio de un sistema óptico virtual (120) que funciona en una computadora (110).

En el montaje de la Figura 8, una onda plana (40) ilumina a la información encriptada (41) en contacto con la llave de seguridad (42). El campo resultante se propaga por el espacio libre una distancia d_1 (45) hasta una lente de longitud focal f (43), para luego propagarse en el espacio libre una distancia d_2 (46) hasta el plano de salida; donde la intensidad

resultante corresponde a la de la información descriptada (400). Las distancias de propagación en el espacio libre d_1 y d_2 y la longitud focal de la lente f , deben satisfacer la relación matemática:

$$d_1 + \frac{d_2 f}{f - d_2} = -d \quad (\text{Ecuación VIII})$$

donde d es la distancia de propagación en el espacio libre entre el elemento de proyección (104) y el elemento de adquisición de luz (105). De este modo el montaje óptico mostrado en la Figura 8 realiza la TFrF de orden $-\alpha$.

Matemáticamente, este proceso se lleva a cabo, primero multiplicando la información encriptada (41) por la llave de seguridad (42):

$$\begin{aligned} ODE(u, v) &= OE(u, v) K_f(u, v) \\ &= F_\alpha(u, v) K_\alpha^*(u, v) K_\alpha(u, v) K_{aux, \alpha}^*(u, v) \end{aligned} \quad (\text{Ecuación IX})$$

Posteriormente, a este producto se le aplica una transformada inversa (TFrF de orden $-\alpha$, lo que equivale a una propagación inversa $-d$), obteniéndose:

$$ode(x, y) = f(x, y) \otimes_\alpha k_\alpha^*(u, v) \otimes_\alpha k_\alpha(u, v) \otimes_\alpha k_{aux}^*(x, y) \quad (\text{Ecuación X})$$

donde $\otimes_\alpha$ es la convolución definida en términos de la TFrF de orden α . El módulo de la Ecuación X representa la información recuperada (400). El término $k_\alpha^*(u, v) \otimes_\alpha k_\alpha(u, v) \otimes_\alpha k_{aux}^*(x, y)$ no es exactamente una función delta de Dirac ($\delta(x, y)$); razón por la cual, se presenta ruido sobre el plano de recuperación. Un ejemplo de información recuperada (400) se muestra en la Figura 9, allí se puede notar que la información recuperada (400) contiene ruido.

Según algunas realizaciones de la invención, en el montaje óptico para descriptación ilustrado en la Figura 8, la onda plana (40) puede ser reemplazada por una onda esférica divergente o convergente.

En algunas realizaciones del método óptico de encriptación-descriptación aquí descrito, se requiere un único registro con el elemento de adquisición de luz (105); y la información encriptada (300) y la llave de seguridad (301) se transmiten al usuario autorizado por canales diferentes.

Aunque la presente invención, en sus modalidades preferidas, el proceso de encriptación se encuentra implementado en el dominio de Fresnel, que involucra la propagación de la luz en el espacio libre (no se incluye ningún elemento óptico entre el elemento de proyección (104) y el elemento de adquisición de luz (105)), se pueden obtener variantes al introducir

una lente en el camino que sigue la luz, permitiendo implementar el proceso óptico en los dominios de Fourier o fraccional dependiendo de las distancias entre la lente, el elemento de proyección (104) y de adquisición de luz (105); si esas distancias son iguales a la longitud focal de la lente se tiene el dominio de Fourier, en otro caso sería el dominio fraccional.

En otras modalidades, el proceso de encriptación-desencriptación también se puede implementar considerando otro tipo de transformadas, como la Hartley, de rotación, jigsaw, Arnold, Mellin o coseno discreta, entre otras; si estas transformadas se pueden hacer ópticamente, se pueden implementar en un dispositivo como el aquí descrito, y en un sistema virtual de desencriptación (120).

Sistema óptico de encriptación - desencriptación de información

En otra modalidad preferida, la presente invención es un sistema óptico de encriptación - desencriptación de información caracterizado por que comprende: un dispositivo óptico de encriptación de información (1), y un dispositivo de computación (110) conectado al dispositivo óptico de encriptación (1), en donde el dispositivo de computación (110) incluye una memoria; y al menos un procesador configurado para: extraer la información encriptada (300) y la llave de seguridad (301) de la información registrada con el elemento de adquisición de luz (105) del dispositivo óptico (1), y recuperar la información original (400), por medio de la información encriptada (300), la llave de seguridad (301) y un sistema óptico virtual de desencriptación (120).

Dicho sistema óptico virtual de desencriptación (120) es ejecutado por el dispositivo de computación (110) y realiza numéricamente el mismo proceso de desencriptación mencionado anteriormente, el cual también puede ser realizado por el montaje físico de la Figura 8.

Modalidades para encriptación-desencriptación libres de ruido

Las anteriores modalidades preferidas ya descritas (dispositivo, método y sistema) pueden incluir procesos de encriptación-desencriptación con recuperación libre de ruido. Para llevar a cabo la desencriptación de un dato libre de ruido se utiliza un contenedor gráfico de información, el cual está basado en códigos CDPO (códigos diseñados para el procesamiento óptico). Los CDPO tienen la ventaja de que la información que contienen puede ser leída a pesar de contener ruido. Los CDPO son imágenes que se generan a partir de la representación binaria de los caracteres alfanuméricos ASCII.

El CDPO de un solo carácter es una imagen binaria dividida en nueve bloques (3×3), de los cuales se usan 8 para representar el byte asociado al código binario (8 bits) y el noveno

bloque siempre permanece negro. El color del centro de cada bloque está definido por el valor del bit correspondiente: negro si el bit es “0” o blanco si el bit es “1”; entre bloques hay un espacio negro o borde. Los bits se asignan a los bloques de izquierda a derecha (tres) y luego de arriba hacia abajo (tres). Como ejemplo de la asignación de los bits se muestra el CDPO para la letra “o” en la Figura 10. La letra “o” tiene como código binario el “01101111”; entonces, el centro del primer bloque (B1) es negro, ya que el bit asociado es 0; el centro del segundo bloque (B2) es blanco, ya que el bit asociado es 1, y así sucesivamente hasta el octavo bloque (B8) cuyo centro es brillante, ya que el bit asociado es 1. Como se indicó antes, el noveno bloque (B9) siempre es negro.

Cuando se trata de un mensaje con varios caracteres, estos se ubican en distintas secciones de una imagen final, manteniendo el mismo tamaño. Por ejemplo, en la Figura 11 se muestra el CDPO asociado al mensaje “Hola” (código binario por letra H:01001000, o: 01101111, l:01101100, y a:01100001), el cual se ha ubicado en una imagen cuadrada. Esta imagen se ha dividido en cuatro secciones y cada sección corresponde al CDPO de una de las letras del mensaje.

Cualquier CDPO puede ser encriptado y desencriptado usando los procedimientos descritos previamente.

La Figura 12 muestra el diagrama del proceso que sigue un CDPO para encriptar y desencriptar un mensaje libre de ruido en el sistema aquí revelado. En primer lugar, la información a encriptar “Hola” (30) se convierte en un CDPO (31). Luego, la imagen asociada al CDPO sigue el proceso de encriptación (32) descrito para el dispositivo óptico (1) hasta generar su información encriptada y llave de seguridad, los cuales son usados para la desencriptación (33) usando un sistema óptico virtual (120) o un montaje óptico-físico según la Figura 8. El CDPO recuperado es luego filtrado (34), multiplicando el mismo por el CDPO del mensaje “ÿÿÿÿ” (cuyos bloques son todos 1). Finalmente, el CDPO filtrado pasa por el proceso de lectura (35) para recuperar la información original “Hola”.

Nótese que el CDPO recuperado y filtrado no es una imagen binaria debido al ruido asociado con la desencriptación. Los pixeles de un bloque “0” no son totalmente negros, por lo que se define un valor de umbral al momento de asociar el valor del bit (0 o 1) a cada bloque durante la lectura.

Finalmente, mediante el proceso ilustrado anteriormente la información contenida en el CDPO puede ser recuperada libre de ruido, a pesar de que los CDPO estén afectados por el ruido asociado a los procesos de encriptación y desencriptación. La “lectura” del CDPO

desencriptado y filtrado garantiza la obtención de la información original sin ningún tipo de ruido.

En otras modalidades, los CDPO usados para una desencriptación libre de ruido pueden ser sustituidos por otro tipo de códigos gráficos con el mismo propósito; por ejemplo, códigos de barras o códigos QR.

Las modalidades aquí reveladas ejemplifican la invención, la cual no está limitada a dichas realizaciones, y su alcance puede incluir variaciones y modificaciones obvias de dichas modalidades.