ENCRIPTACIÓN DE IMÁGENES DIGITALES UTILIZANDO EL MÉTODO DE MÁSCARA DE FASE ALEATORIA

MARIE ELIZABETH BOTHIA VARGAS

CHRISTIAN CAMILO DELGADO MOLINA

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES EXACTAS Y DE LA EDUCACIÓN

PROGRAMA DE INGENIERIA FÍSICA

2017

ENCRIPTACION DE IMÁGENES DIGITALES UTILIZANDO EL MÉTODO DE MÁSCARA DE FASE ALEATORIA

MARIE ELIZABETH BOTHIA VARGAS

CHRISTIAN CAMILO DELGADO MOLINA

Trabajo de grado presentado como requisito parcial para optar por el título de Ingeniera Física e Ingeniero Físico

Trabajo de investigación

Director

Ing. Mario Milver Patiño Velasco, MSc.

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES EXACTAS Y DE LA EDUCACIÓN

PROGRAMA DE INGENIERIA FÍSICA

2017

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

TABLA DE CONTENIDO

LISTA DE FIGURAS

pág.

pág.

pág.

INTRODUCCIÓN

Desde el momento en que el hombre comenzó a comunicarse, se han establecido códigos para hacer más efectiva la transmisión de la información y a lo largo de la historia, se ha hecho necesario discernir entre el tipo de información a compartir y la que se debe mantener en secreto. A partir de este enfoque se han desarrollado sistemas que permiten transmitir información confidencial o privada a personas o grupos, es así que se han desarrollado lenguajes, escrituras, códigos que permiten obtener confiabilidad a la hora de entregar la información. Recientemente, la información se ha hecho más pública, con la llegada de internet, y cada vez es más difícil que sea clasificada como confidencial y se cuide lo privado.

La era digital ha traído consigo un gran flujo de datos e imágenes digitales que son de carácter confidencial. Muchas situaciones de transmisión de información e imágenes como las militares y de estado, videoconferencias confidenciales, imágenes médicas, fotografías personales en línea (álbum), TV por cable, etc. requieren de un sistema de seguridad confiable, rápido y robusto para almacenar y transmitir la información. Esto ha llevado a tratar el tema de seguridad de imágenes digitales de manera más delicada y ha propiciado el desarrollo de técnicas en el área de la encriptación.

Buscando métodos y herramientas que permitan llegar a tener confiabilidad en la información transmitida, se han propuestos protocolos y herramientas, una de ellas la propone la óptica. El trabajo realizado por Refrégiér y Javidi (1995) abrió el camino para el desarrollo de múltiples propuestas en el área de la seguridad óptica; siendo esta contribución la primera idea de lo que hoy son los sistemas ópticos de encriptación. Se han implementado variaciones en sistemas opto-digitales y en sistemas ópticos virtuales de encriptación. El

trabajo inicial, fue mostrar simulaciones numéricas y conceptos matemáticos necesarios para desarrollar la idea de codificar una imagen, sugiriendo que la experiencia podría ser implementada, tanto óptica como electrónicamente. Partiendo de esto, se han desarrollado soluciones a este problema, una de ellas se fundamenta en el sistema desarrollado por Marechal y Croce hacia principios de los años cincuenta, el sistema hoy conocido como arquitectura 4f. Esta arquitectura es la más estudiada para realizar procesamiento óptico de información, ya que es un arreglo experimental de simple descripción matemática, es básico y el más usado para realizar procesados ópticos coherentes, en filtrado espacial, reconocimiento de patrones, correlación óptica, etc. Estas aplicaciones se basan en variaciones de los elementos involucrados en cualquiera de los tres planos principales del sistema 4f: plano de entrada, de frecuencias y de salida.

En el presente documento se realiza un estudio sobre esta técnica, analizando su aplicabilidad a la encriptación de imágenes digitales. En el primer capítulo se encuentra un breve recorrido por el concepto y desarrollo de la difracción de Huygens- Fresnel y el uso de la lente delgada como elemento transformador de Fourier bidimensional. En el segundo capítulo se presenta la historia de la criptología y su relación actual con la óptica. En el tercer capítulo se describe la metodología propuesta para el desarrollo del trabajo y en el cuarto y último capítulo se presentan los resultados obtenidos y su discusión.

1. FUNDAMENTOS DE DIFRACCIÓN

1.1 Introducción

La difracción es el fenómeno por el cual se produce una desviación de los rayos luminosos cuando pasan por un cuerpo opaco o por una abertura de diámetro comparable al de la longitud de onda [5]. La primera referencia de este fenómeno se debe a Grimaldi y fue publicada en 1665. Para observarla, utilizó un dispositivo experimental, análogo a la figura 1.1. En él se iluminaba una pantalla opaca, sobre la que había una abertura suficientemente pequeña, de forma que el efecto penumbra fuese despreciable; y se observaba la intensidad luminosa en un plano ubicado a una determinada distancia detrás de la pantalla. Según la teoría corpuscular de la propagación de la luz, que en la época era utilizada para explicar los fenómenos ópticos, la sombra de la pantalla debería aparecer bien definida; sin embargo, las observaciones de Grimaldi indicaban que la transición entre la luz y la sombra era progresiva y no abrupta.

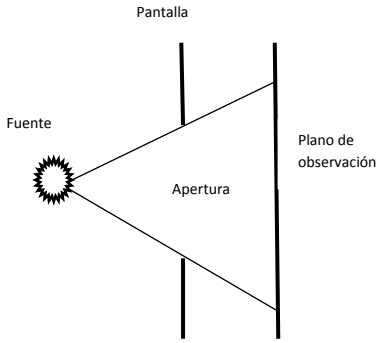


Figura 1.1. Dispositivo utilizado para observar la difracción de la luz

La difracción se explica, a través del principio de Huygens-Fresnel, como el resultado de la superposición de una gran cantidad de ondas secundarias

provenientes tanto del medio de propagación como de los bordes del obstáculo que la onda atraviesa [8].

1.2 Principio de Huygens-Fresnel

Suponiendo que se tiene una configuración como la de la figura 1.2, correspondiente a una ranura que está siendo atravesada por una onda plana y que la apertura, que está en el plano (ξ,η), es iluminada en la dirección positiva del eje z[1]. El campo U sobre un plano (x,y), paralelo al plano (ξ,η) y separado de el por una distancia z será:

$$U(P_o)=\frac{1}{j\lambda}\iint_S U(P_1)\frac{\exp(jkr_{01})}{r_{01}}\cos\theta ds \qquad (1.1)$$

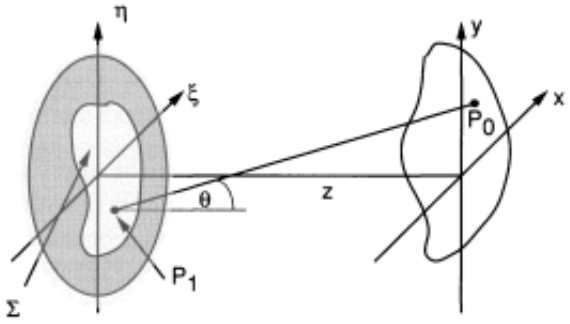


Figura1.2 Geometría de difracción

De acuerdo con la ecuación (1.1), y teniendo en cuenta que $\cos\theta = \frac{z}{r_{01}}$, el principio de Huynges-Fresnel se puede expresar como

$$U(x,y) = \frac{1}{j\lambda}\int\int_S U(\xi,\eta)\frac{exp(jkr_{01})}{r_{01}^2}d\xi d\eta \qquad (1.2)$$

Donde la distancia r_{01} viene dada exactamente por :

$$r_{01} = \sqrt{z^2+(x-\xi)^2+(y-\eta)^2} \qquad (1.3)$$

Cuando la distancia de observacion esta a muchas longitudes de onda de la abertura, $r_{01}>>\lambda$, la funcion descrita por la ecuación 1.2 es rapidamente variable en la fase y lentamente variable en amplitud.

Considerando que el plano de observación está muy alejado de la abertura y que el tamaño de la ranura es pequeño, es posible aplicar la expansion binomial al valor de r_{01} de la siguiente manera:

$$r_{01} \approx z\left[1+\frac{1}{2}\left(\frac{x-\xi}{z}\right)^2+\frac{1}{2}\left(\frac{y-\eta}{z}\right)^2\right] \tag{1.4}$$

Dependiendo del grado de aproximacion necesario para r_{01} se hace necesario utilizar o no con todos los terminos de aproximacion. En la ecuación 1.2, donde el r_{01}^2 que aparece en el denominador, el error introducido por despreciar todos los terminos, excepto z es, en general, aceptablemente pequeño; sin embargo, para el r_{01} que aparece en el exponente, los errores son más críticos, por un lado estan multiplicados por k, que es del orden de $10^7\ m^{-1}$, por lo que cambios de r_{01} pequeños pueden cambiar significativamente el valor de la fase. En este caso , es conveniente en el exponente quedarse con ambos términos del desarrollo de la serie. Por consiguiente, la expresión para el campo en el plano de observación se reduce a:

$$U(x,y)=\frac{e^{jkz}}{2z}e^{j\frac{k}{2z}(x^2+y^2)}\iint_{-\infty}^{\infty}\left\{U(\xi,\eta)e^{j\frac{k}{2z}(\xi^2+\eta^2)}\right\}e^{-j\frac{2\pi}{\lambda z}(x\xi+y\eta)}d\xi d\eta \tag{1.5}$$

La ecuación 1.5 se conoce como integral de Fresnel. Es una práctica común, cuando se utiliza la aproximación de Fresnel, analizar que sucede cuando se aproxima una onda esferica, de la forma $\frac{e^{ikr_{01}}}{r_{01}}$, por superficies cuadráticas dadas por:

$$\frac{\exp(ikz)}{z}\exp\left[\frac{ik}{2z}[(x_0-x_1)^2+(y_0-y_1)^2]\right] \tag{1.6}$$

El error que se comete al despreciar el orden inmediatamente superior es de la forma $-z\frac{u^2}{8}$, esto significa que se considera $e^{\frac{-ikzu^2}{8}}\cong 1$. Una condicion suficiente para la validez de este supuesto será que el maximo cambio de

fase inducido por despreciar el termino $kz\frac{u^2}{8}$ sea mucho menor que un radián. Esta situación ocurre siempre que la distancia z cumpla la condicion:

$$z^3 \gg \frac{\pi}{4\lambda}[(x_0 - x_1)^2 + (y_0 - y_1)^2]^2{}_{max} \tag{1.7}$$

Si además de la aproximacion de Fresnel se satisface la siguiente condición, llamada aproximacion de Fraunhoufer, que es aún más restrictiva:

$$z \gg \frac{k(\xi^2+\eta^2)_{max}}{2} \tag{1.8}$$

Entonces el factor de fase cuadrática bajo el signo de la integral en la ecuacion de Fresnel, ecuación (1.5), es aproximadamente igual a la unidad sobre toda la abertura y la amplitud del campo puede ser hallada a partir de la ecuación:

$$U(x,y) = \frac{e^{jkz}e^{j\frac{k}{2z}(x^2+y^2)}}{j\lambda z}\iint_{-\infty}^{\infty} U(\xi,\eta)\exp\left[-j\frac{2\pi}{\lambda z}(x\xi + y\eta)\right]d\xi d\eta \tag{1.9}$$

Aparte de factores multiplicativos de fase que preceden la integral, esta expresión es la transformada de Fourier de la distribucion del campo sobre la abertura, en funcion de la frecuencias espaciales

$$f_X = \frac{x}{\lambda z} \quad , \quad f_Y = \frac{y}{\lambda z} \tag{1.10}$$

1.3 Efecto de la lente delgada sobre una onda

Una lente está constituida por un material ópticamente denso, en el cual la velocidad de propagación de una perturbación óptica es menor que en el aire. Se dice que una lente delgada simplemente retrasa la fase de un frente de onda incidente en una cantidad proporcional al espesor de la misma en cada punto [4]. El desfase introducido en la onda al atravesar por la lente, en el punto de coordenadas (x,y), se puede escribir de la siguiente forma:

$$\phi(x,y) = kn\Delta(x,y) + k[\Delta_0 - \Delta(x,y)] \tag{1.11}$$

Donde n es el índice de refracción del material de la lente, knΔ(x,y) es el desfase introducido por la lente y k[Δ_0-Δ(x,y)] el introducido por el espacio restante que queda entre los dos planos. La figura 1.3 ilustra las distancias consideradas para definir la función espesor.

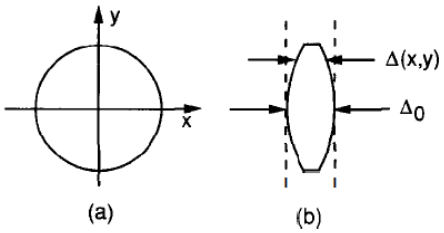


Figura 1.3 Función espesor (a) vista frontal (b) vista lateral

Se puede representar el efecto producido por la lente por medio de una transformación de fase multiplicativa

$$t_l(x,y) = \exp\{jk\Delta_0\}\exp\{jk(n-1)\Delta(x,y)\} \tag{1.12}$$

El campo complejo $U_l'(x,y)$ sobre un plano inmediatamente detrás de la lente se relaciona con el campo complejo incidente $U_l(x,y)$ sobre un plano inmediatamente delante de la lente mediante:

$$U_l'(x,y) = t_l(x,y)U_l(x,y) \tag{1.13}$$

Con el fin de precisar el efecto de la forma de la lente (figura 1.4) sobre las transformaciones de fase introducidas sobre la onda, es necesario tener en cuenta sus radios de curvatura y su espesor.

A partir de la convención de signos, se establece que si el centro de curvatura de una superficie está antes que su vértice entonces su radio de curvatura es un número negativo y en caso contrario, es positivo. Para calcular la expresión de la función espesor se toman en cuenta las tres funciones de espesores individuales (ver figura 1.4) de la siguiente manera:

$$\Delta(x,y) = \Delta_1(x,y) + \Delta_2(x,y) + \Delta_3(x,y) \tag{1.14}$$

donde

$$\Delta_1(x,y) = \Delta_{01} - \left(R_1 - \sqrt{R_1^2 - x^2 - y^2}\right)$$
$$\Delta_2(x,y) = \Delta_{02} = Constante) \qquad (1.15)$$
$$\Delta_3(x,y) = \Delta_{03} - \left(R_2 - \sqrt{R_2^2 - x^2 - y^2}\right)$$

Por tanto la función espesor (1.14) estará dada por

$$\Delta(x,y) = \Delta_0 - R_1\left(1 - \sqrt{1 - \frac{x^2+y^2}{R_1^2}}\right) - R_2\left(1 - \sqrt{1 - \frac{x^2+y^2}{R_2^2}}\right) \qquad (1.16)$$

Donde $\Delta_0 = \Delta_{01} + \Delta_{02} + \Delta_{03}$

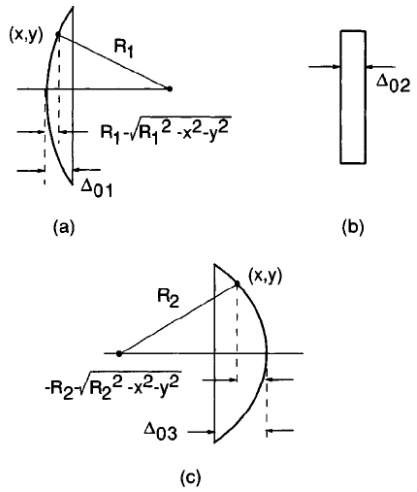


Figura 1.4 Esquema geométrico para el cálculo de los espesores de las distintas partes de la lente. a. Δ1(x,y), b. Δ2 y c. Δ3(x,y)

Analizando la función espesor desde el punto de vista de la teoría paraxial, donde los valores de x e y son muy pequeños, las ecuaciones 1.15 se transforman en:

$$\sqrt{1-\frac{x^2+y^2}{R_1^2}} \cong 1-\frac{x^2+y^2}{2R_1^2}$$

$$\sqrt{1-\frac{x^2+y^2}{R_2^2}} \cong 1-\frac{x^2+y^2}{2R_2^2} \tag{1.17}$$

Por lo que la función espesor se convierte en:

$$\Delta(x,y) = \Delta_0 - \frac{x^2+y^2}{2}\left(\frac{1}{R_1}-\frac{1}{R_2}\right) \tag{1.18}$$

La expresión para la transformación de fase producida por la lente (ecuación 1.12) se convierte en:

$$t_l(x,y) = \exp\{jk\Delta_0\}\exp\left\{-jk(n-1)\frac{x^2+y^2}{2}\left(\frac{1}{R_1}-\frac{1}{R_2}\right)\right\} \tag{1.19}$$

Las características físicas de la lente pueden ser representadas por un único numero f, llamado distancia focal, definido por

$$\frac{1}{f} = (n-1)\left(\frac{1}{R_1}-\frac{1}{R_2}\right) \tag{1.20}$$

Despreciando el factor de fase constante, la transformación de fase será entonces:

$$t_l(x,y) = \exp\left\{-j\frac{k}{2f}(x^2+y^2)\right\} \tag{1.21}$$

Esta ecuación será la forma de representar los efectos de una lente delgada sobre una perturbación incidente (despreciando el espesor finito de la lente). El convenio de signos adoptado permite aplicar este resultado a los demás tipos de lentes, teniendo en cuenta el signo de su distancia focal.

El significado físico de la transformación de fase producida por una lente se puede comprender mejor considerando el efecto que produce sobre una onda plana que incide normalmente sobre ella. Si la onda incidente, sobre el plano tangente a la cara anterior de la lente, tiene una amplitud igual a la

unidad, las ecuaciones (1.13) y (1.21) conduce a la siguiente expresión para el campo U_l' a la salida de la lente:

$$U_l'(x,y) = \exp\left\{-j\frac{k}{2f}(x^2+y^2)\right\} \tag{1.22}$$

Esta expresión se puede interpretar como una aproximación cuadrática a una onda esférica. Una lente limitada por dos superficies esféricas transformará una onda plana incidente en una onda esférica, bajo la aproximación paraxial. Si las condiciones de incidencia de la onda no son paraxiales, el frente de onda emergente presentará diferencias con la onda esférica perfecta (aberraciones), incluso cuando las superficies de la lente sean perfectamente esféricas.

1.4 Generación de la transformada de Fourier con una lente

Una de las propiedades más importantes y útil de una lente convergente es su capacidad para realizar la transformada de Fourier bidimensional de una distribución de campo presente en su entrada. Para lograrlo, es necesario que la onda incidente sea monocromática y que el plano de observación esté ubicado en el plano focal de la lente [6].

Para modelar matemáticamente esta característica, se supone que la iluminación es monocromática y que el sistema bajo estudio es lineal. Bajo estas condiciones los sistemas son coherentes y lineales en la amplitud compleja, por lo que interesa es la distribución de la amplitud sobre un plano concreto detrás de la lente convergente. La imagen a la que se le realizará la transformada de Fourier se introduce en el sistema óptico mediante un elemento cuya transmitancia en amplitud es proporcional a la función de entrada objeto de estudio. La ubicación de la información de entrada define tres sistemas, que se presentan en la figura 1.5.[3]

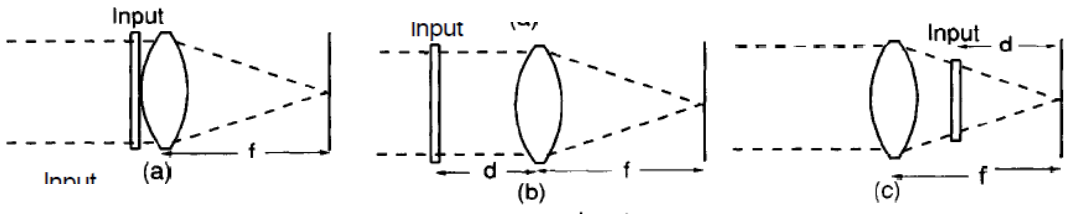


Figura 1.5. Configuraciones geométricas para la realización de la transformada de Fourier con una lente convergente (a) dispositivo objeto colocado justo delante de la lente. (b) dispositivo colocado a una distancia d delante de la lente, (c) colocado detrás de la lente a una distancia d de su plano focal

1.4.1 Objeto situado antes de la lente

La transmitancia en amplitud del objeto viene representada por t_A. Por otra parte, sea $F_o(f_X, f_Y)$ el espectro de Fourier de la onda transmitida por el objeto y $F_l(f_X, f_Y)$ el espectro de Fourier de la onda incidente sobre la lente: esto es:

$$F_o(f_X, f_Y) = \mathcal{F}\{At_A\} \qquad F_l(f_X, f_Y) = \mathcal{F}\{U_l\} \tag{1. 23}$$

Suponiendo valida la aproximación paraxial para la propagación sobre una distancia d, entonces F_o y F_l están relacionados por medio de la expresión:

$$F_l(f_X, f_Y) = F_o(f_X, f_Y) exp\{-j\pi\lambda d(f_X^2 + f_Y^2)\}, \tag{1.24}$$

donde se ha omitido un desplazamiento de fase constante

Asumiendo que la lente tiene un diámetro mayor que el objeto, la expresión puede ser escrita así:

$$\mathrm{U_f(u,v)} = \frac{\exp\left\{\mathrm{j}\frac{\mathrm{k}}{2\mathrm{f}}(\mathrm{u}^2+\mathrm{v}^2)\right\}}{\mathrm{j\lambda f}} F_l\left(\frac{u}{\lambda f}, \frac{v}{\lambda f}\right) \tag{1.25}$$

Sustituyendo (1.24) en (1.25) se obtiene:

$$\mathrm{U_f(u,v)} = \frac{\exp\{\mathrm{j}\frac{\mathrm{k}}{2\mathrm{f}}(1-\frac{d}{f})(\mathrm{u}^2+\mathrm{v}^2)\}}{\mathrm{j\lambda f}} \times \iint_{-\infty}^{\infty} \mathrm{t}_A(\xi\mathrm{u}, \eta\mathrm{v})\, \mathrm{d}\xi\mathrm{d}\eta \tag{1.26}$$

La amplitud y la fase de la onda en las coordenadas (u,v) del plano de observación están de nuevo relacionadas con la amplitud y la fase del espectro del objeto en las frecuencias (u/λf. v/λf). Cuando el objeto está situado en el plano focal de entrada de la lente (d = f), la curvatura de fase desaparece, dando lugar a una transformada de Fourier exacta.

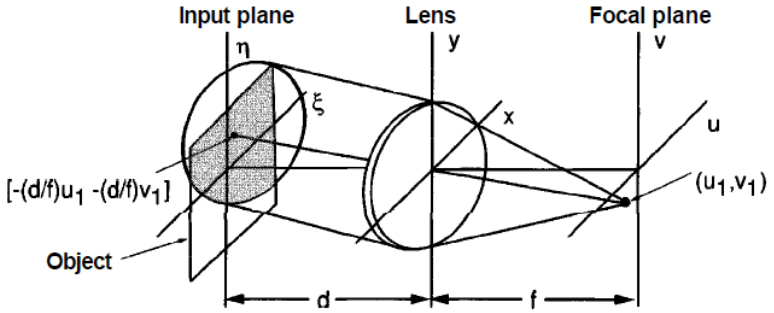


Figura 1.6. Recorte de la señal de entrada. El área sombreada en el plano de entrada representa la parte del objeto que contribuye a la transformada de Fourier en (u1, v1)

La amplitud de la luz en las coordenadas (u_1, v_1) es debida a la contribución de todos los rayos que se propagan en la dirección cuyos cosenos directores son $(\xi \approx u_1/f, \eta \approx v_1/f)$. Por lo tanto, pueden ser tenidas en cuenta las dimensiones finitas de la abertura por medio de la proyección geométrica de esta sobre el plano del objeto, realizando la proyección a lo largo de la línea que une el punto de coordenadas (u_1 , v_1) en el plano focal imagen. En la figura 1.6 el valor de U_f en el punto de coordenadas (u,v) puede ser hallado por la transformada de Fourier de la parte del objeto que abarca la proyección de la función pupila P, centrada en las coordenadas [ξ=-(d/f)u, η=-(d/f)v]. Lo anterior se expresa mediante:

$$U_f(u,v) = \frac{A\exp\{j\frac{k}{2f}(1-\frac{d}{f})(u^2+v^2)\}}{j\lambda f} \times \iint_{-\infty}^{\infty} t_A(\xi,\eta)\, P\left(\xi+\frac{d}{f}u, \eta+\frac{d}{f}v\right) \exp\left\{-j\frac{2\pi}{2j}(\xi u+\eta v)\right\} d\xi d\eta \quad (1.27)$$

La limitación efectiva del objeto por la abertura de la lente es conocida como efecto de *viñeteo*. Este efecto en el espacio objeto es débil cuando el objeto está colocado muy cerca de la lente y cuando la abertura de esta es mucho mayor que el objeto. En la práctica, cuando lo que interesa es la transformada de Fourier del objeto, a menudo se prefiere colocar este directamente contra la lente para minimizar el viñeteo: sin embargo, para simplificar los cálculos, es generalmente más cómodo colocar el objeto en el plano focal objeto, donde la relación de transformación se libera de los factores cuadráticos de fase.

1.5 Formación de la imagen

La propiedad más popular de las lentes es, sin duda alguna, su capacidad para formar imágenes. Si se coloca un objeto delante de una lente convergente y se ilumina, bajo condiciones apropiadas aparecerá, en un segundo plano, una distribución de intensidad de luz que se asemeja al objeto.

A esta distribución de intensidad se le denomina *imagen* del objeto. La imagen puede ser real, en el sentido de que la distribución de intensidad aparece realmente en un plano situado detrás de la lente, o puede ser *virtual* si la luz parece provenir de una distribución de intensidad en otro punto situado delante de la lente. (Figura 1.7)

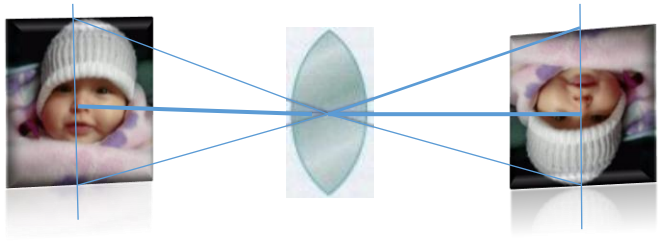


Figura 1.7. Formación de una imagen con una lente convergente

1.5.1 Respuesta de impulso de una lente convergente

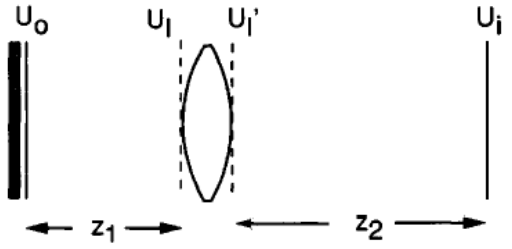


Figura 1.8 configuración geométrica para la formación de la imagen

Teniendo en cuenta la linealidad del fenómeno de propagación de la onda, se puede expresar el campo U_i (Figura 1.8) como la superposición de infinitas funciones básicas de onda [4], es decir:

$$U_i(u,v) = \iint_{-\infty}^{\infty} h(u,v;\xi,\eta)U_o(\xi,\eta)d\xi d\eta \qquad (1.28)$$

Donde $h(u,v;\xi,\eta)$ es la amplitud del campo en el punto de coordenadas (u,v) producida para una fuente puntual de amplitud unitaria situada en el punto de coordenadas (ξ,η). Para un sistema lineal y estacionario estarán definidas las propiedades del sistema formador de imagen especificando su respuesta al impulso $h(u,v;\xi,\eta)$.

Si U_i es parecida a U_o esto equivale a una respuesta de impulso muy parecida a una delta Dirac , así:

$$h(u,v;\xi,\eta) \approx K\delta(u \pm M\xi, v \pm M\eta) \qquad (1.29)$$

donde K es una constante compleja y M representa el aumento del sistema. Los signos más y menos están incluidos para evidenciar la ausencia o la presencia de la imagen invertida.

Para determinar la respuesta de impulso *h*, se considera una función δ en las coordenadas (ξ, η), que en la aproximación paraxial se puede escribir mediante:

$$U_l(x.y) \approx \frac{1}{j\lambda z_1} exp\{j\frac{1}{2z_1}[(x-\xi)^2+(y-\eta)^2]\} \qquad (1.30)$$

Después de su paso a través de la lente, la distribución de campo tiene la forma:

$$U_l'(x.y) = U_l(x.y)P(x,y)exp\{-j\frac{1}{2f}[x^2+y^2]\} \qquad (1.31)$$

Utilizando la ecuación para la difracción de Fresnel y teniendo en cuenta la distancia de propagación z_2, se tiene:

$$h(u,v;\xi,\eta) = \frac{1}{\lambda^2 z_1 z_2}\exp\left\{j\frac{k}{2z_2}(u^2+v^2)\right\}\exp\left\{j\frac{k}{2z_2}(\xi^2+\eta^2)\right\}\times\iint_{-\infty}^{\infty}P(x,y)\exp\{j\frac{k}{2}\left(\frac{1}{z_1}+\frac{1}{z_2}-\frac{1}{f}\right)(x^2+y^2)\times\exp\left\{-jk\left(\frac{\xi}{z_1}+\frac{\eta}{z_2}\right)x+\left(\frac{\eta}{z_1}+\frac{v}{z_2}\right)y\right\}dxdy \qquad (1.32)$$

Las ecuaciones (1.28) y (1.32) proporcionan una solución formal, especificando la relación existente entre el objeto U_o y la imagen U_i. Sin embargo, es difícil determinar las condiciones bajo las cuales U_i puede ser llamada una imagen de U_o.

Los términos que contienen los factores cuadráticos de fase son los más molestos de la respuesta de impulso. Dos de estos términos son independientes de las coordenadas de la lente, así:

$$\exp\{j\frac{k}{2z_2}(u^2+v^2)\} \quad \text{y} \ \exp\{j\frac{k}{2z_1}(\xi^2+\eta^2)\} \qquad (1.33)$$

Mientras que el otro si depende de las variables de integración:

$$\exp\{j\frac{k}{2}(\frac{1}{z_1}+\frac{1}{z_2}-\frac{1}{f})(x^2+y^2)\} \qquad (1.\ 34)$$

El efecto del ensanchamiento de la respuesta de impulso se le atribuye a la presencia de un factor cuadrático de fase, sin el cual se tendría una transformada de Fourier exacta [7]. Por esta razón se elige la distancia z_2 al plano imagen de tal manera que este término sea idénticamente nulo. Es decir:

$$\frac{1}{z_1} + \frac{1}{z_2} - \frac{1}{f} = 0 \qquad (1.35)$$

La ecuación anterior es la ecuación de las lentes delgadas de la óptica geométrica y debe ser satisfecha para conseguir formar la imagen.

Por otra parte, el factor de fase cuadrático que depende solamente de las coordenadas del plano imagen (u.v) se puede ignorar bajo las siguientes condiciones:

1. Si nos interesa la distribución de intensidad en el plano imagen, en este caso la distribución de fase asociada con la imagen es irrelevante.

2. Si nos interesa la distribución de amplitud del campo imagen y ésta se encuentra medida sobre una superficie esférica de radio z_2, centrada en el punto donde el eje óptico atraviesa la lente delgada.

En las coordenadas del plano objeto (ξ,η) se considera el factor cuadrático de fase; este término depende de las variables sobre las cuales se realiza la operación de convolución, afectando significativamente al resultado de esa integración. Existen tres condiciones diferentes bajo las cuales este término puede ser ignorado:

1. El objeto está sobre la superficie de una esfera de radio z1, centrada en el punto en el que el eje óptico atraviesa la lente delgada.

2. El objeto está iluminado por una onda esférica que converge hacia el punto en el que el eje óptico atraviesa la lente.

3. La fase del factor cuadrático cambia en una cantidad que es solo una fracción pequeña de radián dentro de la región del objeto que contribuye significativamente al campo en el punto imagen concreto (u,v).

Suele suceder en la práctica que la primera de estas condiciones no se cumple; sin embargo, la segunda se cumple fácilmente, eligiendo una estrategia adecuada de iluminación. En la figura 1.9, la iluminación con una onda esférica tiene como consecuencia que la transformada de Fourier del objeto aparezca en la pupila de la lente. El factor cuadrático de fase se anula completamente con esta onda esférica convergente.

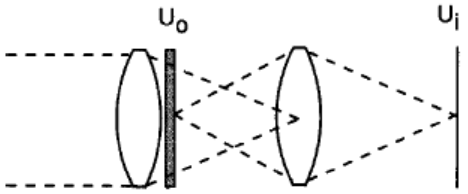


Figura 1.9 Iluminación convergente del objeto

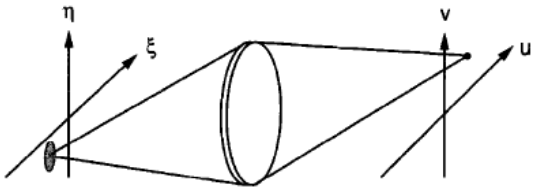


Figura 1.10 Región del espacio objeto que contribuye al campo en un punto concreto de la imagen

Para eliminar el efecto del factor cuadrático de fase en las coordenadas del objeto, como lo afirma la tercera condición, se requiere modificar la configuración del sistema. En una configuración geométrica para la formación de la imagen, la respuesta del sistema a un impulso en las coordenadas concretas del objeto debe extenderse solamente sobre una

pequeña región del espacio imagen que rodea exactamente al punto imagen que corresponde a ese punto objeto particular. Si este no fuera el caso, el sistema produciría una imagen borrosa inaceptable. La respuesta al impulso para un punto imagen fijo, como especifica la función de peso en el espacio objeto que contribuye a ese punto imagen, debe considerar solo una región pequeña del objeto que pueda contribuir a la formación un punto imagen dado. En la figura 1.10+ el circulo gris de la izquierda es el área que aporta las contribuciones más significativas el punto imagen concreto de la derecha. Sobre esta región el factor $(k/2z_1)(\xi^2+\eta^2)$ cambia en una cantidad que es solo una pequeña fracción de radián, el factor cuadrático de fase en el plano objeto puede ser sustituido por una única fase que depende del punto imagen (u,v) que viene siendo de interés, pero no depende de las coordenadas del objeto (ξ,η). Bajo esta consideración, la ecuación representativa se convierte en:

$$\exp\left\{j\frac{k}{2z_1}(\xi^2+\eta^2)\right\} \longrightarrow \exp\left\{j\frac{k}{2z_1}\left(\frac{u^2+v^2}{M^2}\right)\right\} \tag{1.36}$$

Donde M es el aumento del sistema y tiene un valor de $-z_2/z_1$. Si el interés se centra en la distribución de intensidad de la imagen, este nuevo factor cuadrático de fase en el espacio imagen puede ser ignorado.

La aproximación es válida siempre que el tamaño del objeto no sea mayor de aproximadamente ¼ del tamaño de la abertura de la lente. La siguiente expresión es el resultado de la afirmación anterior, para la respuesta de impulso del sistema formador de imagen:

$$h(u,v:\xi,\eta) \approx \frac{1}{\lambda^2 z_1 z_2}\iint_{-\infty}^{\infty} P(x,y)\times\exp\{-jk[\left(\frac{\xi}{z_1}+\frac{u}{z_2}\right)x+\left(\frac{\eta}{z_1}+\frac{v}{z_2}\right)y]\}dxdy \tag{1.37}$$

Recordando que el aumento del sistema está dado por $-z_2/z_1$, se ha incluido el signo menos para suprimir los efectos de la inversión de la imagen, la respuesta de impulso quedara:

$$h(u,v:\xi,\eta) \approx \frac{1}{\lambda^2 z_1 z_2}\iint_{-\infty}^{\infty} P(x,y)\times \exp\{-j\frac{2\pi}{\lambda z_2}[(u-M\xi)x+(v-M\eta)y]\}dxdy \quad (1.38)$$

Como la ecuación de las lentes delgadas se cumple, la respuesta al impulso viene dada por la figura de difracción de Fraunhofer de la abertura de la lente, centrada en el punto del plano imagen de coordenadas (u=Mξ, v=Mη) al elegir z_2 de manera que satisfaga la ecuación de las lentes delgadas, es decir, se busca el plano hacia el cual converge la onda esférica que sale de la lente, limitando la extensión de la onda esférica.

1.5.2 Relación entre objeto e imagen

Definiendo un sistema formador de imagen perfecto, se obtiene una réplica invertida y aumentada (o disminuida) del objeto. Estableciéndose la relación:

$$U_i(u,v) = \frac{1}{|M|}U_0\left(\frac{u}{M},\frac{v}{M}\right) \quad (1.39)$$

La respuesta es la de un sistema lineal espacialmente variante, resultado directo del aumento y de la inversión de la imagen que tiene lugar durante la operación de formación. Sin embargo, objeto e imagen están relacionados por una integral de superposición, pero no por una integral de convolución. Se ha de normalizar las coordenadas del objeto para eliminar la inversión y el aumento, así se reduce la relación objeto-imagen en la ecuación de convolución. Normalizando en las variables del plano objeto:

$$\tilde{\xi} = M\xi \; ; \; \tilde{\eta} = M\eta \quad (1.40)$$

La respuesta de impulso se reduce a:

$$h(u,v:\tilde{\xi},\tilde{\eta}) \approx \frac{1}{\lambda^2 z_1 z_2}\iint_{-\infty}^{\infty} P(x,y)\times \exp\{-j\frac{2\pi}{\lambda z_2}[(u-\tilde{\xi})x+(v-\tilde{\eta})y]\}dxdy \quad (1.41)$$

Dependiendo así de las diferencias $u-\tilde{\xi}, v-\tilde{\eta}$.

Normalizando aún más las coordenadas se tiene:

$$\tilde{x} = \frac{x}{\lambda z_2} \; ; \; \tilde{y} = \frac{y}{\lambda z_2} \; ; \; \tilde{h} = \frac{h}{|M|} \tag{1.42}$$

Resultando la relación objeto-imagen:

$$U_i(u,v) = \iint_{-\infty}^{\infty} \tilde{h}\left(u-\tilde{\xi}, v-\tilde{\eta}\right)\left[\frac{1}{|M|} U_0\left(\frac{\tilde{\xi}}{M}, \frac{\tilde{\eta}}{M}\right)\right] d\tilde{\xi} d\tilde{\eta} \tag{1.43}$$

Es decir,

$$U_i(u,v) = \tilde{h}(u,v) \otimes U_g(u,v) \tag{1.44}$$

$$\text{Donde } U_g(u,v) = \frac{1}{|M|} U_0\left(\frac{u}{M}, \frac{v}{M}\right) \tag{1.45}$$

es la imagen predicha por la óptica geométrica y

$$\tilde{h}(u,v) = \iint_{-\infty}^{\infty} P(\lambda z_2 \tilde{x}, \lambda z_2 \tilde{y}) \exp[-\mathrm{j}2\pi(\mathrm{u}\tilde{x} + \mathrm{v}\tilde{y})] \, d\tilde{x} d\tilde{y} \tag{1.46}$$

Es la respuesta al impulso del sistema y representa la función de dispersión de punto introducida por la difracción.

A partir de la ecuación (1.43) se puede concluir que:

1. La imagen ideal producida por un sistema óptico limitado por la difracción, es decir libre de aberraciones, es una versión a escala e invertida del objeto.
2. El efecto de la difracción es hacer la convolución de la imagen ideal con la figura de difracción de Fraunhofer de la pupila de la lente.

Bibliografía

[1] *BOROVIKOV V A and E. T. Kinber B. Ye.: Geometrical theory of diffraction. Published by: the institution of Electrical Engineers. London, United Kingdom 1994*

[2] *GOODMAN Joseph W.: Introduction to Fourier Optics. Vol II. McGraw-Hill book Company, 1996, pp 30-46*

[3] *GOODMAN Joseph W.: Introduction to Fourier Optics. Vol II. McGraw-Hill book Company, 1996, pp 57-65*

[4] *GOODMAN Joseph W.: Introduction to Fourier Optics. Vol II. McGraw-Hill book Company, 1996, pp 77-95*

[5] *KBAKER, B., and E.T. Copson E.: The mathematical Theory of Huygens' Principle, Oxford al the clarendon Press, 1939*

[6] *LEMMI Claudio.: Optica de Fourier,Laboratorio de procesamiento de imágenes, departamento de Fisica-FCEyN-UBA, Argentina.2011*

[7] *MARÉCHAL, A.; CROCE, P. Un filtre de fréquences spatiales pour lamélioration du contraste des images optiques. COMPTES RENDUS HEBDOMADAIRES DES SEANCES DE L ACADEMIE DES SCIENCES, 1953, vol. 237, no 12, p. 607-609.*

[8] *OKAN K. Ersoy.: Diffraction, Fourier optics, and imaging, Wiley-Interscience a John Wiley & sons, INC, 2007*

2. CRIPTOLOGÍA

2.1 Historia de la criptografía

Desde el inicio de la humanidad, el hombre ha tenido la necesidad de comunicarse y con el transcurso del tiempo se ha hecho necesario disfrazar la información, permitiendo que solo un grupo reducido reciba la información compartida, sin levantar sospechas.

La criptografía es la ciencia que estudia los procedimientos de transformar la información, haciéndola incomprensible si no se dispone de la clave adecuada para revelarla. Frente a la criptografía, el criptoanálisis intenta abrir el secreto sin disponer de la clave. La historia registra al profeta Daniel como el primer criptoanalista, los *crackers* serian su sucesores en el mundo actual. Es evidente que un buen criptógrafo debe conocer lo mejor posible los métodos usados por los criptoanalistas, para robustecer sus propios sistemás de cifrado. ‘‘El tire y afloje’’ constante a lo largo de los tiempos entre estos dos mundos que integran la criptología ha hecho que los procedimientos o algoritmos de cifrado estén en constante evolución. La disponibilidad de potentes ordenadores, capaces de romper con gran facilidad códigos poco sofisticados, ha obligado al uso de claves más elaboradas y/o complejas para proteger los mensajes de alto valor estratégico.

La escritura no solo separó la prehistoria de la historia, también permitió vislumbrar muchas posibilidades como también se evidenció los peligros que conlleva que su lectura fuera hecha por personas ajenas, motivando lo que luego se conocería como el arte de codificar información. La escritura secreta data de hace 4000 años a.c. en Egipto, posteriormente se tienen

registros de que Mesopotamia, la India y la China fueron las primeras civilizaciones que usaron de alguna manera la encriptación, principalmente para que solo el receptor del mensaje pudiese tener la información, sin que terceros se diesen cuenta, siendo un método muy útil durante las guerras. Los éforos de Esparta usaron la escítala para cifrar, hacia el año 400 a. c, Este fue el primer sistema criptográfico por transposición, el cual consistía en un cilindro al cual se colocaba un papiro en forma de espiral y solo se hacía visible la información colocando la cinta sobre otra escítala de iguales dimensiones que la primera; esta era la única manera que podía recuperarse el mensaje original, además era necesario colocar el papiro exactamente en la misma posición en la que había sido escrito, en este caso el diámetro de la escítala era la clave.

.

A Julio César se le atribuye ser el primer criptógrafo, ya que ideó un sistema de cifrado elemental para comunicarse con Cicerón y otros comandantes de las legiones de Roma. Julio César utilizó un método basado en la sustitución de cada letra por una que ocupa otra posición en el alfabeto, creando así el cifrado que lleva su nombre ‘el método Cesar’; en este la A era sustituida por la D, la B por la E y así sucesivamente.

Escribas egipcios, alrededor de 1900 a.c., sustituían algunos signos jeroglíficos por otros arbitrarios para realzar su historia. Los alfareros de Mesopotamia, alrededor del 1500 a. c., usaban signos cuneiformes con valores silábicos poco frecuentes para ocultar sus técnicas de fabricación de cerámica esmaltada. En el siglo IX d. c. los califatos islámicos iniciarían con el moderno criptoanálisis, a partir del descubrimiento de que cada lengua tiene una frecuencia de aparición de sus letras dando a entender que era una característica propia, es así que bastaba con contar el número de veces que aparecería la letra, número o símbolo en el texto cifrado para saber cuál era la letra cifrada, independientemente de su aparición. Este fue el fracasado

método monoalfabético; posteriormente para subsanar este momento, el método polialfabético hace su aparición hacia el renacimiento con Lione Battista Albertí, inventor del primer dispositivo de cifrado, 'el cifrado de disco', que consistía en dos coronas circulares concéntricas, la inferior llevaba grabado el alfabeto cifrado y era fija, así cada letra del alfabeto real correspondía con otra del alfabeto cifrado pudiéndose cambiar esa correspondencia, al cambiar la corona exterior. Hasta este instante la posibilidad de que este fuera un instrumento de poder en la creación de los estados modernos, apenas se insinuaba.

En la Edad Media, el uso de la escritura codificada se incrementó. En 1518 Johannes Trithemius, escribió el primer libro impreso de criptología. En 1580 François Viete (1540-1603), matemático francés, fue quien introdujo la primera notación algébrica sistematizada. A pesar de ser más conocido como matemático, él también fue uno de los mejores especialistas en cifras de todos los tiempos. En 1586, Blaise de Vigenère publica su Traicté des chiffres, un tratado de 600 páginas sobre criptología. En él se discute el sistema de la "auto-llave corriente", usada en algunas máquinas de cifrado modernas, método llamado "Vigenère tableau". María Estuardo de Escocia perdió literalmente su cabeza cuando en 1587 fueron interceptadas y descifradas, por el fundador del servicio secreto británico, unas cartas secretas suyas alentando una conspiración para acabar con Isabel de Inglaterra. A finales del siglo XVI Francia comienza a consolidar su liderazgo en el criptoanálisis. En 1671 Gottfried Wilhelm von Leibniz (1646-1716), filósofo y matemático alemán, inventó el cálculo diferencial e integral (independientemente de Sir Isaac Newton), la máquina de calcular y describió minuciosamente el sistema binario. Su máquina de calcular usaba escala binaria. Esta escala, obviamente más elaborada, es utilizada hasta hoy y es la base del código ASCII. En 1840 Samuel Morse (1791-1872) desarrolló el código que recibió su nombre, que consistía en un alfabeto

cifrado en sonidos cortos y largos. Morse también fue el inventor de un dispositivo que llamó telégrafo, en 1844. La invención del telégrafo alteró profundamente la criptografía y hizo del cifrado una necesidad absoluta. Mejoras significativas a la cifra de Vigenère, avances en los sistemas de encriptación, la aparición de la radio revolucionaron las comunicaciones y obligó a la criptografía a desarrollarse como ciencia. Después de la segunda guerra mundial se producen los avances teóricos más significativos de la historia de la criptografía

La rotura del código de la máquina alemana Enigma para cifrar desafió a las mentes más brillantes de entre los aliados, como Alan Turing. Hoy la civilización reposa en la seguridad de que muchos mensajes, con información muy valiosa, puede ser cifrados de modo tal que solo los que disponen de la clave adecuada pueden descifrarlos y conocer su contenido original[2].

Sin duda alguna, la encriptación ha jugado un papel muy importante en la consolidación de los estados y gobiernos actuales.

2.2 La era actual

Actualmente, la criptografía está muy presente en nuestro diario vivir, así acciones tan cotidianas como hacer y recibir una llamada en nuestros teléfonos móviles, transacciones bancarias, realizar compras por internet, las redes sociales; son algunas acciones que nos muestran la dependencia que tenemos con las tecnologías digitales y su avance. Es necesario tener cautela con la información transmitida y se hace necesario ‘disfrazar’ lo compartido. En este punto es donde se requieren el uso de claves o llaves, sin las cuales se hace imposible recuperar la información. Se han desarrollado sistemas más seguros que la trasposición y la sustitución, como

el Data Encriptation Standart o DES, que es un criptosistema de clave privada que en su momento reto a grandes criptoanalistas, finalizando en su quebrantamiento. Diffie y Hellman propusieron utilizar criptosistemás cuyo criptoanálisis fuese equivalente a la resolución de un problema computacionalmente muy difícil [5]. De esta manera, a pesar de conocer los algoritmos que generan el texto cifrado, no es posible recuperar el mensaje en un tiempo aceptable, prolongando su hallazgo. Este es el principio de los sistemas de clave pública, como en 1978 con el RSA. Philip Zimmermann en 1991, desarrolló un sistema criptográfico, aparentemente inviolable, el Pretty Good Privacy por sus siglas P.G.P, y lo distribuyó libremente en las redes de comunicación. Actualmente, es uno de los más utilizados para la protección de los correos electrónicos. Sin embargo, permanentemente hay usuarios no autorizados que buscan interceptar desde un acceso remoto, y decodificar los datos de la red. Esto ha producido en los últimos años un creciente interés en desarrollar sistemas de codificación que involucren nuevos algoritmos y mejorar la seguridad de los existentes. En estos momentos, se pretende que los sistemas criptográficos sean, rápidos, seguros y sencillos de implementar. A esto se le suma la exigencia en hacer que las velocidades de transmisión de grandes volúmenes de datos sean más eficientes, siendo necesario un incremento en la capacidad de almacenamiento y de procesamiento de los dispositivos actuales.

El reciente avance de las comunicaciones a nivel digital, así como el procesamiento óptico de datos establecen sistemas eficaces para la transmisión de datos. Por tanto, las tecnologías ópticas se convierten en una muy buena alternativa, ya que las velocidades de transmisión de importantes volúmenes de información son superiores a las manejadas electrónicamente, los sistemas son robustos y la información puede ser codificada usando cualquiera de los grados de libertad que ofrece la óptica, como por ejemplo la fase, la longitud de onda, la polarización etc.

Estas técnicas ópticas de seguridad transforman los datos en una distribución de ruido blanco estacionario. Una distribución aleatoria es muy difícil de duplicar y su propagación o transformada de Fourier dan como resultado una distribución de speckle. Estas distribuciones luminosas tienen la propiedad de ser portadores aleatorios de información. M. Françon en el año 1975 propuso utilizar sistemas ópticos para codificar, sugiriendo codificar un mensaje usando los cambios aleatorios de fase producidos por un difusor, y para extraer el mensaje es absolutamente necesario poseer la información del difusor, la cual actúa como llave. Se les debe el término 'encriptación' para referirse a la codificación de datos, a O. Kafri y E. Keren en 1987, quienes formularon la idea de codificar información usando esas distribuciones aleatorias.

En 1964 Vander Lugt, propone una arquitectura de correlación óptica, el correlador 4f, que se basa en el uso de un filtro complejo adaptado. En 1995, P. Refregier y B. Javidi [3] introducen por primera vez un sistema de encriptación óptica basado en la arquitectura 4f. Este arreglo permitió trasformar los datos de entrada en ruido blanco estacionario, mediante el uso de dos máscaras de fase aleatorias. Por esta razón se le llama, a esta configuración, arquitectura de doble máscara de fase aleatoria (*Double Random Phase Encoding*, conocida como DRPE). Las máscaras deben ser estadísticamente independientes, una en el plano de entrada, unida a los datos a encriptar y la otra, la máscara llave, se ubica en el plano de frecuencias. En esta primera versión, en el proceso de desencriptación, la información original se recupera a partir de los datos encriptados y del complejo conjugado de la máscara llave, cuando los datos de entrada son de amplitud [1]. En el caso que los datos de entrada sean en fase pura se necesitan el complejo conjugado de las dos máscaras.

Un año después, B. Javidi, G. Zhang y J. Li[4] implementaron experimentalmente el proceso de encriptación-desencriptación con la arquitectura DRPE usando como medio de registro una placa holográfica y máscaras aleatorias generadas empleando moduladores de fase. En 1997, B. Javidi, G. Zhang y J. Li extendieron la propuesta anterior al almacenamiento múltiple de datos encriptados. En ese trabajo se almacenaron en una única placa holográfica dos imágenes encriptadas empleando máscaras llaves estadísticamente independientes. En 1998, G. Unnikrishnan, J. Joseph y K. Singh implementaron la técnica usando un cristal fotorrefractivo como medio de almacenamiento. Mediante el mezclado de cuatro ondas dentro del cristal se genera el complejo conjugado de los datos encriptados. Con esta nueva variante no se requiere emplear el complejo conjugado de la máscara llave para decodificar los datos, es decir se usan las mismas máscaras empleadas que en la etapa de encriptación. Este cambio facilitó la implementación experimental del método de doble máscara de fase aleatoria DRPE. A partir de ese momento se desarrollaron muchas investigaciones encaminadas a analizar el desempeño del método y sus debilidades antes los ataques. Este sistema presenta una alta sensibilidad a los problemas de alineamiento del sistema óptico, por otra parte, los datos encriptados son de amplitud compleja, es decir contienen información tanto de amplitud como de fase, requiriendo el empleo de alguna técnica holográfica y un medio de registro apropiado para su almacenamiento. También es necesario utilizar en la etapa de desencriptación, el complejo conjugado de los datos encriptados ó de las máscaras usadas como llaves.

Las investigaciones en la línea de la encriptación óptica están encaminadas a encontrar la manera de incrementar la seguridad de los sistemas de transmisión de la información; sin embargo, a pesar de los avances en el tema, es estrecha la relación con las comunicaciones; hasta que se originó

con el desarrollo de dispositivos optoelectrónicos, redes ópticas y otras aplicaciones opto-digitales que han permitido mejorar e incursionar en los sistemas híbridos. Por otro lado, una alternativa interesante, que mejora significativamente la seguridad, es el almacenamiento múltiple de datos encriptados (multiplexado) en un único medio de registro. Los primeros trabajos en esta línea fueron por, O. Matoba y B. Javidi[4], donde aprovecharon la selectividad angular de los medios de volumen, para almacenar múltiples datos encriptados. Luego, Ching- Cherng Sun et al. Implementaron un proceso de múltiple almacenamiento de información encriptada que combina el multiplexado angular y desplazamientos laterales del difusor. Estos trabajos pioneros llevaron a indagar el empleo de diferentes parámetros ópticos para multiplexar datos encriptados. Es de destacar que, aunque los primeros trabajos realizados usaban medios de volumen para el registro, también se hacía posible almacenar múltiples datos encriptados en un medio plano. Cuando se recupera la información de un canal en un proceso de multiplexado, a la información desencriptada se le superpone ruido correspondiente a los objetos de entrada que no son correctamente desencriptados. Naturalmente, el ruido en los datos recuperados aumenta cuando se incrementa la cantidad de canales. Este hecho limita la cantidad de datos encriptados que pueden ser multiplexados en un medio para un sistema dado. Esta es una de las razones de la resistencia frente a los ataques, ya que es muy difícil determinar, a partir del patrón encriptado multiplexado, el número de objetos codificados. Esto se debe a la naturaleza de la información encriptada, dándole ruido al ruido blanco aleatorio que da como resultado un nuevo patrón de ruido blanco, donde las distribuciones encriptadas individuales asociadas a cada canal son indistinguibles.

La manipulación de elementos estáticos da una primera idea para manipular secuencias dinámicas, y garantizar que la transmisión por medios digitales mantenga su grado de confidencialidad. Este es el objetivo principal de la

encriptación óptica, garantizar una alta confiabilidad en la transmisión de datos.

Bibliografía

[1] *FRAUEL Yann;CASTRO Alcertina; NAUGHTON Thomás J;JAVIDI Bahram. 'RESISTANCE OF THE DOUBLE RANDOM PHASE ENCRYPTION AGAINST VARIOUS ATTACKS'. Sociedad Americana de óptica. Agosto 6 de 2007 / Vol. 15, No. 16 / OPTICS EXPRESS 10253.* yann@leibniz.iimás.unam.mx

[2] *Galindo T, Alberto, EL ARTE DE DISFRAZAR LA INFORMACION: DE LA C A LA Q, Universidad Complutense, 28040 Madrid, España. Vol 101 N°2 pp307-320 2007.* agt@fis.ucm.es

[3] *Javidi B y Refregier P, 'OPTICAL IMAGE ENCRYPTION BASED ON INPUT PLANE AND FOURIER PLANE RANDOM ENCODING', Universidad de Conecticut Abril 1, 1995 , Vol. 20, No. 7, OPTICS LETTERS pp 767 - 769*

[4] *Javidi B y et al. 'FAULT TOLERANCE PROPERTIES OF A DOUBLE PHASE ENCODING ENCRYPTION TECHNIQUE', Departamento de ingeniería de sistemás y electronica, Storrs, Connecticut 06269-3157, Vol. 36 No. 4, abril1997* bahram@eng2.uconn.edu

[5] *Menezes A. y et al, MANUAL DE CRIPTOGRAFIA APLICADA, 'HANDBOOK OF APPLIED CRYPTOGRAPHY'. CRC press, Inc. Capítulo 1 pp 1-15*

3. ARQUITECTURA 4F Y LA DOBLE MÁSCARA DE FASE ALEATORIA DRPE

Los sistemas coherentes al ser lineales en amplitud compleja, pueden realizar operaciones de la forma

$$I(x,y) = K\left|\iint_{-\infty}^{\infty} g(\xi,\eta)h(x-\xi,y-\eta)d\xi d\eta\right|^2$$

Hay muchas configuraciones diferentes del sistema que pueden ser utilizadas para realizar esta operación. Para lograr realizar una arquitectura que permita llegar a esta operación es necesario tener en cuenta la transformada de Fourier [2].

Una de las propiedades más importantes y útil de una lente convergente es su capacidad inherente para realizar una transformada de Fourier bidimensional o distribución espectral de un campo de entrada, cuando éste se ubica en el plano focal anterior de la lente y se observa en el plano focal posterior. Este tipo de arquitectura es la llamada $2f$. La arquitectura 4f se obtiene mediante el uso de dos sistemas $2f$ contiguos, de tal manera que entre el plano de salida del sistema y el de entrada hay justamente una distancia equivalente a 4 veces la distancia focal f de la lente utilizada. La información del objeto referencia en la arquitectura 4f está contenida en un filtro que se ubica en el plano de Fourier. Estos filtros usualmente contienen información tanto de amplitud como de fase. En 1963 Vander Lugt propone una nueva técnica para sintetizar las máscaras en el plano de frecuencias para los procesadores ópticos coherentes, las máscaras en el plano de frecuencias generadas por esta técnica tienen la importante propiedad que pueden controlar la amplitud y la fase de una función de transferencia a pesar de constar sólo de patrones de absorción. Por medio de esta técnica, fue posible solucionar las limitaciones que tenían los sistemas ópticos

coherentes. El filtro es sintetizado con ayuda de un sistema interferométrico. La técnica decodificación DRPE está basada en la arquitectura 4f [3][4].

En el arreglo se emplean dos máscaras para transformar los datos de entrada en ruido blanco estacionario. Dichas máscaras son funciones complejas de amplitud unitaria y fase aleatoria uniformemente distribuida entre 0 y 1, que a su vez deben ser estadísticamente independientes entre ellas. Una de las máscaras es unida a los datos a encriptar en el plano de entrada de la arquitectura 4f, resultando una redistribución aleatoria de la información en el dominio de frecuencias. La otra máscara (máscara llave o encriptadora) se ubica en el plano de Fourier multiplicando al campo resultante de la primera transformada.[6]

Los desarrollos actuales en la codificación óptica de información plantean el uso de la arquitectura 4f, la cual presenta un arreglo experimental, como el presentado en la figura 3.1

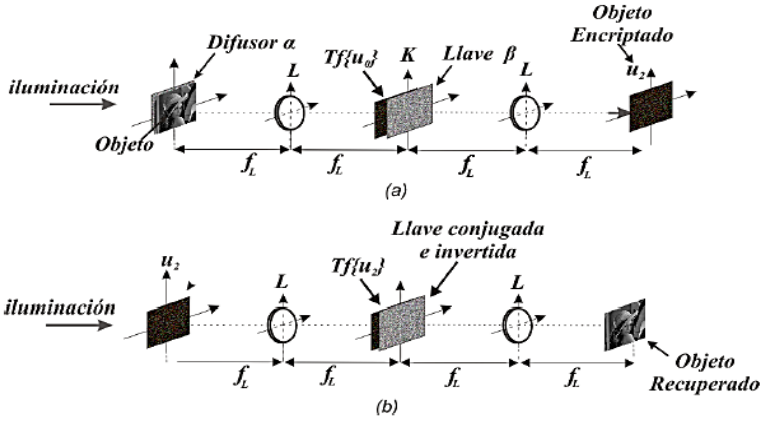


Figura 3.1. Codificación de doble máscara de fase en una arquitectura 4f.

En la figura 3.1 se observa los sistemas de: (a) encriptación y (b) desencriptación. K: plano de Fourier; u_2: objeto encriptado. L: lente de distancia focal f_L; Tf{*}: transformada de Fourier. En el arreglo experimental anteriormente expuesto, la imagen es encriptada usando una doble máscara

de fase aleatoria. La primera máscara de fase es localizada en el plano de entrada junto con el objeto a ser encriptado. Una segunda máscara de fase se ubica en el plano de Fourier de la entrada. Luego, una segunda lente realiza la transformada de Fourier, resultando la información codificada (suele utilizarse como máscara aleatoria de fase pura un difusor). De esta forma el objeto de entrada queda codificado en una distribución estacionaria de ruido blanco. La implementación de este esquema requiere, como se observa en la figura 3.1 (a) de la generación de un haz de fase conjugado. El mezclado de cuatro ondas es un método conveniente para la generación de un haz de fase conjugada. Es justamente la generación de este haz lo que permite la decodificación de la información de entrada sin la necesidad de emplear el conjugado de la máscara llave. Si la llave no es correcta, la imagen original no será reconstruida. Asimismo, si alguno de los parámetros ópticos utilizados para codificar los datos de entrada son modificados, aun empleando en la etapa de desencriptación la misma máscara de fase utilizada en la etapa de encriptación, el objeto de entrada no podrá ser reconstruido. En resumen, es suficiente modificar alguno de los parámetros ópticos de registro para evitar la recuperación de la información. Entre los parámetros, cuya modificación altera la correcta desencriptación, se pueden mencionar, la modificación de la longitud de onda, el estado de polarización, entre otros.

A continuación, se describen brevemente algunas de las técnicas de multiplexado basadas en el empleo de la arquitectura 4f. En la primera técnica los diversos objetos de entrada son codificados modificando, entre exposiciones, la posición de la máscara de fase. En la etapa de desencriptación cada uno de los datos de entrada es recuperado con máxima fidelidad únicamente cuando la posición de la máscara llave coincide exactamente con la que tenía en la etapa de encriptación.

Otra de las técnicas de multiplexado de imágenes encriptadas está basada en el uso de diferentes arreglos de aberturas en la segunda lente de la arquitectura 4f. Aquí las imágenes son codificadas cambiando el arreglo de pupilas entre exposiciones. En este caso, además de las características propias de la máscara de fase, se incorpora al sistema como nuevo grado de seguridad del sistema, la información del arreglo de aberturas. En particular, si la máscara de fase es interceptada, el sistema no podrá ser violado sin el correcto conocimiento de los parámetros geométricos de la pupila del sistema óptico.

Otra técnica para incrementar la seguridad en la transmisión de datos se basa en un multiplexado tipo “rompecabezas”. El principio básico del método se basa en la descomposición de una imagen de entrada, de igual manera que las piezas de un rompecabezas. Cada conjunto de partes de la imagen descompuesta es encriptado en canales separados, pero en el mismo medio de almacenamiento. El uso de canales separados implica modificar alguno de los parámetros del sistema óptico (posición de la máscara de fase, longitud de onda, estado de polarización, etc). Para recuperar la información completa es necesario desencriptar adecuadamente y componer todos los diferentes canales [7]

En este proyecto, la técnica planteada se fundamenta en encriptar la información como ruido blanco por medio de la simulación del uso de una máscara de fase ubicada en el plano de Fourier de la primera lente. Para la desencriptación es necesario utilizar el conjugado de la máscara de fase, simular su ubicación en el plano de Fourier y recuperar la imagen usando la transformada inversa. Este proceso se fundamenta en la teoría de la doble máscara de fase, donde la máscara que afecta la imagen de entrada tiene una función de transmitancia unitaria. En la figura 3.2 se ilustra este proceso.

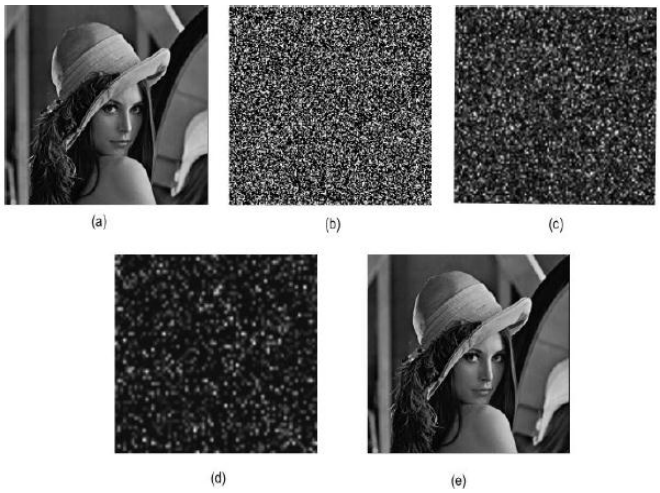


Figura 3.2 (a) Imagen original, (b) llave de seguridad (máscara aleatoria de fase), (c) imagen encriptada, (d) imagen desencriptada cuando se usa una llave distinta a la usada en la encriptación y (e) imagen desencriptada cuando se usa la llave adecuada.

3.1 Modelo teórico

Para encriptar el objeto $f(x_o.y_o)$, que es la información que se ha de encriptar y $\alpha(x_o.y_o) = \exp(i2\pi b(x_o.y_o))$ la máscara de fase del plano de entrada, $b(x_o.y_o)$ es la función aleatoria uniformemente distribuida entre los valores [0,1], el producto entre el objeto a encriptar y la máscara de fase generan el campo en el plano de entrada

$$u_o(x_o.y_o) = f(x_o.y_o)\alpha(x_o.y_o) \tag{3.1}$$

al iluminar con una onda plana y monocromática de amplitud1, en el plano focal de la lente L1 se obtiene la transformada de Fourier óptica del plano de entrada

$$U_1(x_1,y_1) = \frac{1}{i\lambda f_L}\mathrm{F}\left(\frac{x_1}{\lambda f_L},\frac{y_1}{\lambda f_L}\right) \otimes \mathrm{A}\left(\frac{x_1}{\lambda f_L},\frac{y_1}{\lambda f_L}\right)\beta(x_1,y_1) \tag{3.2}$$

$\mathrm{F}(x_1,y_1)$ y $\mathrm{A}(x_1,y_1)$ corresponden a las transformadas de Fourier de $f(x_o.y_o)$ y $\alpha(x_o.y_o)$ respectivamente f_L es la distancia focal de la lente, λ es la longitud de onda del láser usado La transformada de Fourier incide sobre la llave de

seguridad cuya transmitancia es $\beta(x_1, y_1) = \exp[i2\pi b(x_1, y_1)]$, con $b(x_1, y_1)$ aleatoria y distribuida en el rango [0,1]. Luego la segunda lente permite llevar a cabo una segunda transformada de Fourier, la inversa en este caso, así que en el plano de salida del sistema de arquitectura 4f se obtiene la imagen encriptada

$$U_2(x_2, y_2) = \frac{e^{i\pi}}{(\lambda f_L)^2} f(-x_2, -y_2)\alpha(-x_2, -y_2) \otimes \mathrm{B}\left(\frac{x_2}{\lambda f_L}, \frac{y_2}{\lambda f_L}\right) \qquad (3.3)$$

La ecuación (3.3) representa la imagen encriptada, nótese que la encriptación está dada por el producto convolutivo entre el plano de entrada en el momento de encriptar y la función aleatoria $\mathrm{B}\left(\frac{x_2}{\lambda f_L}, \frac{y_2}{\lambda f_L}\right)$

Para visualizar la transformada de Fourier de una señal, se hace uso del espectro de magnitud [1], definido como

$$F(u, v) = \sqrt{(real(F(u, v)))^2 + (imag(F(u, v)))^2} \qquad (3.4)$$

Para obtener la desencriptación se ubica la imagen encriptada en el plano de entrada de un sistema 4f (figura 3.1 b), se ilumina con un haz monocromático colimado y se realiza la transformada de Fourier con la lente *L*, obteniéndose en el plano *K* una distribución de campo de la forma

$$U_3(x_3, y_3) = \frac{e^{i\pi}}{i(\lambda f_L)}\left[f\left(-\frac{x_3}{\lambda f_L}, -\frac{y_3}{\lambda f_L}\right) \otimes \mathrm{A}\left(-\frac{x_3}{\lambda f_L}, -\frac{y_3}{\lambda f_L}\right)\right]\beta(-x_3, -y_3) \qquad (3.5)$$

Obteniendo el complejo conjugado de la máscara invertida $\beta(x_3, y_3)$ y multiplicando $u_3(x_3, y_3)$ por ese complejo $\beta^*(-x_3, -y_3) = e^{-i2\pi h(-x_3, -y_3)}$ y realizando una segunda transformada de Fourier, en el plano de desencriptación se obtiene el campo de entrada o imagen desencriptada, así:

$$u_4(x_4.y_4) = f(x_4.y_4)\alpha(x_4.y_4) \qquad (3.6)$$

Si se multiplica $u_3(x_3, y_3)$ por una máscara de fase distinta $\gamma(x_3, y_3)$ con transformada de Fourier $D(x_4, y_4)$ se obtiene

$$u_4(x_4, y_4) = f(x_4, y_4)\alpha(x_4, y_4) \otimes \mathrm{B}(x_4, y_4) \otimes D(x_4, y_4) \quad (3.7)$$

Que no corresponde a la información de entrada.

3.2 Modelo algorítmico

El diagrama de flujo que se utilizó como referencia para este trabajo consta de tres pasos [5]:

Paso 1: A la imagen $f(x.y)$ se multiplica por una función de fase aleatoria $\mathrm{R}(x.y) = exp(i\phi(x, y))$, esto es $f(x, y) \cdot R(x, y)$, que es una distribución aleatoria de fase con valores uniformemente distribuidos en el rango $-\pi$ a π.

Paso 2: el espectro resultante de la transformada de Fourier del producto anterior se multiplica por otra función de fase aleatoria que es la llave del proceso de encriptación, expresada como $S(u, v) = \exp(i\varphi(u, v))$.

Paso 3: se calcula la transformada de Fourier inversa

$$f_c(x', y') = F^{-1}\{F[f(x, y) \cdot R(x, y)] \cdot S(x, y)\} = [f(x', y') \cdot R(x', y')] * S(x', y') \quad (3.8)$$

$f_c(x', y')$= señal que lleva oculta la imagen encriptada f(x,y). Las funciones R(x,y) y S(u,v) convierten a la imagen f(x,y) en ruido blanco

Para desencriptar la imagen

Paso 1: se calcula la transformada de Fourier del conjugado de la señal encriptada $\{f_c(x', y')\}^*$, más exactamente

$$F[\{f_c(x', y')\}^*] = F\{[f^*(x', y') \cdot R^*(x', y')] * S^*(x', y')\} = F[f^*(x', y') \cdot R^*(x', y')] \cdot F[S^*(x', y')] \quad (3.9)$$

Paso 2. Multiplicación de la ecuación (3.9) por la llave $S(u,v)$ utilizada en el proceso de encriptación

$$F[f^*(x',y')\cdot R^*(x',y')]\cdot F[S^*(x',y')]\cdot S(u,v) \qquad (3.10)$$

Paso 3. Se calcula la transformada inversa al producto de la ecuación (3.10)

$$f_d(x¨,y¨)=F^{-1}\{F[f^*(x',y')\cdot R^*(x',y')]\cdot F[S^*(x',y')]\cdot S(u,v)\}=[f(x¨,y¨)\cdot R^*(x¨,y¨)]*[S^*(x¨,y¨)\otimes S(x¨,y¨)] \qquad (3.11)$$

$\otimes$ Es el producto de correlación. $f^*(x¨,y¨)$ es una función real, entonces $f^*(x¨,y¨)=f(x¨,y¨)$. Este es la recuperación de la señal $f(x¨,y¨)$, siempre que el factor de fase $R^*(x¨,y¨)$ desaparece en el momento de la detección, Ya que se registra en un detector de intensidad, la distribución .Se obtiene

$$f_d(x¨,y¨)=[f(x¨,y¨)\cdot R^*(x¨,y¨)]*\left[S^*(x¨,y¨)\otimes \tilde{S}(x¨,y¨)\right] \qquad (3.12)$$

Obteniéndose la imagen original.

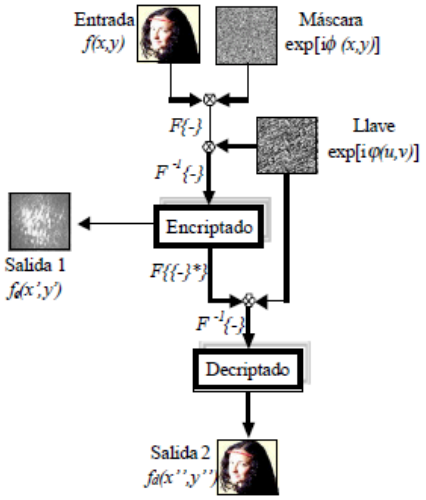


Figura 3.3 [5] Flujograma de encriptación-desencriptación mediante la transformada de Fourier. {-}*: Complejo conjugado; F{-}: transformada de Fourier; F-1{-}: transformación de Fourier Inversa; Ä: multiplicación

3.3 Implementación digital

El algoritmo propuesto por (Rueda y et al, 2005)[5], fue implementado en la plataforma Qt con librerías de Opencv, en un computador lenovo licenciado a Windows 7 home Premium, service pack 1; procesador Intel(R) core(TM) i7-3610QM CPU@2.30GHz; memoria RAM 6.00Gb, sistema operativo de 64bits, Qt con Opencv 2.3

Para el proceso de encriptación no se utilizó una máscara de fase aleatoria inicial, es decir, se asumió que esta máscara de fase tenía una función unitaria de trasmitancia, por lo que no alteraba la imagen. Esto con el fin de reducir el tiempo de cómputo del proceso.
Se seleccionó una imagen a encriptar, que se encontraba en un formato cualquiera, se convirtió a escala de grises (0 a 255) y se procedió a hallarle la transformada de Fourier 2D, con la cual se realizó la encriptación. Se generó una máscara de fase aleatoria, la cual debía tener el mismo tamaño de la imagen a encriptar, se almacenó para usarla posteriormente como llave y se le halló la transformada de Fourier, para luego ser multiplicada punto a punto (convolución) con la transformada de Fourier de la imagen a encriptar. Al resultado se le aplicó la transformada inversa de Fourier. Los valores obtenidos se sometieron a un proceso de normalización para efectos de visualización. Después de haber realizado todos estos pasos se ha obtenido la imagen encriptada.

Para obtener la imagen desencriptada se toma la imagen encriptada y su máscara de fase correspondiente, se conjuga la máscara para obtener la llave, luego, se halla la transformada de Fourier de ambas y se multiplican punto a punto (convolución), a este resultado se le halla la transformada inversa de Fourier y se obtiene la imagen original, procediéndose luego a

realizarle un proceso de normalización para así obtener una imagen digital que puede ser visualizada.

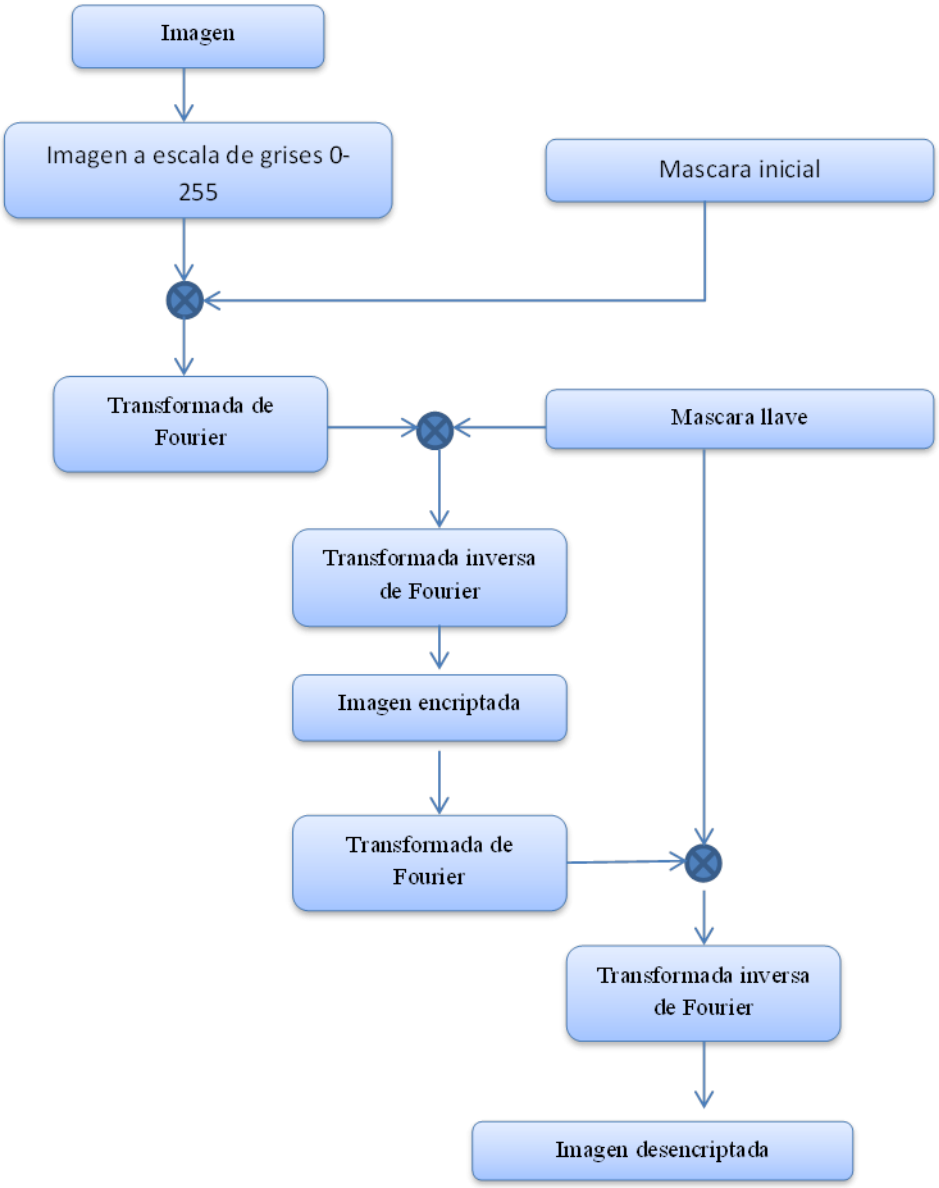


Figura 3.4 Esquema resumen del algoritmo

En los sistemas clásicos de encriptación, la máscara de fase aleatoria y la máscara llave son difusores. Estos difusores pueden ser considerados como

un arreglo de pequeños centros dispersores con distribuciones aleatorias de fase, posición y forma. Idealmente un difusor sería un arreglo de fuentes puntuales (pequeñas dimensiones) con fases iniciales estadísticamente independientes una de la otra. La llave es generada como un arreglo de MxN pixeles, la representación matemática de este tipo de máscaras de fase equivale a tener la convolución de una función rect (abertura rectangular), con la dimensión de un pixel, con una muestra de funciones aleatorias, donde cada muestra está dada por una función delta de Dirac, la cual ha sido modulada por algún valor de fase aleatorio

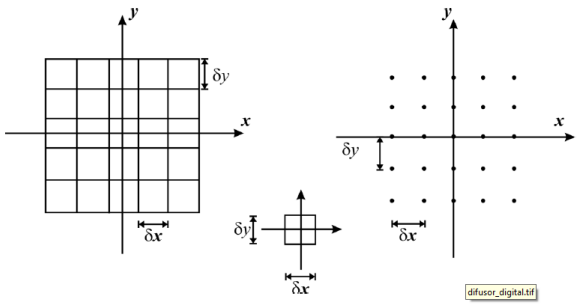


Figura 3.5 Representación del modelo de la llave digital como la convolución de una función rect (área de un pixel) con un arreglo periódico bidimensional de valores de fases aleatorias.

En el proceso, las máscaras de fase aleatorias estadísticamente independientes sirven como llaves para la arquitectura[4], de esta manera, el sistema encripta la imagen a un ruido blanco, pero no cifrado así que se hace necesario realizar la convolución entre las transformadas para que ese ruido blanco sea estacionario, como se observa $f_c(x', y')$ en la figura 4.1. Para el proceso de desencriptación se utiliza la técnica de conjugación de fase para descifrar la imagen, es necesario utilizar las mismas máscaras de fase tal como se utiliza durante la encriptación para decodificar los datos con éxito.

Bibliografía

[1] *FORERO V. Manuel y et al. ‘‘ESTUDIO DEL EFECTO DE LAS MÁSCARAS DE CONVOLUCIÓN EN IMÁGENES MEDIANTE EL USO DE LA TRANSFORMADA DE FOURIER’’ Revista Ingeniería e Investigación No. 48 Diciembre de 2001*

[2] *GOODMAN Joseph W.: Introduction to Fourier Optics. Vol II. McGraw-Hill book Company, 1996*, pp 171- 177

[3] *JAVIDI B y Refregier P,’‘OPTICAL IMAGE ENCRYPTION BASED ON INPUT PLANEAND FOURIER PLANE RANDOM ENCODING’’, Universidad de Conecticut Abril 1, 1995 , Vol. 20, No. 7, OPTICS LETTERS pp 767 - 769*

[4] *JAVIDI B y et al. ‘FAULT TOLERANCE PROPERTIES OF A DOUBLE PHASE ENCODING ENCRYPTION TECHNIQUE’, Departamento de ingeniería de sistemás y electronica, Storrs, Connecticut 06269-3157, Vol. 36 No. 4, abril1997 bahram@eng2.uconn.edu*

[5] *RUEDA Jorge E; ROMERO Ana L; CASTRO Lina M, ‘CRIPTOGRAFIA DIGITAL BASADA EN TECNOLOGIA OPTICA’. Bistua: Revista de la facultad de Ciencias Básicas, Julio, año. vol. 3, número 002. Universidad de Pamplona. Bucaramanga, ISSN 0120-4211 Colombia. pp 19-25.*

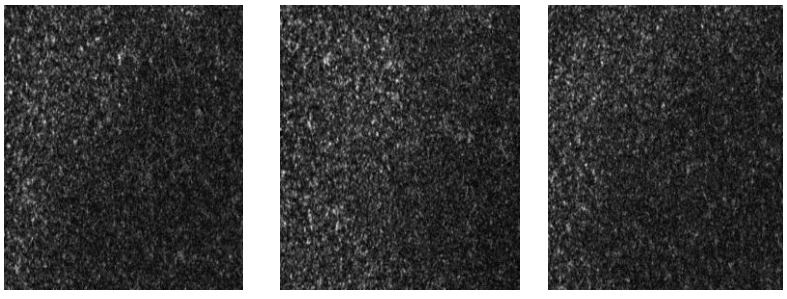
[6] *RÍOS Carlos A., RUEDA Edgar A., BARRERA John F., ‘SISTEMA ÓPTICO DE ENCRIPTACIÓN DE DOBLE MÁSCARA DE FASE BAJO ARQUITECTURA 4F’.Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia. Revista. Tecno Lógicas Segunda Edición Especial, ISSN 0123-7799, Diciembre 2010, pp. 75-96*

[7] *TEBALDI Myriam. 'MÉTODOS ÓPTICOS COMO HERRAMIENTA PARA ENCRIPTAR-DESECRIPTAR INFORMACIÓN'. Revista Bistua Universidad de Pamplona.Pamplona-Colombia*

4. RESULTADOS Y DISCUSIONES

En el capítulo anterior, se estudió el fundamento teórico de la arquitectura 4f y la doble máscara de fase aleatoria [10], junto con la implementación digital, la cual va a ser de interés en este capítulo [11].

Como se afirma en el numeral 3.3, basados en la arquitectura 4f y en el sistema de codificación de doble máscara de fase, se detalla su implementación en un sistema el cual implementa la transformada de Fourier discreta cuyo procedimiento para calcularla rápidamente es la transformada rápida de Fourier (*Fast Fourier Transform FFT*) como herramienta para hacer el análisis computacional. Se hace necesario destacar que, para el proceso de encriptación se usó una máscara *speckle* obtenida experimentalmente (figura 4.1), y una máscara aleatoria obtenida digitalmente, la cual se multiplica por la imagen de entrada. Se procede con una propagación de *Fraunhoufer* (campo lejano) y se tomó la apertura de la lente infinita, tomando en cuenta que la onda al llegar a la lente era casi plana, esto con el fin de minimizar el tiempo de computo; los resultados obtenidos de aplicar la teoría de encriptación óptica con arquitectura 4f y máscara de fase aleatoria a imágenes digitales se detallan a continuación.



Mascara *speckle* 1 Mascara *speckle* 2 Mascara *speckle* 3

Figura 4.1. Mascaras *speckle* generadas en el laboratorio

Inicialmente y para poner a prueba el algoritmo implementado, se somete a prueba imágenes binarias en formato mapa de bits .bmp, de tamaño 320×240 (Figura 4.2 primera fila) y 640×480 (Figura 4.2 segunda fila), con el objetivo de establecer un rango en la resolución de las imágenes del cual partir y realizar las pruebas siguientes. La imagen sometida (Figura 4.2a.) es convolucionada con la máscara aleatoria (Figura 4.2b.) dando por resultado una imagen con ruido blanco la cual, efectivamente ha ocultado la información (figura 4.2c.) la transformada de Fourier de la máscara aleatoria del proceso algorítmico de FFT, cuyas frecuencias bajas se encuentran en el centro y las altas en las esquinas(Figura 4.2d.), es nuevamente utilizada para desencriptar, consiguiendo una imagen nítida, con una pérdida mínima de información y limpia, se aprecia la imagen recuperada con escaso ruido (figura 4.e.). Por tanto el algoritmo propuesto es válido y cumple con el objetivo buscado.

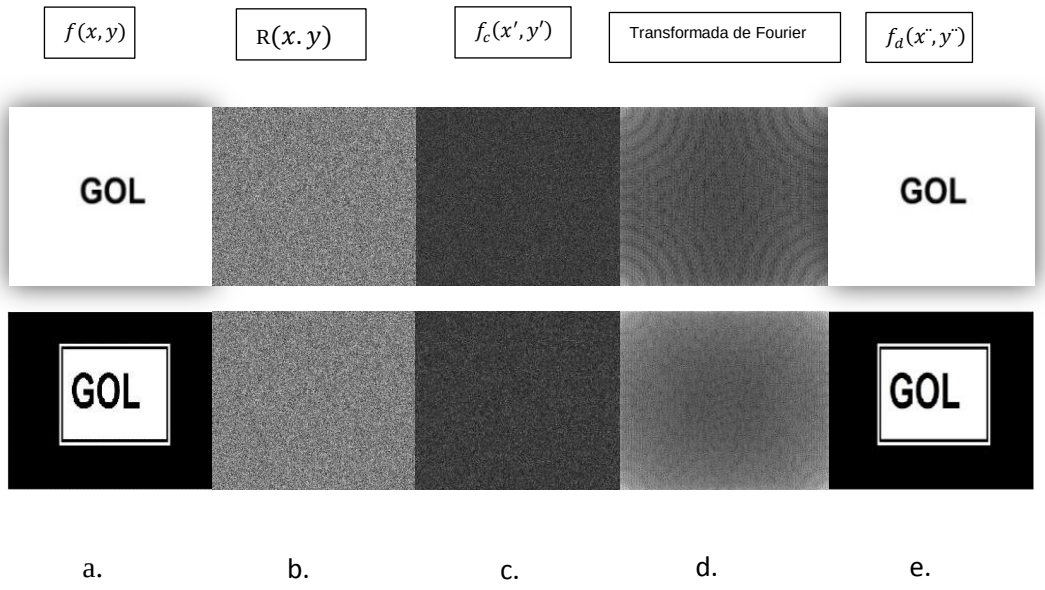


Figura 4.2: proceso de encriptación y desencriptación con máscaras aleatorias. Imagen binaria original $f(x,y)$; R$(x.y)$ Máscara real; $f_c(x',y')$ Intensidad de la imagen encriptada; Transformada de Fourier; $f_d(x'',y'')$ Imagen desencriptada

Las imágenes GOL, al ser binarias, sus valores son 0 para negro y 255 para blanco, que resulta ser el valor máximo. Por lo regular al realizar la transformada óptica de Fourier, las imágenes pueden ser sometidas a un proceso de recuperación donde la imagen recuperada no compensa la inicial, de esta forma resultará la imagen con ruido *speckle* superpuesto [7]. En el caso estudiado, debido a que la recuperación se realiza digitalmente, al desencriptarla se obtiene una réplica muy similar a la imagen original debido al algoritmo de FFT usado. Se observó que la máscara de fase ha de tener igual tamaño que la imagen para obtener un proceso de encriptación y desencriptación exitoso.

La imagen desencriptada es casi idéntica a la imagen original, con el objetivo de analizar qué tanta fidelidad tendrá con la imagen original, se le extrajo la raíz cuadrada del error cuadrático medio (RMSE) y el pico de la relación señal ruido (PSNR) donde O es la imagen original, D es la imagen reconstruida y p es el valor del pixel donde la imagen es máxima, esto con el fin de analizar la calidad de la imagen recuperada.

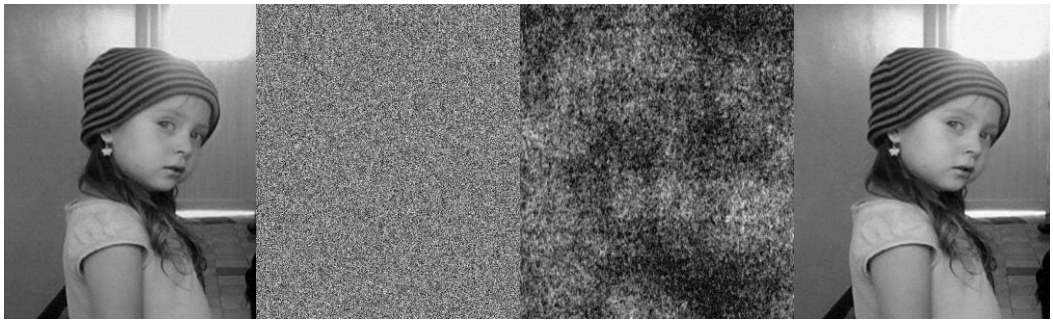
$$RMSE = \frac{1}{256}\sqrt{\frac{1}{nm}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(O_{ij} - D_{ij}\right)^2} \tag{4.1}$$

$$PSNR(O,D) = 10 * \log_{10}\left(\frac{p^2}{\frac{1}{nm}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(O_{ij}-D_{ij}\right)^2}\right) \tag{4.2}$$

Se considera que el PSNR ha de ser mayor a 20dB, para considerar, una imagen resultante de alta calidad y se contempla que un incremento de 20dB es un decrecimiento de la décima parte en la diferencia del RMSE[1]; para las imágenes binarias GOL se tiene (figura 4.2 arriba) el RMSE igual a 0.00251 y su PSNR igual a 51.9; (figura 4.2 abajo) el RMSE es 0.0021 y su PSNR es de 53.6; la calidad que arrojan el PSNR es muy alta mostrando una gran eficacia al recuperar las imágenes binarias de la figura 4.2.

Consecuentemente y siguiendo las pruebas se somete imágenes en formato de compresión de imágenes jpg, la cual es convertida algorítmicamente a escala de grises, iniciando con la resolución mínima acordada en 320×240 pixeles, con 256 niveles de gris, a esta se le aplicó el proceso de encriptación y desencriptación con el algoritmo descrito anteriormente (capitulo 3).

La máscara aleatoria (Figura 4.3b.) y la inicial arrojaron una imagen con ruido blanco como lo plantea en la Ec.3.7 (Figura 4.3c.), la cual satisfactoriamente ocultó la información de la imagen original mostrada en la Figura 4.3a, al realizar el proceso de desencriptación la imagen obtenida fue muy similar a la original, con una pérdida mínima de información y limpia (Figura 4.3d.)



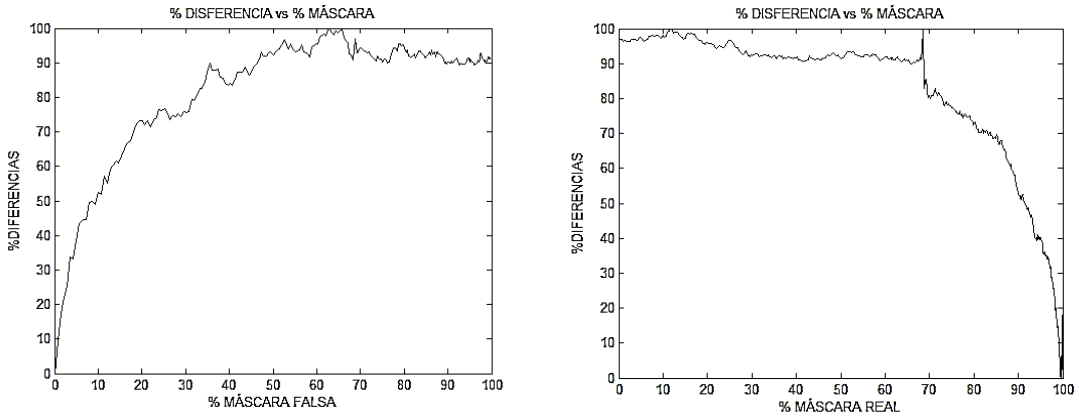
a) b) c) d)

Figura 4.3. Imagen de 320×240 pixeles con 256 niveles de gris a) imagen original en escala de grises, b) máscara llave c) intensidad de la imagen encriptada con mascara aleatoria d) imagen desencriptada. (Se observa un ligero cambio de contraste)

Se somete una imagen de 320×240 pixeles al proceso de encriptación y desencriptación. Buscando establecer estadísticamente un posible descifrado de la información, se graficó el recorrido de las máscaras (figura 4.4a) con el objetivo de cuantificar hasta qué punto la información era visible; posteriormente se observó el comportamiento al desencriptar (figura 4.4b). Se hace evidente que el sistema haría posible una protección que supera la mitad de los pixeles de la imagen. Se puede determinar la información

asociada a la diferencia de fase $\Delta(x,y) = \phi(x,y) - \phi_0$ en el proceso la fase inicial y la fase aleatoria [13]; esta diferencia muestra el proceso de codificación de la información a medida que recorre la imagen este dará una idea de cuanta será la información encriptada (figura 4.4)

Las pruebas mostraron un pico de relación señal ruido PSNR, con un valor de 36dB, demostrando que la imagen reconstruida es muy similar a la original, su RSME es de 0.0122.



a. b.

Figura 4.4 Representación del comportamiento de la diferencia de las máscaras al recorrer la imagen: a. durante la encriptación y b. durante la desencriptación

Al aumentar la resolución de las imágenes y analizarlas en escala de grises. Se analiza una imagen de tamaño 640×480 pixeles, con 256 niveles (256 valores discretos), se observó el mismo comportamiento que la imagen de 320×240 pixeles mostrada en la figura 4.3.

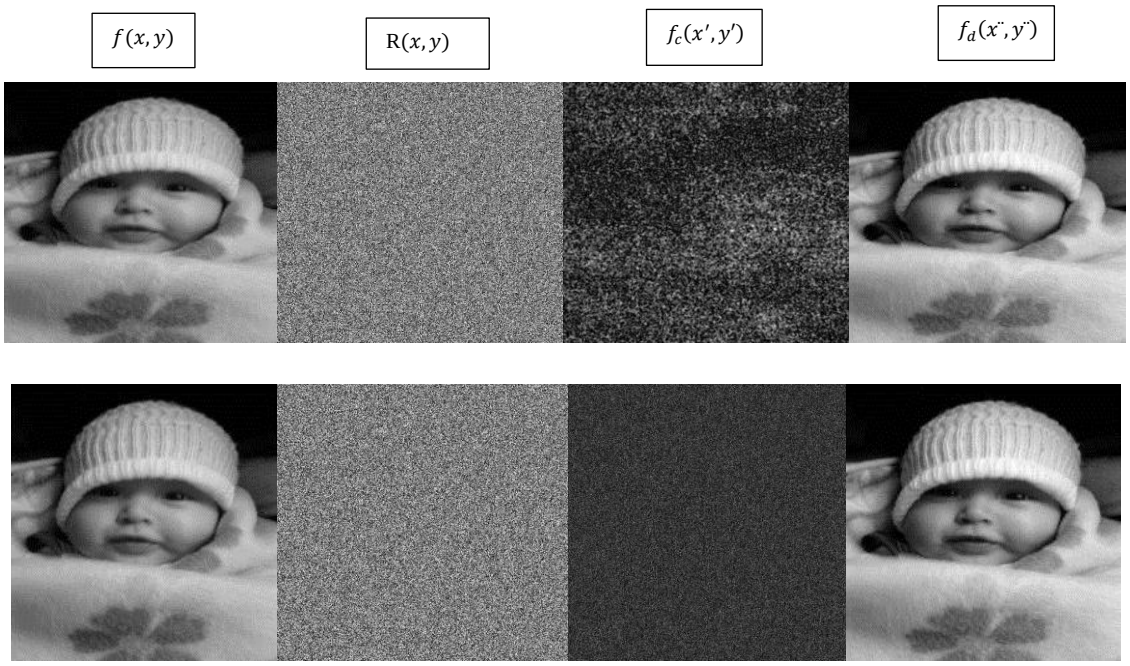
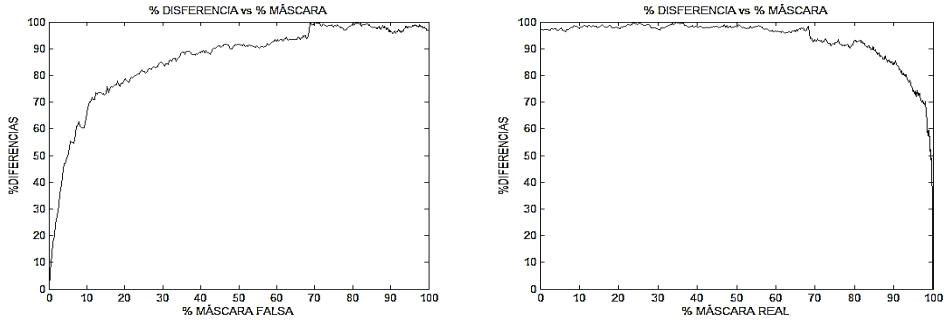


Figura 4.5 (Arriba) Imagen original f(x,y); Mascara aleatoria R(x,y); encriptacion con *speckle* y aleatoria $f_c(x',y')$; Imagen desencriptada $f_d(x'',y'')$; (abajo) imagen original f(x,y); mascara aleatoria R(x,y); imagen encriptada con doble mascara aleatoria $f_c(x',y')$; Imagen desencriptada $f_d(x'',y'')$



a. b.

Figura 4.6 Representación del comportamiento de la diferencia de las máscaras al recorrer la imagen: a. durante la encriptación y b. durante la desencriptación

Si se utiliza para la desencriptación la llave o máscara correcta, se obtendrá la imagen recuperada como lo describe la ecuación (3.11) cuyos niveles de grises tienen una diferencia mínima con respecto a la imagen original dando fiabilidad de la información recuperada. Esta situación no se presenta con la llave incorrecta $\gamma(x_3, y_3)$ la cual responde a la ecuación (3.6) y se observa en la figura 4.7

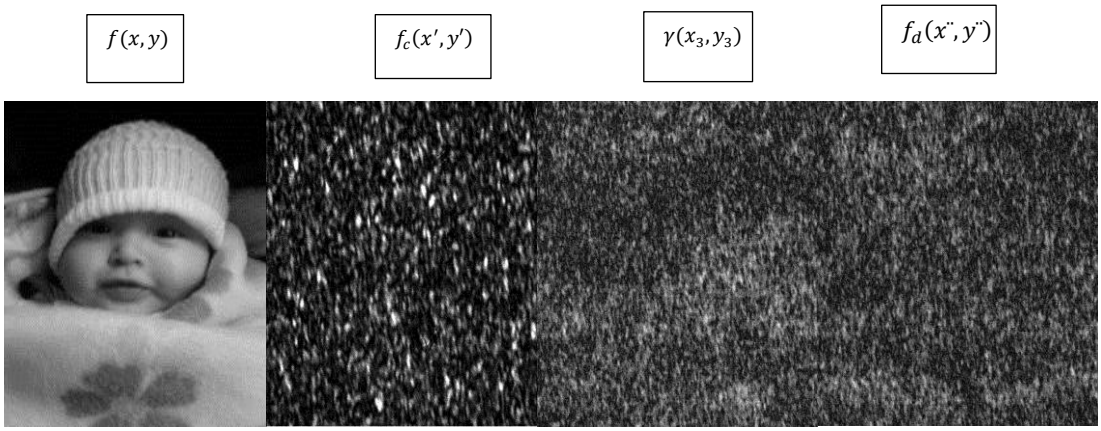


Figura 4.7 Imagen original f(x,y); imagen encriptada $f_c(x', y')$); máscara falsa $\gamma(x_3, y_3)$ Imagen desencriptada con la máscara falsa $f_d(x'', y'')$;

Es de destacar que durante el proceso se hace importante la convolución de las máscaras[5], el proceso de convolución en el cual los bordes y demás cambios bruscos de los niveles de gris están relacionados con las componentes de alta frecuencia, mientras que los factores de iluminación y color tienen que ver con las frecuencias baja (ecuación (3.4)). Al implementar en el algoritmo, la transformada de Fourier esta siempre centrada, la convolución de las dos fases convierten la imagen original en ruido blanco estacionario, se observa que a medida que las máscaras recorren la imagen presentan disminución o pérdida de los detalles correspondientes tanto a frecuencias altas como bajas resultando en una imagen con ruido blanco donde no se puede observar la información, como

se observa en la figura 4.8 donde se aprecian los fotogramas a lo largo del recorrido de las máscaras y la encriptación resultante

El proceso de desencriptación se hace reversible ya que se conoce la máscara de fase de información compleja. En el proceso de reconstrucción de la imagen, el uso de la fase conjugada y el uso de la transformada inversa, lo convierte en un sistema robusto que lo hace altamente seguro a varios ataques cuyo objetivo es la información contenida en la imagen original [3].

La calidad de la imagen restaurada con ayuda de la ecuación 4.1 que indica su RMSE, da un valor de 0.01375 y con la ecuación 4.2 el valor del PSNR fue de 36dB; la imagen estudiada tiene un valor pico muy superior a 20dB y se confirma que la imagen recuperada tiene una alta calidad demostrándose en el último fotograma de la figura 4.9.

Los fotogramas que se muestran a continuación (Figura 4.8 y Figura 4.9) demuestran que los procesos de encriptación y desencriptación son totalmente reversibles, siempre y cuando se tenga en cuenta que las máscaras han de tener igual tamaño a la imagen original.

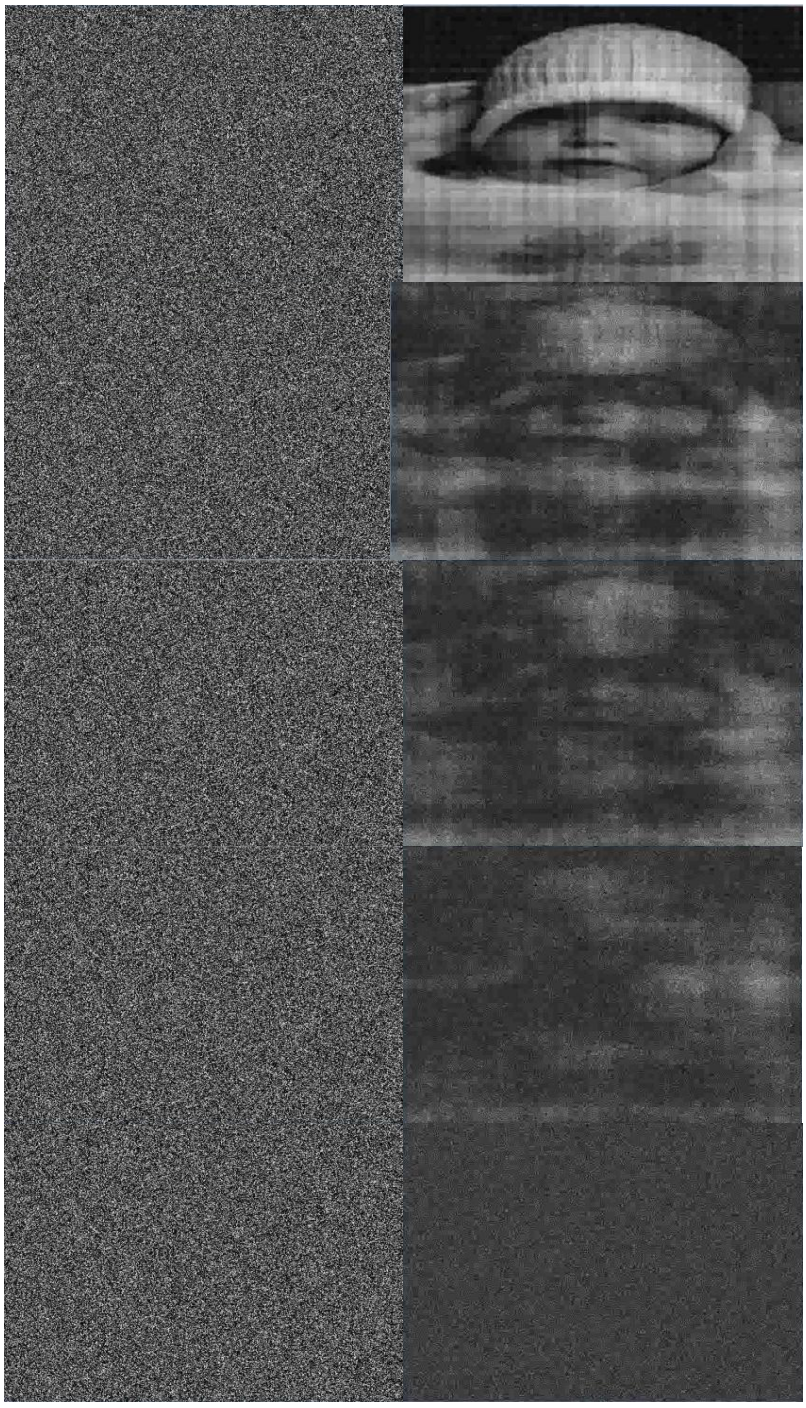


Figura 4.8 fotogramas del proceso de encriptación

De acuerdo con el algoritmo de desencriptación paso 3 para obtener la imagen desencriptada se usa la ecuación (3.11)

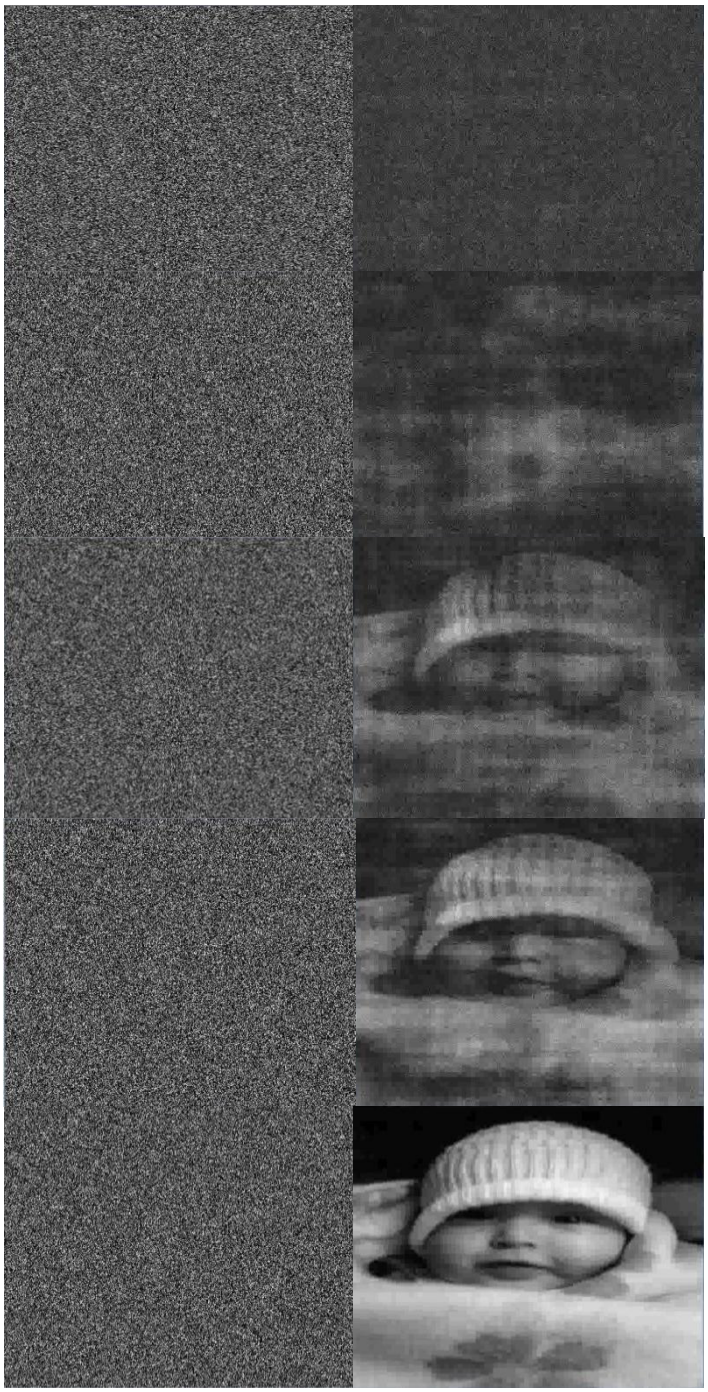
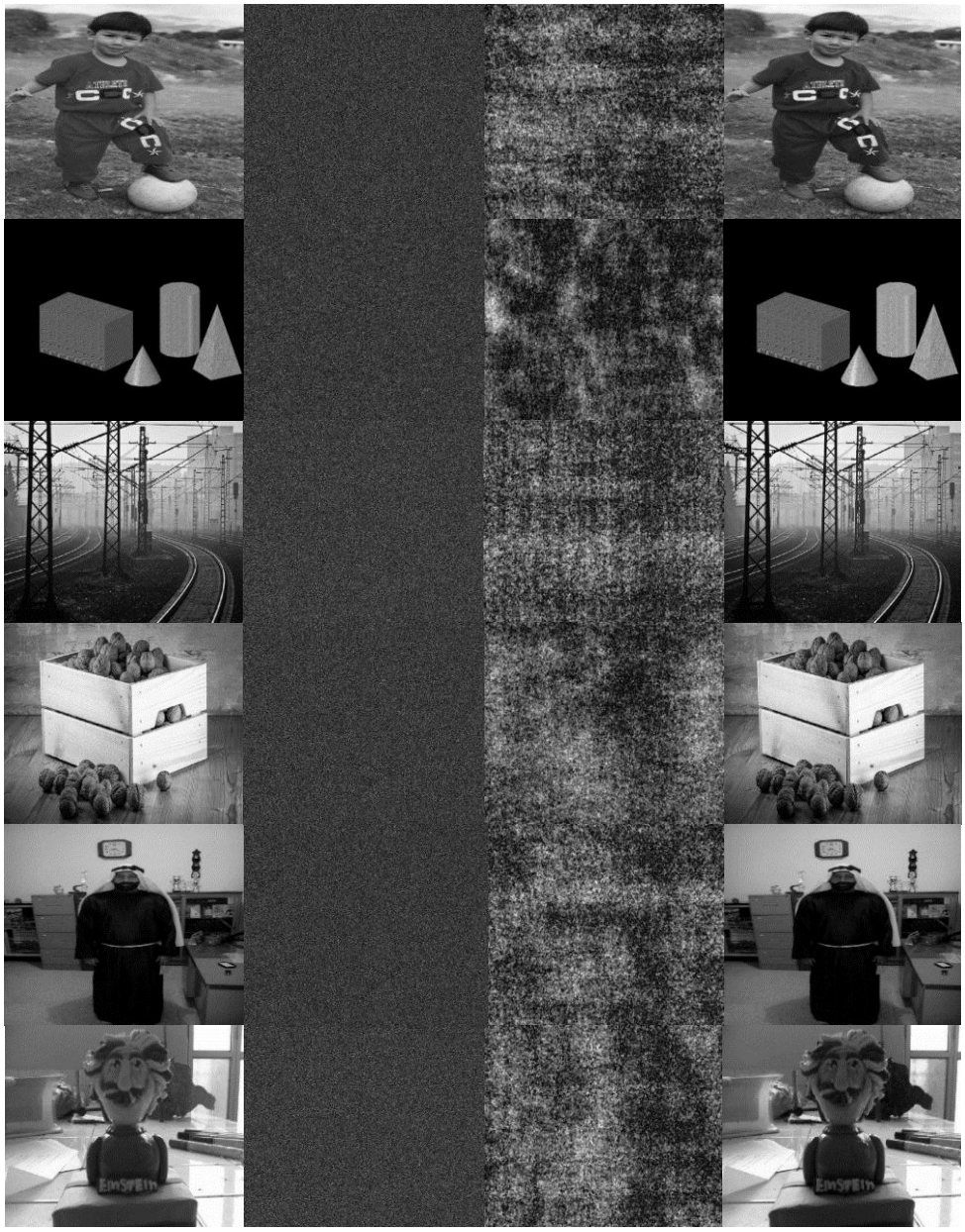


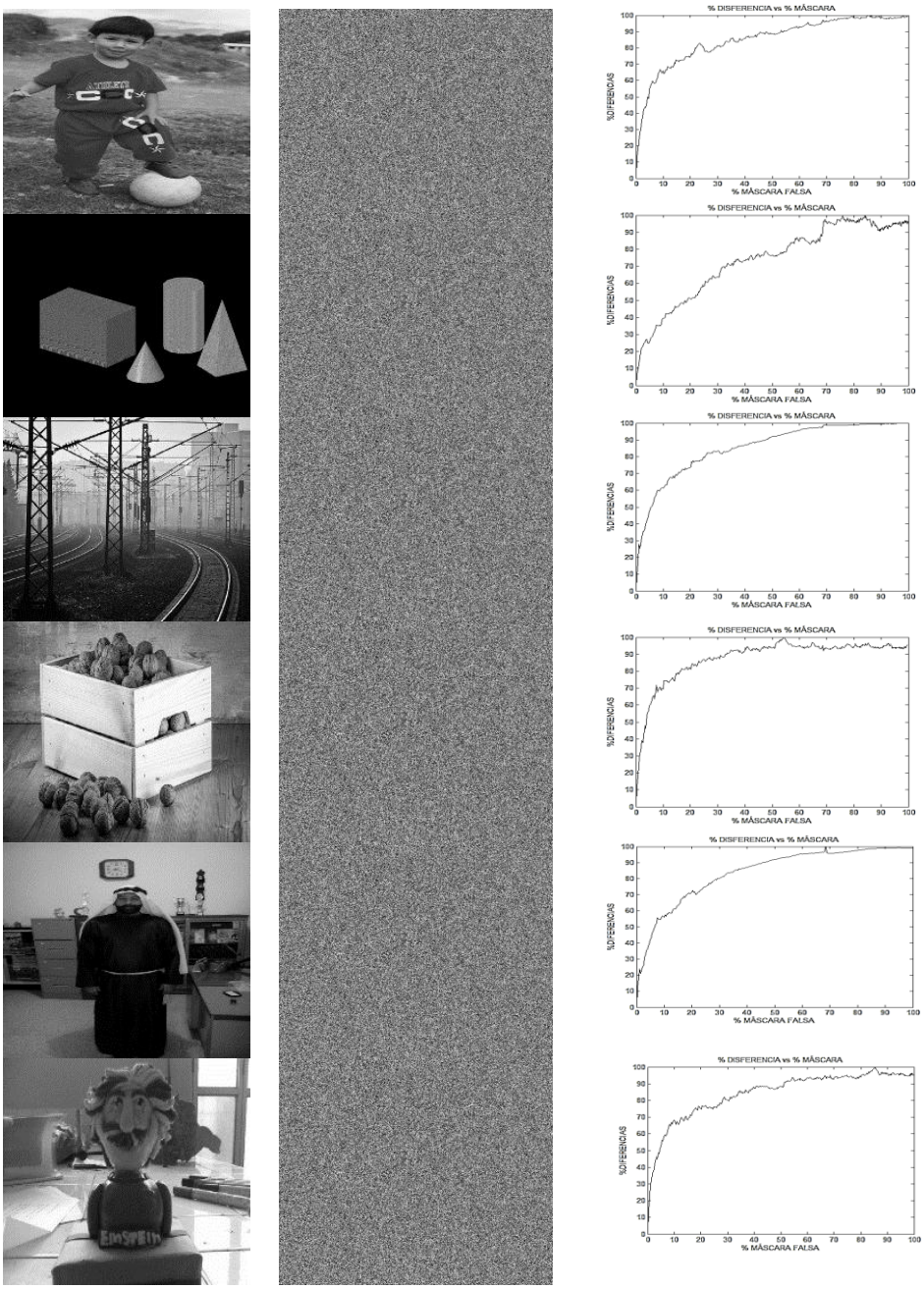
Figura 4.9 Fotogramas que describen el proceso de desencriptación

Con la finalidad de analizar el proceso se sometió varias imágenes, analizando la diferencia entre la imagen original y la recuperada.



a b c d

Figura 4.10 Proceso de encriptación-desencriptación de 6 imágenes de 640×480 pixeles, con 256 valores discretos. a) Imagen en escala de gris original; b) encriptada con máscaras aleatorias c) Intensidad de la imagen encriptada con *speckle y aleatoria*; d) imagen desencriptada.



a b) c).

Figura 4.11. Comparación de la gráfica de diferencias en las distintas imágenes; a).Imagen en escala de grises; b). Llave aleatoria; c).Grafica de diferencias entre la fase real y la fase modificada

De la misma manera anterior se procedió a realizar la desencriptación

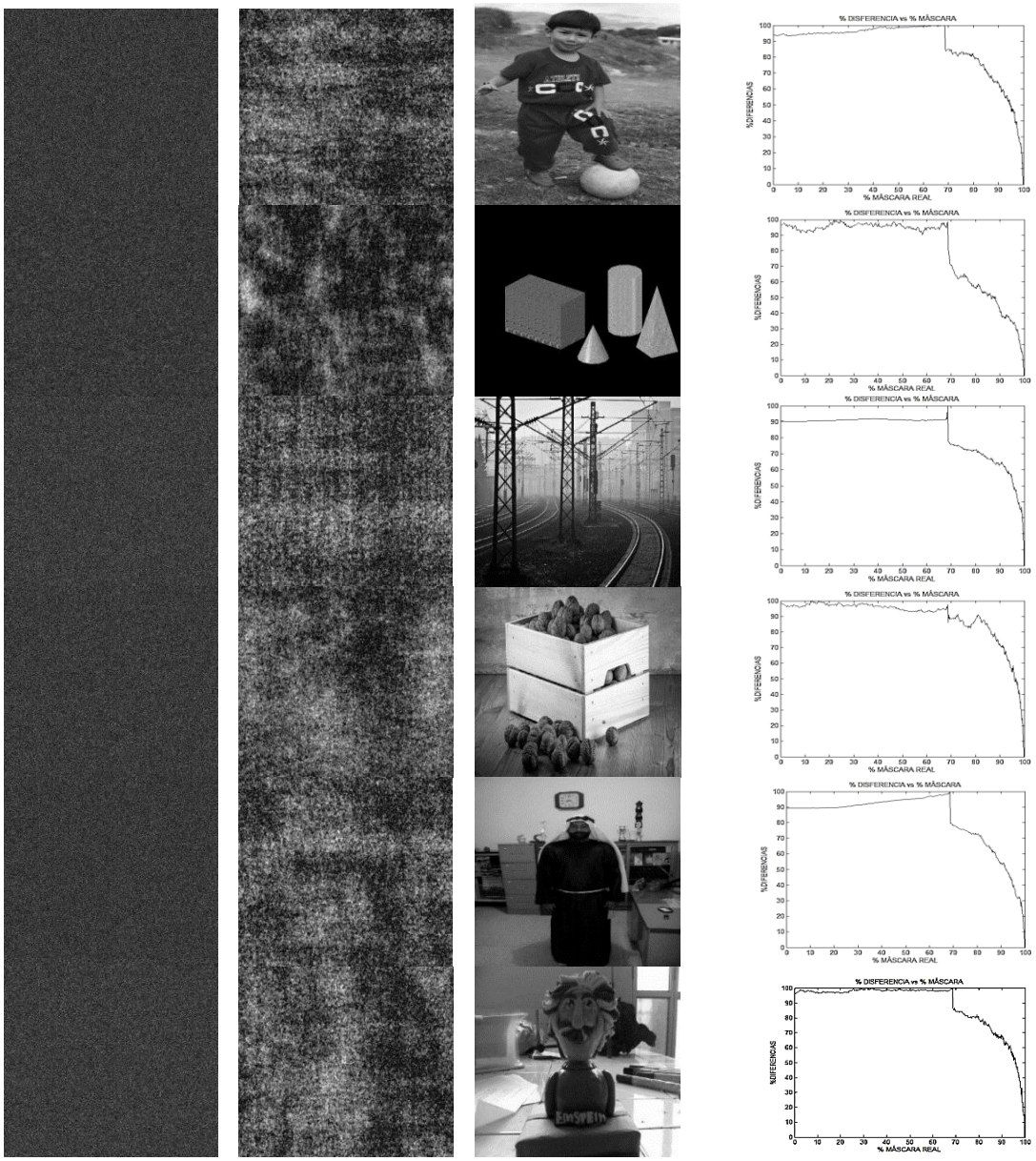


Figura 4.12 Comparación de la gráfica de diferencias en las distintas imágenes; a) imagen encriptación con aleatorias; b). Imagen encriptada con *speckle* y aleatoria c) imagen desencriptada; d).Grafica de diferencias entre la fase real y la fase modificada durante la desencriptación

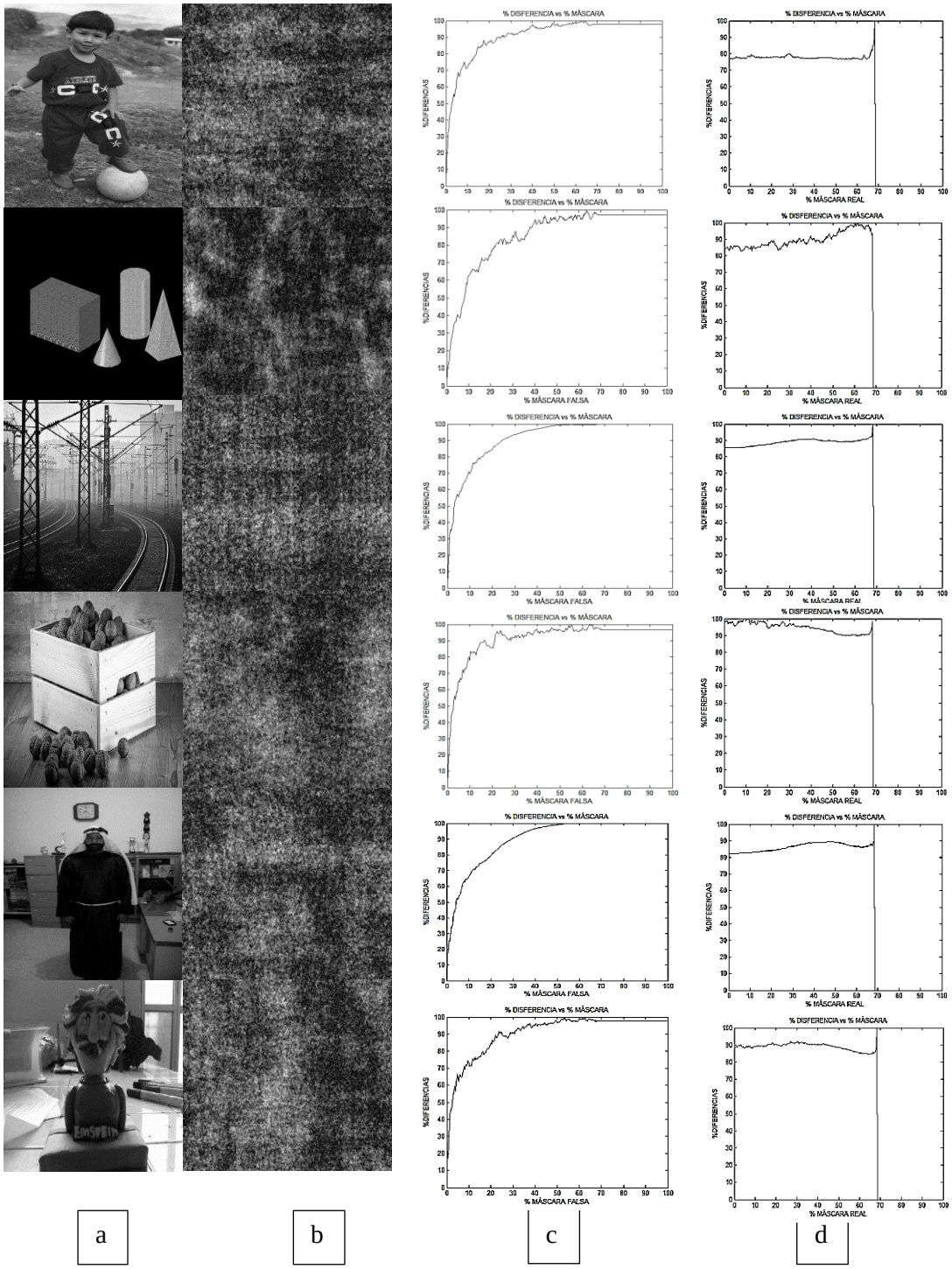


Figura 4.13 Resumen de encriptación desencriptación en recorrido en espiral donde a) imagen recuperada, b) imagen encriptada, c) diferencia de fases en la encriptación d) diferencias de fase en la desencriptación

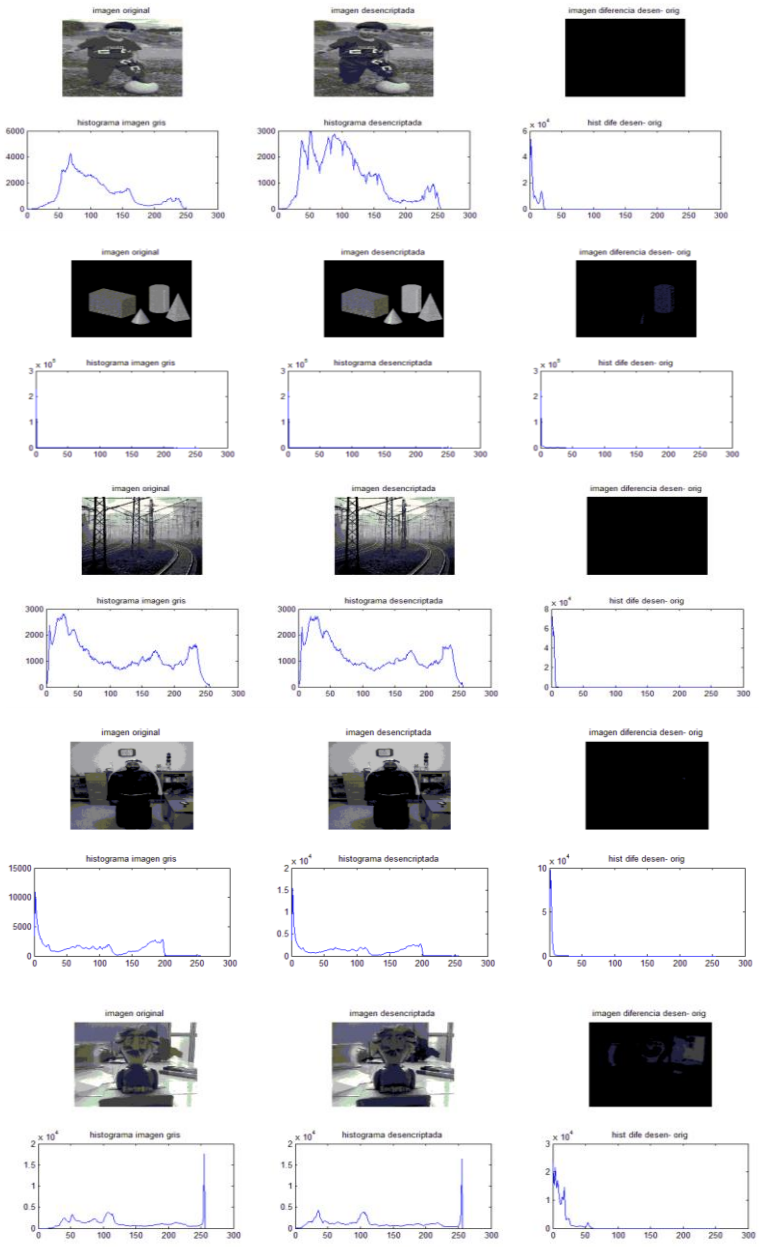


Figura 4.14 histogramas de las imágenes original, desencriptada y su diferencia

Se observa que la pérdida de información es mínima, siendo evidente el ligero cambio de contraste entre la imagen original y la recuperada. Adicionalmente el estadístico que realiza un mapeo de la deformación entre la intensidad de la imagen inicial y la recuperada es muy cercano a 1 (figura 4.15) evidenciando las mínimas perdidas.

La figura 4.14 describe los histogramas de la imagen original, la desencriptada y su diferencia la cual es usada para trabajar el error cuadrático medio (ecuación 4.1) y el pico de la relación señal ruido (ecuación 4.2) relacionados en la figura 4.15

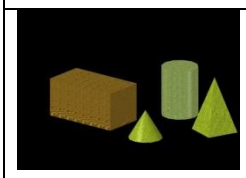
Imagen	Correlación entre las imágenes original y desencriptada	Error cuadrático medio	Valor de RMSE	Valor de PSNR	Pixel máximo
	0.9899	0.0154	0.0077	41	239
	0.9979	0.0212	0.0091	40	238
	0.9998	0.0099	0.0062	43	237
	0.9946	0.0096	0.0061	43	239
	0.9942	0.0071	0.0052	45	240
	0.9894	0.0143	0.0075	47	239

Figura 4.15. Valores de correlación de imagen inicial y final en el proceso, error encontrado, RMSE, PSNR y el pixel de máximo nivel para las distintas imágenes de tamaño 640×480 pixeles

El estadístico PSNR, el cual enseña la relación señal ruido entre la diferencia de la imagen original y la desencriptada[14], se encuentra entre los 40dB y 47dB demostrando una muy buena eficiencia entre la imagen recuperada en la desencriptación con respecto a la imagen original, esta estadística ha de ser superior a 20dB para garantizar una buena calidad en la información de la imagen recuperada [14].

Analizando la posibilidad de ataques, la gráficas de diferencias/pixeles (Figura 4.12, Figura 4.13) de las imágenes reconstruidas permiten estimar una probabilidad de ataques teniendo menos de la mitad de la información. Si se somete una encriptacion a un ataque muy fuerte como es el ataque de fuerza bruta, se estima que el tiempo para encontrar una llave de seguridad que tienen una dimensión de ~ 10^{30} posibles combinaciones, está en el orden de 1.6x10^{10} años. Por tanto si se considera la llave de encriptación, cuyo tamaño es de 640x480 pixeles, discretizada a 8 bits, esto equivale a que ante un ataque de búsqueda exhaustiva las combinaciones posibles de encontrar la llave seria de una en $2^{8\times640\times480}$. Al tomar en cuenta que se tiene menos de la mitad de la información entonces 320x240 pixeles y aplicar un ataque de búsqueda exhaustiva o fuerza bruta las posibles combinaciones para encontrar la llave seria de una en $2^{8\times320\times240}$, se concluye que el tiempo de ejecución seria de un orden demasiado grande para ser vulnerado resultando en un tiempo razonablemente ilógico, para encontrar la combinación correcta de fases que permita decodificar la imagen; adicionalmente el usuario no autorizado debería hacer un recorrido completo sobre el plano de filtrado para poder aplicar cada ataque convencional lo que llevaría mucho tiempo. [8]

La mayoría de las técnicas de encriptación DRPE dependen del gran tamaño de su clave, esto garantiza la seguridad ante los ataque de fuerza bruta [7], es decir, que la probabilidad de adivinar al azar la clave correcta es prácticamente nula lo que da confiabilidad en la encriptación; la presencia de

una clave incorrecta de Fourier introducirá errores en tanto la amplitud como la fase de la salida [6] como en la Figura 4.6

El tiempo de respuesta está dado en milisegundos (ms) para el proceso de encriptación y desencriptación, para una imagen de 640×480 se tiene un tiempo estimado de 80 milisegundos por *frame*, realizado de manera directa desde el valor de memoria

El trabajo realizado para imágenes usando máscara aleatoria bajo la arquitectura 4f, permitió implementar el uso de la encriptación para analizar sistemas dinámicos (video), analizando una secuencia en tiempo real (Figura 4.16).

Cada fotograma o imagen de la escena contiene información correspondiente a una situación que evoluciona en el tiempo representando una escena de 320×240 pixeles con una profundidad de 8 bits. El proceso realizado al encriptar y desencriptar una imagen fue implementado en el sistema dinámico, manifestando el mismo comportamiento estadístico observado para imágenes [9].Con el paso del tiempo en los fotogramas de este tamaño no ocurre una ralentización notable del video, tampoco se observó solapamiento entre imágenes constituyendo en un sistema de encriptación a baja resolución robusto [12]

Se realizó el ejercicio para una resolución de 640×480 tornándose más lenta la reproducción, se sugiere realizar estudios posteriores tomando en cuenta más niveles de resolución

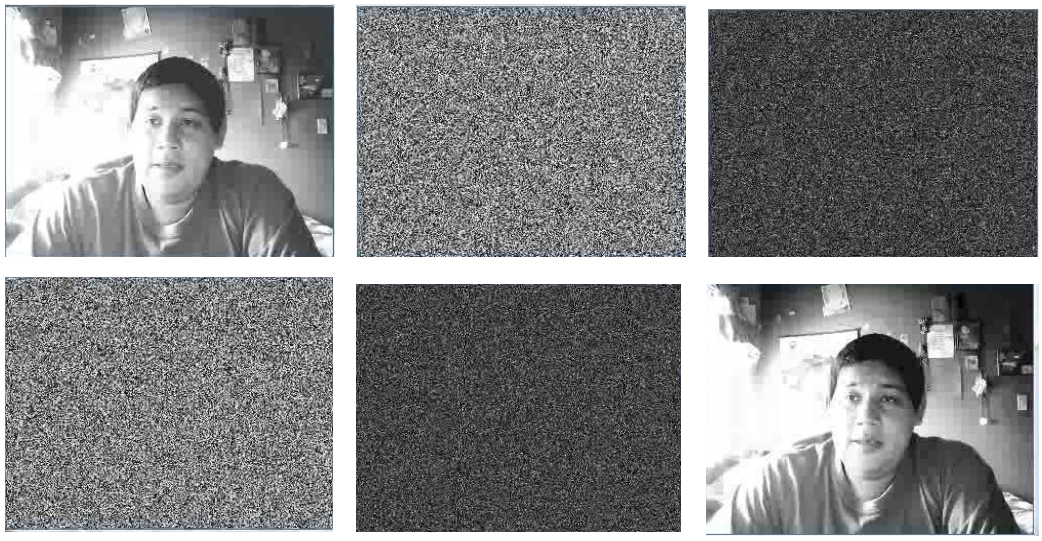


Figura 4.16 Reproducción en tiempo real a 320×240 resolución de cámara web, de derecha a izquierda, arriba: reproducción real, máscara real, encriptación. Abajo: máscara falsa, desencriptación con la llave incorrecta, desencriptación con la llave correcta.

Bibliografía

[1] *ALFALOU A. y et al. COMPRESION DE IMAGEN OPTICAY METODOS DE ENCRITACION "OPTICAL IMAGE COMPRESSION AND ENCRYPTION METHODS" Advances in Optics and Photonics 1, 2009*

[2] *Brito C. Leonardo. " ENCRIPTAMIENTO DE IMÁGENES DIGITALES A COLOR MEDIANTE TRANSFORMADA DE FOURIER". Revista Colombiana de física, VOL. 35, No.1. 2003*

[3] *D. AMAYA, M. TEBALDI, R. TORROBA AND N. BOLOGNINI, PRUEBAS DEL GRADO DE ENCRIPTACION EN UNA ARQUITECTURA 4F, " ENCODING DEGREE TESTING IN A 4F ARCHITECTURE", Proc. SPIE 8011, 801179,2011*

[4] *DENNING Dorothy E, Cristología y seguridad de datos, 'CRYPTOGRAPHY AND DATA SECURITY', Addison-Wesley publishing Company,1982 www.nps.edu/library*

[5] *FORERO V. Manuel y et al. "ESTUDIO DEL EFECTO DE LAS MÁSCARAS DE CONVOLUCIÓN EN IMÁGENES MEDIANTE EL USO DE LA TRANSFORMADA DE FOURIER" Revista Ingeniería e Investigación No. 48 Diciembre de 2001*

[6] *FRAUEL Yann y et al. RESISTENCIA DE LA DOBLE FASE ALEATORIA ANTE VARIOS ATAQUES "RESISTANCE OF THE DOUBLE RANDOM PHASE ENCRYPTION AGAINST VARIOUS ATTACKS". Vol. 15, No. 16, OPTICS EXPRESS 102536 Agosto 2007*

[7] *GLÄSER, M., KOCHSIEK, M. ADVANCES IN SPECKLE METROLOGY AND RELATED TECHNIQUES. WILEY-VCH Verlag & Co. KGaA, 2011.pag 239-244*

[8] *MONAGHAN S. David y et al. INVESTIGACION ESTADISTICA DE LA TECNICA DE ENCRIPTACION DE DOBLE FASE ALEATORIA"STATISTICAL INVESTIGATION OF THE DOUBLE RANDOM PHASE ENCODING TECHNIQUE". Vol 26 N°9 Optical Society of America September 2009*

[9] *MOSSO Fabian y et al. PELICULAS TOTALMENTE OPTICAS " ALL-OPTICAL ENCRYPTED MOVIE". Vol. 19, No. 6 OPTICS EXPRESS 570614 Marzo 2011*

[10] *RÍOS Carlos A., RUEDA Edgar A., BARRERA John F., 'SISTEMA ÓPTICO DE ENCRIPTACIÓN DE DOBLE MÁSCARA DE FASE BAJO ARQUITECTURA 4F'.Grupo de Óptica y Fotónica, Instituto de Física,*

Universidad de Antioquia. Revista. Tecno Lógicas Segunda Edición Especial, ISSN 0123-7799, Diciembre 2010, pp. 75-96

*[*11] *RUEDA Jorge E; ROMERO Ana L; CASTRO Lina M, 'CRIPTOGRAFIA DIGITAL BASADA EN TECNOLOGIA OPTICA'. Bistua: Revista de la facultad de Ciencias Básicas, Julio, año. vol. 3, número 002. Universidad de Pamplona. Bucaramanga, ISSN 0120-4211 Colombia. pp 19-25*

[12] *TEBALDI Myriam. 'MÉTODOS ÓPTICOS COMO HERRAMIENTA PARA ENCRIPTAR-DESECRIPTAR INFORMACIÓN'. Revista Bistua Universidad de Pamplona.Pamplona-Colombia*

[13] *VARGAS C. A. y et al. ENCRIPTACIÓN ÓPTICO-DIGITAL USANDO UNA ARQUITECTURA 4F ''OPTICAL-DIGITAL ENCRYPTION IN A 4F ARQUITECTURE''. Revista Colombiana de Física, vol. 44, No. 3, 2012*

[14] *WENSI LIU Y ET AL. UN ALGORITMO HEURISTICO HIBRIDO PARA MEJORAR EL ATAQUE DE UN TEXTO PLANO CONOCIDO SOBRE ENCRIPTACION EN EL PLANO DE FOURIER, 'A HYBRID HEURISTIC ALGORITHM TO IMPROVE KNOWNPLAINTEXT ATTACK ON FOURIER PLANE ENCRYPTION', Peking University, Vol. 17, No. 16 / OPTICS EXPRESS 13928, 2009*

CONCLUSIONES

La descripción teórica y los resultados experimentales demuestran que es posible manipular información de manera segura empleando una técnica experimental de codificación de doble máscara de fase. La codificación con fase aleatoria usando la transformada discreta de Fourier que en el caso presentado anteriormente se realiza una transformada digital de Fourier, la cual permite la protección de información y a su vez una recuperación con mínimo tipo de ruido o deterioro.

La aplicación del método de encriptación-desencriptación a imágenes de video brindó resultados satisfactorios para videos de tamaños menores a 640×480 pixeles. Por lo tanto, esta técnica puede ser útil para trasmitir video encriptado de mediana resolución de manera segura. Se sugiere realizar estudios para resoluciones mayores.

No importa la posición del ataque la encriptación y desencriptación presenta el mismo comportamiento de tal manera que las probabilidades de ataque se hacen mínimas, constituyendo lo anterior en una fiabilidad del método estandarizando la respuesta a un posible ataque como el ataque de fuerza bruta estudiado.

Los avances a nivel virtual brindan una ventaja para estudiar sistemas ópticos complejos, ya que se puede simular para disminuir la probabilidad de error al experimentar. La facilidad para estudiar arquitecturas con varios grados de libertad hace que sea más eficiente a la hora de trabajar en pruebas de laboratorio disminuyendo el tiempo en este, así como el trabajo matemático y de diseño, permitiendo una mayor comprensión del proceso y

el posible comportamiento como sus virtudes y alcances facilitando indagar en nuevas configuraciones que se ajusten al fin propuesto y reduciendo las eventualidades experimentales

Los resultados experimentales para el cifrado de imágenes muestran que la encriptación de imágenes digitales usando máscaras de fase aleatorias es una técnica promisoria para la transmisión de la información, transformando la información de interés en una señal que aparenta ser ruido blanco e indescifrable al ojo humano.

La desencriptación digital de la señal codificada permitió obtener la imagen original, con una pérdida de información relativamente baja y con una gran calidad en la imagen recuperada.

Se destaca que la aplicación del trabajo fue transformada de Fourier digital, ya que en la trasformada óptica se ha de tener en cuenta la lente, la distancia focal, la apertura de las pupilas, los cambios de fase del campo incidente, los cuales generaran aberraciones que han de ser compensadas usando la llave de seguridad correcta.