UNIVERSIDAD INDUSTRIAL
DE SANTANDER

GRUPO DE ÓPTICA Y TRATAMIENTO
DE SEÑALES

ENCRIPTACIÓN ÓPTICA DE SEÑALES

USANDO TRANSFORMADA DE FOURIER FRACCIONAL

ZANDRA YOANA LIZARAZO MEJÍA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE FÍSICA
2004

UNIVERSIDAD INDUSTRIAL
DE SANTANDER

GRUPO DE ÓPTICA Y TRATAMIENTO
DE SEÑALES

ENCRIPTACIÓN ÓPTICA DE SEÑALES USANDO TRANSFORMADA DE FOURIER FRACCIONAL

ZANDRA YOANA LIZARAZO MEJÍA

Trabajo de Investigación para obtener el título de Magister en Física

Director
Dr. Yezid Torres Moreno

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE FÍSICA
2004

Agradecimientos

Agradezco a la Universidad Industrial de Santander por mi formación en mi maestría y por una beca que me ha permitido dedicar el mayor tiempo posible a mi trabajo.

Agradezco al Grupo de Óptica y Tratamiento de Señales y especialmente agradezco a mi director Yezid Torres quien ha participado activamente en mi formación.

Para mi compañero intelectual y sentimental, RAFAEL TORRES

Índice general

Índice de figuras

TÍTULO [1]: ENCRIPTACIÓN ÓPTICA DE SEÑALES USANDO LA TRANSFORMADA DE FOURIER FRACCIONAL.

Autor: Zandra Yoana Lizarazo Mejía [2].

Palabras Claves: Tranformación de Fourier fraccional, Máscaras de fase aleatorias, Encriptación óptica.

Resumen

Los sistemas de encriptación óptica reportados en la literatura se basan en la transformación de Fourier estándar, donde se aprovecha el hecho que es invertible y se pueden realizar operaciones sobre las señales en el dominio de las frecuencias. Este tratamiento puede generalizarse usando la transformación de Fourier fraccional, de la cual la transformación de Fourier estándar es un caso particular cuando el orden fraccional es igual a la unidad. Esta nueva transformación agrega al sistema otro grado de libertad de acuerdo al orden fraccional empleado. En este trabajo de investigación se propone y se lleva a cabo una configuración óptica para realizar encriptación y decriptación usando la transformación de Fourier fraccional. En un sistema de encriptación uno de los elementos más importantes son las llaves. En óptica este proceso se puede hacer de diferentes formas, modulando la amplitud, la fase o la polarización de una onda lelctromagnt́ica. En particular se escogió modular la fase del frente de onda. Por esto se realiza un estudio del tipo de máscara a usar ya que es necesario determinar si es indiferente el uso de estos elementos. Este tipo de estudio no ha sido reportado aun en la literatura. Usando el principio de conjugación de fase se demuestra la existencia de transformaciones de Fourier fraccional ópticas inversas, principio que permite usar una misma configuración óptica llevar a cabo tanto el proceso de encriptación como el de decriptación.

[1] Trabajo de Investigación.

[2] Facultad de Ciencias. Maestría en Física. TORRES MORENO, Yezid.

TITLE [3]: OPTICAL SIGNAL ENCRYPTION USING THE FRACTIONAL FOURIER TRANSFORM.

Author: Zandra Yoana Lizarazo Mejía [4].

Keywords: fractional Fourier transform, random phase mask, optical encryption.

Resumen

The optical encryption systems reported in the literature that based on Fourier transformation, since this operator is invertible and operations can be carried out in the frequency domain. This treatment can be generalized using the fractional Fourier transformations, taking into account that Fourier transformations is an particular case when the orden equal the unit. This new transformations adds freedom degree according to the order used. In this research work an optical configuration is proposed and developed to carry out encryption and decryption using the fractional Fourier transformation. In applications to security is very important the keys. In optical configurations this process can be done of different way, modulating the amplitude, phase and polarization the electromagnetic wave. In this work have been selected the phase modulation. Is developed an preliminary study for establishing the type mask to use in the optical configurations. This new approach has not been yet reported widely in literature becoming highly important in encryption and decryption systems. Using the physical phenomenon of phase conjugation is showed the existence of the optical inverse fractional Fourier transform. This demonstration permit use an seem optical configurations for booth process, encryption and decryption.

[3]Research Work.

[4]Facultad de Ciencias. Maestría en Física. TORRES MORENO, Yezid.

Introducción

Dos hechos que marcaron el inicio de una nueva era en las comunicaciones fueron el surgimiento de los ordenadores en el año de 1960 y el advenimiento de Internet en el año 1972, estos dos eventos han cambiado radicalmente la forma en que nos comunicamos e intercambiamos información.

Estas tecnologías han evolucionado hacia un mismo objetivo el cual es aumentar la velocidad, tanto en los dispositivos electrónicos que componen los ordenadores como en las redes de comunicación, el avance en estos dos aspectos permiten procesar e intercambiar grandes cantidades de información a altas velocidades. Como consecuencia de estos cambios se crean nuevos desafíos para la seguridad y privacidad de las comunicaciones e información, para responder a estas necesidades debe hacerse uso de técnicas criptográficas.

En la actualidad las redes de comunicación se basan en redes de fibra óptica, que cuentan con un gran ancho de banda y por tal razón se pueden enviar grandes volúmenes de información a través de estos canales. Para responder a estas necesidades los sistemas criptográficos deben trabajar a velocidades similares a la velocidad del flujo de datos para garantizar la seguridad de la información en tiempo real. Con este fin se han desarrollado aplicaciones en software y hardware que permiten encriptar la información con alto grado de fiabilidad, pero a pesar de los avances en este campo, aún se siguen presentando casos de interceptación ilegal de la información, lo cual lo convierte en un campo abierto de investigación.

Una alternativa de uso la presentan los sistemas de encriptación ópticos, los cuales poseen características que los hacen atractivos para este tipo de aplicaciones. Principalmente porque estos sistemas trabajan a la velocidad de la luz, y la información se procesa en paralelo y prácticamente en tiempo real. Uno de los elementos más importante en la encriptación son las llaves para encriptar, y en la óptica estas pueden realizarse de diferentes formas, cambiando apropiadamente ciertas características del campo electromagnético ya sea la fase, la amplitud o la polarización por ejemplo. La modulación apropiada de cualquiera de estos elementos garantiza la seguridad de la información además de su recuperación.

Los sistemas de encriptación óptica reportados en la literatura se basan en la transformación de Fourier estándar, donde se aprovecha el hecho que es invertible y se pueden realizar operaciones sobre las señales en el dominio de las frecuencias. Este tratamiento puede generalizarse usando la transformación de Fourier fraccional, de la cual la transformación de Fourier estándar es un caso particular cuando el orden fraccional es igual a la unidad. Esta nueva transformación agrega al sistema otro grado de libertad de acuerdo al orden fraccional empleado [1]-[3],[4]. Se debe tener en cuenta que esta transformación es variante al corrimiento, que de acuerdo

a la aplicación puede ser una ventaja o desventaja. Lo expuesto anteriormente hacen de esta transformación una herramienta idónea para ser utilizada en aplicaciones a la encriptación óptica. En este trabajo de investigación se propone y se lleva a cabo una configuración óptica para realizar encriptación y decriptación usando la transformación de Fourier fraccional, se realiza un análisis del tipo de máscaras a usar, este tipo de análisi no ha sido reportado en la literatura y es importante determinar si es indiferente el tipo de máscaras. Usando el principio de conjugación de fase se demuestra la existencia de transformaciones de Fourier fraccional ópticas inversas.

Capítulo 1

Marco de referencia

1.1. Marco Teórico

Algunos elementos teóricos importantes a tener en cuenta en este trabajo de investigación son:

- † Sistemas de encriptación basados en la transformación de Fourier estándar.
- † Transformación de Fourier fraccional.
- † Transformación de Fourier fraccional en óptica.
- † Cristales fotorrefractivos.
    - Conjugación de Fase.
    - Transformación de Fourier fraccional óptica inversa

En el campo de la encriptación óptica se tienen varios antecedentes entre los cuales hay una amplia gama de arquitecturas que hacen uso de la transformación de Fourier estándar [5]-[10]. Dado que esta transformación permite ir del dominio directo de las señales al dominio de las frecuencias y viceversa, hace posible realizar diversas operaciones sobre el contenido espectral de las señales y volver al dominio directo para encontrar una nueva señal la cual es una versión encriptada de la señal original. Ópticamente las llaves pueden generarse usando diferentes técnicas como son modular la amplitud, la fase o la polarización de una onda electromagnética.

Un sistema de encriptación tiene dos etapas una en la que se realiza el proceso de encriptación y otra que realiza el proceso de decriptación.

Un sistema de encriptación basado en la transformación de Fourier estándard, como el mostrado en la figura 1.1, para obtener la señal encriptada lo primero que se hace es llevar a cabo una transformación de Fourier sobre el objeto o, ya en el dominio de las frecuencias se realiza el producto por la llave (Máscara de fase aleatoria M) y sobre este producto se efectúa otra transformación de Fourier, obteniéndose a la salida la señal encriptada (k), que no mas que la convolución del objeto o con la función de encriptación, siendo esta operación la responsable del proceso de encriptación como tal.

Para decriptar la señal se hace una devolución en el proceso, se efectúa una transformación de Fourier sobre la señal encriptada k, en este dominio se multiplica por la máscara conjugada M^*, de esta forma se elimina la fase y con otra transformación de Fourier se obtiene el objeto del que se partió en este caso o.

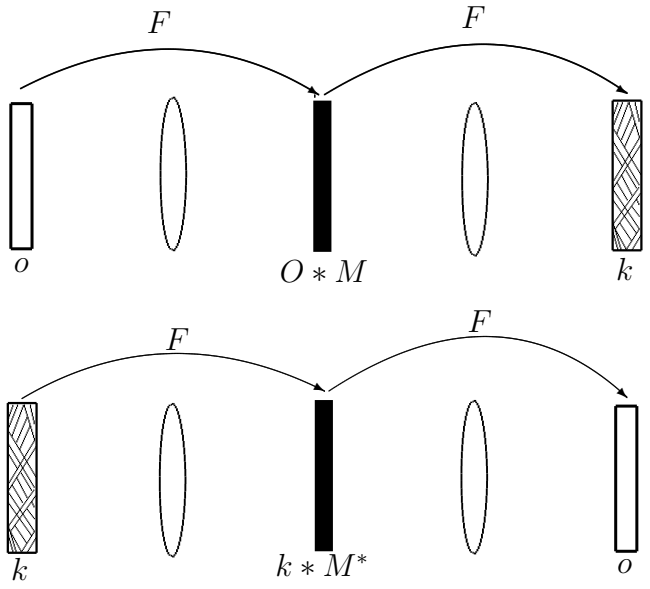


Figura 1.1: Esquema de encriptación usando la transformada de Fourier estándar

1.1.1. Transformación de Fourier fraccional

El sistema óptico de encriptación desarrollado en esta tesis se basa en la transformación de Fourier fraccional (TFf), la cual tuvo la primera respresentación integral en el año de 1960 por Víctor Namías [11], como una herramienta para solucionar ecuaciones diferenciales aplicadas al oscilador armónico mecánico cuántico. Esta definición de TFf se basa en las funciones de Hemitte-Gauss las cuales son también funciones propias del operador transformada de Fourier estándar. La expresión integral es

$$\mathcal{F}^{\alpha}[f](x') = \frac{e^{i\pi/4}e^{-i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{-i\pi x'^2\cot\alpha} \int_{\mathbb{R}} e^{-i\pi x^2\cot\alpha} e^{\frac{2i\pi xx'}{\sin\alpha}} f(x)dx\,, \tag{1.1}$$

donde $\alpha = p\pi/2$. Cuando el orden fraccional $p = 1$, se obtiene el operador transformación de Fourier estándar, [11].

En aplicaciones y en especial en este tipo de trabajo es importante tener en cuenta algunas propiedades y Teoremas de la transformada de Fourier estándar que se han extendido a la TFf,

† Linealidad

$$\mathcal{F}^{\alpha}[af(x) + bg(x)](x') = a\mathcal{F}^{\alpha}[f(x)](x') + b\mathcal{F}^{\alpha}[g(x)](x') \tag{1.2}$$

† **Inversa**

$$(F^{\alpha})^{-1} = \mathcal{F}^{-\alpha} \tag{1.3}$$

† **Aditividad del Índice**

$$\mathcal{F}^{\alpha_2}\mathcal{F}^{\alpha_1} = \mathcal{F}^{\alpha_2+\alpha_1} \tag{1.4}$$

† **Conmutatividad**

$$\mathcal{F}^{\alpha_2}\mathcal{F}^{\alpha_1} = \mathcal{F}^{\alpha_1}\mathcal{F}^{\alpha_2} \tag{1.5}$$

† **Asociatividad**

$$\mathcal{F}^{\alpha_3}(\mathcal{F}^{\alpha_2}\mathcal{F}^{\alpha_1}) = (\mathcal{F}^{\alpha_3}\mathcal{F}^{\alpha_2})\mathcal{F}^{\alpha_1} \tag{1.6}$$

† **Teorema del corrimiento**

$$\mathcal{F}^{\alpha}[f(x-\zeta)](x') = e^{-i\pi \sin\alpha(\gamma^2\cos\alpha - 2x'\gamma)} f_{\alpha}(x' - \gamma\cos\alpha) \tag{1.7}$$

† **Teorema del escalamiento**

$$\mathcal{F}^{\alpha}[f(cx)](x') = \sqrt{\cos\beta/\cos\alpha}\ \ e^{\frac{1}{2}i(\alpha-\beta)} e^{i\pi x'^2 \cot\alpha(1-\frac{\cos^2\beta}{\cos^2\alpha})} f_{\beta}(x'\frac{\sin\beta}{c\sin\alpha}), \tag{1.8}$$

donde $\tan\beta = c^2\tan\alpha$.

Tanto el Teorema del corrimiento como el Teorema del escalamiento en aplicaciones a la encriptación y en otros campos deben ser tenidos en cuenta, ya que agregan un alto grado de complejidad en el posicionamiento de los elementos ópticos y el alineamiento de todos los componentes del sistema cuando se trabaja con la transformación de Fourier fraccional. Teniendo en cuenta esto es importante hacer una demostración formal del mismo. La TFf de una función trasladada toma la siguiente forma,

$$\mathcal{F}^{\alpha}[f(x-\gamma)](x') = \frac{e^{i\pi/4}e^{-i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{-i\pi x'^2\cot\alpha} \int e^{-i\pi x^2\cot\alpha} e^{\frac{2i\pi x x'}{\sin\alpha}} f(x-\gamma)d(x-\gamma) \tag{1.9}$$

Haciendo el cambio de variable,

$$x - \gamma = \xi$$

$$\begin{aligned}
\mathcal{F}^{\alpha}[f(x-\gamma)](x') &= \frac{e^{i\pi/4}e^{-i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{-i\pi x'^2\cot\alpha} \int e^{-i\pi(\xi+\gamma)^2\cot\alpha} e^{\frac{2i\pi(\xi+\gamma)x'}{\sin\alpha}} f(\xi)d(\xi) \\
&= \frac{e^{i\pi/4}e^{-i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{-i\pi x'^2\cot\alpha} e^{-i\pi x'^2\cot\alpha} e^{-i\pi\gamma^2\cot\alpha} e^{\frac{-i2\pi\gamma x'}{\sin\alpha}} \\
&\times \int e^{-i\pi\xi^2\cot\alpha} e^{\frac{i2\pi\xi}{\sin\alpha}(x'-\gamma\cos\alpha)} f(\xi)d\xi
\end{aligned} \tag{1.10}$$

reemplazando,

$$x' - \gamma\cos\alpha = \chi$$

$$\begin{aligned}
&= \frac{e^{i\pi/4}e^{-i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{-i\pi x'^2\cot\alpha} e^{\frac{i2\pi\gamma x'}{\sin\alpha}} e^{-i\pi\gamma^2\cot\alpha} \\
&\times \int e^{-i\pi\xi^2\cot\alpha} e^{\frac{i2\pi\xi\chi}{\sin\alpha}} f(\xi)d(\xi) \\
&= e^{-i\pi x'^2\cot\alpha} e^{\frac{i2\pi\gamma x'}{\sin\alpha}} e^{-i\pi\gamma\cot\alpha} e^{i\pi\chi^2\cot\alpha} \mathcal{F}^\alpha[f(\chi)] \\
\mathcal{F}^\alpha[f(x-\gamma)](x') &= e^{-i\pi\sin\alpha(\gamma^2\cos\alpha - 2\gamma x')} f_\alpha(x' - \gamma\cos\alpha) \qquad (1.11)
\end{aligned}$$

Lo que muestra este teorema es que la transformación de Fourier fraccional de una función trasladada no se desplaza en la misma proporción, se puede decir que es otro grado de complejidad que puede ser agregado al sistema de encritación.

Existen varias definiciones de la transformación de Fourier fraccional, todas ellas equivalentes, pero entre todas estas, para este trabajo se tomó la que guarda una relación más estrecha con la óptica. Entre la definiciones conocidas se ilustran las siguientes que en su mayoría provienen de la aplicabilidad a la solución de ecuaciones diferenciales

1. Transformada Integral Lineal.
2. Potencias Fraccionarias de la Transformada de Fourier estándar usando la ecuación de valores propios en el espacio de las funciones de Hermite-Gauss.
3. Rotación de la Distribución de Wigner en el plano espacio directo-frecuencia.
4. Transformación de los Operadores Multiplicación y Diferenciación de Coordenadas.
5. Ecuación Diferencial.
6. Operador Hyperdiferencial.

Se puede demostrar que es posible pasar de una definición a otra sin ningún problema, lo cual indica que cada una de estas definiciones son completamente consistentes [12].

1.2. Transformación de Fourier fraccional en Óptica

De la transformación de Fourier fraccional en óptica se tienen tres realizaciones, la primera fue reportada por Mendlovic y Ozaktas en un medio GRIN [13],[14] y la segunda, posteriormente fue reportada por Lohmann quien propone dos configuraciones ópticas conocidas como Lohmann Tipo I y II, ver figuras 1.2 y 1.3. En este trabajo se usa la configuración Lohmann tipo I para llevar a cabo las transformaciones de Fourier fraccional [15]. Pellat-Finet [16] halló que la difracción de Fresnel puede expresarse como una Transformación de Fourier fraccional haciendo que la propagación de las ondas electromagnéticas en el espacio libre es un vehículo natural para realizar esta transformación.

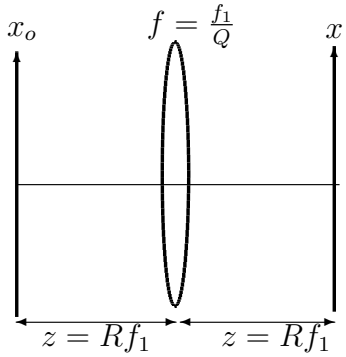


Figura 1.2: Configuración Lohmann Tipo I

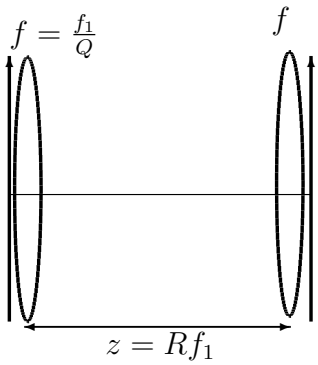


Figura 1.3: Configuración Lohmann Tipo II

1.2.1. Sistemas Lohmann basados en la Distribución de Wigner

Los sistemas propuestos por Lohmann se basan en una de las definiciones de la transformación de Fourier fraccional, la cual consiste en la rotación de la Distribución de Wigner de la señal, un ángulo $\alpha = p\frac{\pi}{2}$.

Para llegar a definir estas configuraciones ópticas es necesario estudiar cual es el efecto de los diferentes elementos físicos que intervienen en estas configuraciones sobre la Distribución de Wigner, tales efectos son: la transformación de Fourier óptica, el efecto de la lente y la propagación en el espacio libre. En este orden se procede a hacer el desarrollo matemático en términos de la distribución de Wigner.

La Distribución de Wigner de $u(x)$, se define como:

$$\mathcal{W}_u(x,\nu) = \int u(x+\frac{x'}{2})u^*(x-\frac{x'}{2})e^{-i2\pi x'\nu}dx' \,. \tag{1.12}$$

Usando la representación de la señal en el plano de Fourier

$$u(x) = \int \widetilde{u}(\nu)e^{i2\pi\nu' x}d\nu' \,, \tag{1.13}$$

e insertando esto en la ecuación se obtiene

$$\mathcal{W}_u(x,\nu) = \int \widetilde{u}(\nu+\frac{\nu'}{2})\widetilde{u}^*(\nu-\frac{\nu'}{2})e^{i2\pi\nu' x}d\nu' \,. \tag{1.14}$$

Teniendo en cuenta estas relaciones matemáticas de la distribución de Wigner se puede asociar a parámetros ópticos y encontrar el conjunto de elementos ópticos que efectúen las mismas operaciones sobre la señal.

Las frecuencias que contiene la señal se relacionan con las posiciones en el plano de Fourier de la forma:

$$\lambda f_1 \nu = \xi \,,$$

donde ν son las frecuencias espaciales con dimensiones $\frac{1}{longitud}$ y f_1 es una longitud "focal" arbitraria. Teniendo en cuenta estos parámetros podemos escribir la función de la siguiente forma:

$$u_F(\xi) = \tilde{u_o}(\frac{\xi}{\lambda f_1}) = \int u_o(x) e^{-i2\pi \frac{\xi x}{\lambda f_1}} dx \,. \tag{1.15}$$

La distribución de Wigner $u_o(x)$ en función de los parámetros ópticos asociados es

$$\mathcal{W}_{u_o}(x,\xi) = \int u_o(x + \frac{x'}{2}) u_o^*(x - \frac{x'}{2}) e^{-i2\pi x' \frac{\xi}{\lambda f_1}} dx' \,. \tag{1.16}$$

En términos de las coordenadas del espacio recíproco la distribución de Wigner resulta

$$\mathcal{W}_{u_o}(x,\xi) = \int u_F(\xi + \frac{\xi'}{2}) u_F^*(\xi - \frac{\xi'}{2}) e^{i2\pi x \frac{\xi'}{\lambda f_1}} d\xi' \,. \tag{1.17}$$

Lo cual conduce a:

$$\mathcal{W}_{u_o}(x,\xi) \quad \rightarrow \quad \mathcal{W}_F(x,\xi) = \mathcal{W}_{u_o}(-\xi, x) \,. \tag{1.18}$$

De esta expresión se concluye que se produce una rotación de 90° de la distribución de Wigner, en sentido de las manecillas del reloj.

Se puede analizar que efectos tienen otros fenómenos físicos sobre la distribución de Wigner. Para definir las configuraciones ópticas propuestas por Lohmann es necesario estudiar dos fenómenos esencialmente:

‡ Paso a través de una lente delgada.

$$u_o \rightarrow u_o(x) e^{-i\pi \frac{x^2}{\lambda f}} = u_L(x),$$

lo que equivale a efectuar sobre la distribución de Wigner

$$W_{u_o}(x,\xi) \rightarrow W_{u_o}(x, \xi + Qx) = W_{u_L}(x,\xi).$$

Esto indica que el efecto de la lente sobre la distribución de Wigner se traduce en una cizalladura en las coordenadas ξ.

‡ Propagación en el espacio libre.

Usando la representación de la señal en el dominio de las frecuencias espaciales

$$u_F(\xi) \rightarrow u_F(\xi)e^{-i\pi\frac{\xi^2}{\lambda f_1}} = u_z(\xi),$$

el efecto sobre la distribución de Wigner es

$$W_{u_o}(x,\xi) \rightarrow W_{u_z}(x,\xi) = W_{u_o}(x - R\xi, \xi).$$

En este caso el efecto sobre la distribución de Wigner es una cizalladura en las coordenadas x. Teniendo en cuenta que:

$$f = \frac{f_1}{Q}, \qquad z = Rf_1.$$

El efecto de la lente y la propagación en el espacio libre sobre la distribución de Wigner pueden escribirse en términos del operador multiplicación y convolución chirp respectivamente. Las matrices canónicas lineales de estos tres operadores se escriben

$$\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{bmatrix} \begin{bmatrix} x \\ \xi \end{bmatrix} = \begin{bmatrix} x' \\ \xi' \end{bmatrix} \tag{1.19}$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}; \qquad \begin{bmatrix} 1 & 0 \\ Q & 1 \end{bmatrix}; \qquad \begin{bmatrix} 1 & -R \\ 0 & 1 \end{bmatrix} \tag{1.20}$$

La transformación de coordenadas de la distribución de Wigner, se puede expresar como una matriz de rotación un ángulo α.

$$\begin{bmatrix} \cos(\alpha) & -\operatorname{sen}(\alpha) \\ \operatorname{sen}(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} x \\ \xi \end{bmatrix} = \begin{bmatrix} x\cos(\alpha) - \xi\operatorname{sen}(\alpha) \\ \xi\operatorname{sen}(\alpha) + x\cos(\alpha) \end{bmatrix}. \tag{1.21}$$

El orden de la transformación de Fourier fraccional queda interpretado como un ángulo:

$$\alpha = \frac{p\pi}{2},$$

cuando $p = 1$ la matriz de transformación es una matriz de rotación de 90°.

La distribución de Wigner de la transformada de Fourier fraccional u_p se relaciona con la distribución de Wigner de la función u_o por

$$W_{u_o}(x,\xi) \rightarrow W_{u_p}(x,\xi) = W_{u_o}(x\cos\phi - \xi\operatorname{sen}\phi, \xi\cos\phi + x\operatorname{sen}\phi).$$

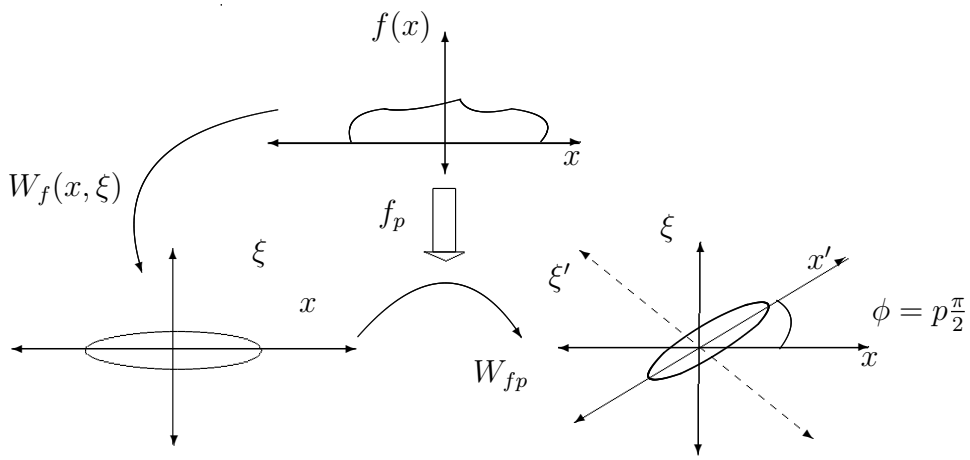


Figura 1.4: Efecto de TFf sobre la distribución de Wigner

Este resultado indica que la TFf produce una rotación de $\phi = p\frac{\pi}{2}$ en la distribución de Wigner de la función, ver figura 1.4 donde f_p es la transformada de Fourier fraccional de orden p

Teniendo en cuenta que las coordenadas se relacionan de la siguiente manera,

$$u' = u\cos(\alpha) - \xi\,\mathrm{sen}(\alpha), \qquad \xi' = \xi\cos(\alpha) + u\,\mathrm{sen}(\alpha).$$

El sistema Lohmann tipo I se puede expresar como RQR, y el sistema Lohmann tipo II como QRQ, teniendo en cuenta los siguientes parámetros:

$$I : R = \tan(\tfrac{\phi}{2}), \qquad Q = \mathrm{sen}(\phi)$$

$$II : Q = \tan(\tfrac{\phi}{2}), \qquad R = \mathrm{sen}(\phi)$$

1.3. Cristales Fotorrefractivos

Cuando un material fotorrefractivo es expuesto a la luz portadores de cargas libres son generados por fotoexcitación de forma tal que el movimiento de estos portadores de carga puede llevarse a cabo por tres diferentes mecanismos: arrastre, difusión y efecto fotovoltaico, lo cual puede escribirse, [17]

$$j(z,t) = e\mu n(z,t)[E_{sc}(z,t) - \frac{V}{L}] - \mu k_B T\frac{dn(z,t)}{dz} + eL_{ph}\dot{n}_1(z,t)\,, \tag{1.22}$$

$$n(z,t) = n_d + n_1(z,t), \qquad n_1(z,t) = \tfrac{\Phi\alpha I(z,t)}{h\nu},$$

$$j(z,t) = [\sigma_o + \mu bI(z,t)][E_{sc}(z,t) - \frac{V}{L}] - Db\frac{dI(z,t)}{dz} + k\alpha I(z,t)\,. \tag{1.23}$$

De acuerdo al tipo de cristal fotorrefractivo uno de estos tres mecanismos de transporte puede dominar, ejemplo de esto, es el tipo de cristal que se uso para este trabajo de investigación, es un cristal paraeélectrico en los cuales el efecto fotovoltaico es despreciable, quedando solamente la contribución por arrastre y difusión.
De la ecuación (1.21) y (1.22) se puede calcular el campo de carga espacial teniendo en cuenta que las densidades de corriente eléctrica de arrastre y difusión pueden ser iguales en magnitud y opuestas en signo, de tal forma que la densidad de corriente desaparece. La ecuación 1.22 se puede expresar como 1.23 donde μ es la movilidad de los portadores de carga, E_{sc} es la componente del campo de carga espacial en la dirección z, V es el voltaje externo aplicado entre los electrodos ubicados en dos caras del cristal, L es el espaciamiento de los electrodos, k_B es la constante de Boltzmann, T es la temperatura absoluta, n_d es la concentración de portadores de carga libre excitados térmicamente en la oscuridad, $n_1(z,t)$ es el exceso de portadores de carga libre debido a la iluminación, α es la constante de absorción, Φ es la eficiencia cuántica, $h\nu$ es la energía del fotón, D es la constante de difusión, $I(z,t)$ intensidad de la luz, $\mu b I(z,t)$ es la fotoconductividad con $b = \frac{e\Phi\alpha}{h\nu}$ y $\sigma_d = e\mu n_d$ es la conductividad en la oscuridad.

Los portadores de carga libre fotogenerados van desde niveles de impurezas a otros niveles de energía en una rata proporcional a la potencia óptica creando una distribución de carga espacial que produce un campo eléctrico interno el cual modula localmente el índice de refracción del material via el efecto electro-óptico (Pockels) . Esta distribución inhomogénea de carga puede permanecer en el lugar por un período de tiempo después que la luz ha sido removida. Materiales de este tipo pueden volver a su estado inicial por iluminación con luz uniforme o por calentamiento, por esta razón pueden usarse para almacenar y recuperar información.

El fenómeno físico que domina el proceso de registro sobre un material fotorrefractivo es el de interferencia [18], ver figura 1.5a.

Cuando dos ondas de la forma

$$\varepsilon_1 = \varepsilon_{10} e^{i\varphi_1} e^{i\mathbf{k}_1\cdot\mathbf{r}}, \qquad \varepsilon_2 = \varepsilon_{20} e^{i\varphi_2} e^{i\mathbf{k}_2\cdot\mathbf{r}},$$

ε_1 y ε_2 : Campos eléctricos de las ondas 1 y 2.
ε_{10} y ε_{20} : Respectivas amplitudes.
φ_1 y φ_2 : Fases de cada haz.
$\mathbf{k}_1$ y $\mathbf{k}_2$: dirección de propagación de los haces, dada por cada vector de onda.

inciden sobre un cristal, puede verse la variación espacial del patrón en el cristal figura 1.5b, y esto puede expresarse como el modulo cuadrado del campo eléctrico.

$$\mathcal{I} = [\varepsilon_1 + \varepsilon_2]^2 = \varepsilon_{10}^2 + \varepsilon_{20}^2 + 2\varepsilon_{10}\varepsilon_{20}\cos(\mathbf{K}\cdot\mathbf{r} + \varphi_2 - \varphi_1)\,, \tag{1.24}$$

donde

$$\mathbf{K} = \mathbf{k_1} - \mathbf{k_2}, \qquad \mathbf{K} = \tfrac{2\pi}{\Lambda},$$

$\mathbf{\Lambda}$: Espaciamiento de Red. $\mathbf{K}$: Vector de red.
Esta relación entre el vector de red y los vectores de onda de los haces incidentes se cumple solo si se satisface la condición de Bragg, donde la red dieléctrica de vector de onda K difractará un haz incidente de vector de onda k_1 en la dirección k_2, ver figura 1.5c.

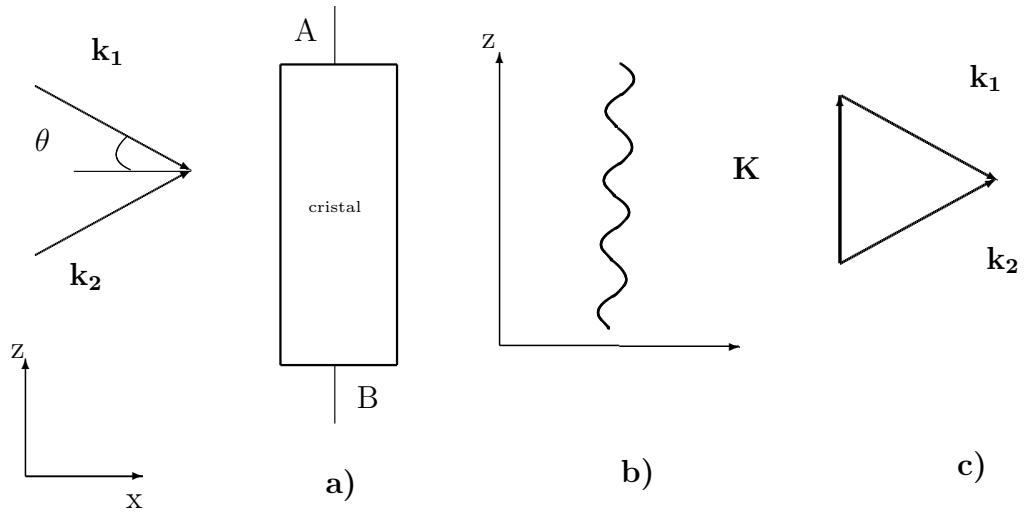


Figura 1.5: a)Esquema de mezclado de dos ondas en un cristal fotorrefractivo, b) Patrón de intensidad dentro del cristal, c) Un vector de red **K** es creado por los dos haces de vectores de onda $\mathbf{k_1}$ y $\mathbf{k_2}$

1.3.1. Conjugación de fase

El fenómeno de conjugación de fase puede llevarse a cabo usando un cristal fotorrefractivo cumpliendo la condición de Bragg. Cuando en el cristal inciden dos haces de la forma,

$$\mathcal{H}_o, \qquad \mathcal{H}_r = Ae^{i2\pi\alpha x}$$

Con base en los principios de la Holografía la inforamación almacenada en el cristal,

$$\mathcal{I} = [H_o + H_r]^2 = H_o^2 + A^2 + H_o{}^* \cdot e^{i2\pi\alpha x} + H_o \cdot e^{-i2\pi\alpha x} \tag{1.25}$$

Si se ilumina el cristal con el haz referencia conjugado como se muestra en el esquema [18].

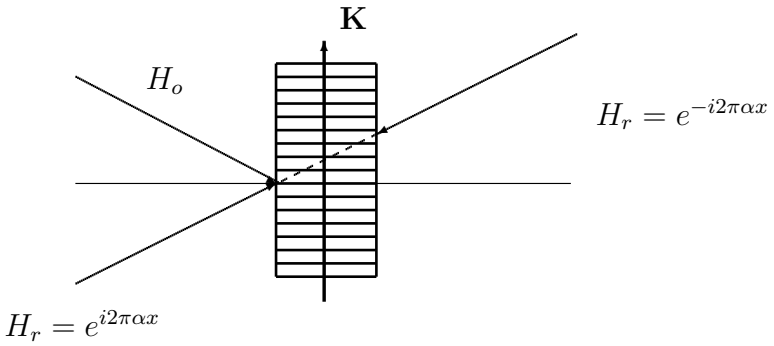


Figura 1.6: Esquema de conjugación de fase

se tiene,

$$H = (H_o^2 + A^2) \cdot e^{-i2\pi\alpha x} + H_o{}^* + H_o \cdot e^{-i4\pi\alpha x} \tag{1.26}$$

Uno de los haces se propaga en la misma dirección del haz objeto pero en sentido contrario y conjugado, que corresponde a la amplitud conjugada del campo objeto.

1.4. Transformación de Fourier fraccional Inversa

Uno de los problemas a tratar con las operaciones ópticas es el hecho que no existen en la óptica la forma de realizar transformaciones inversas directamente, por lo cual se recurre a reemplazar esta transformación inversa por otra transformación con la ayuda de algunas propiedades como por ejemplo la periodicidad del operador TFf o la búsqueda del operador paridad, pero en este trabajo se abordó otra alternativa con base en el fenómeno físico de conjugación de fase y se demostró que es posible llevar a cabo una transformación de Fourier fraccional inversa ópticamente.

La transformada de Fourier fraccional de una función conjugada, se escribe

$$\begin{aligned}
\mathcal{F}_\alpha[f^*](x') &= \frac{e^{i\pi/4}e^{-i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{-i\pi x'^2\cot\alpha} \int e^{-i\pi(x^2\cot\alpha} e^{\frac{2i\pi xx'}{\sin\alpha}} f^*(x)d(x) \\
&= [\frac{e^{-i\pi/4}e^{i\alpha/2}}{\sqrt{|\sin\alpha|}} e^{i\pi x'^2\cot\alpha} \int e^{i\pi(x^2\cot\alpha} e^{\frac{-i2\pi xx'}{\sin\alpha}} f(x)d(x)]^* \\
\mathcal{F}_\alpha[f^*](x') &= [\mathcal{F}_{-\alpha}[f](x')]^*, \qquad (1.27)
\end{aligned}$$

esta expresión indica que la transformación de Fourier fraccional de una función conjugada es igual al conjugado de la transformación de Fourier fraccional inversa de la función.

Capítulo 2

Configuración Óptica para Encriptación-Decriptación

La configuración óptica usada para el proceso de encriptación-decriptación es como se muestra en la figura 2.1. A la salida del láser se usa un filtrado espacial, luego se obtiene una onda plana la cual incide sobre el BS_1 de donde emergen los dos haces principales para la configuración óptica, el haz que sirve para el proceso de encriptación y el haz conjugado que se usa en la configuración de decriptación. Cada uno de los procesos se explica brevemente en la siguiente sección.

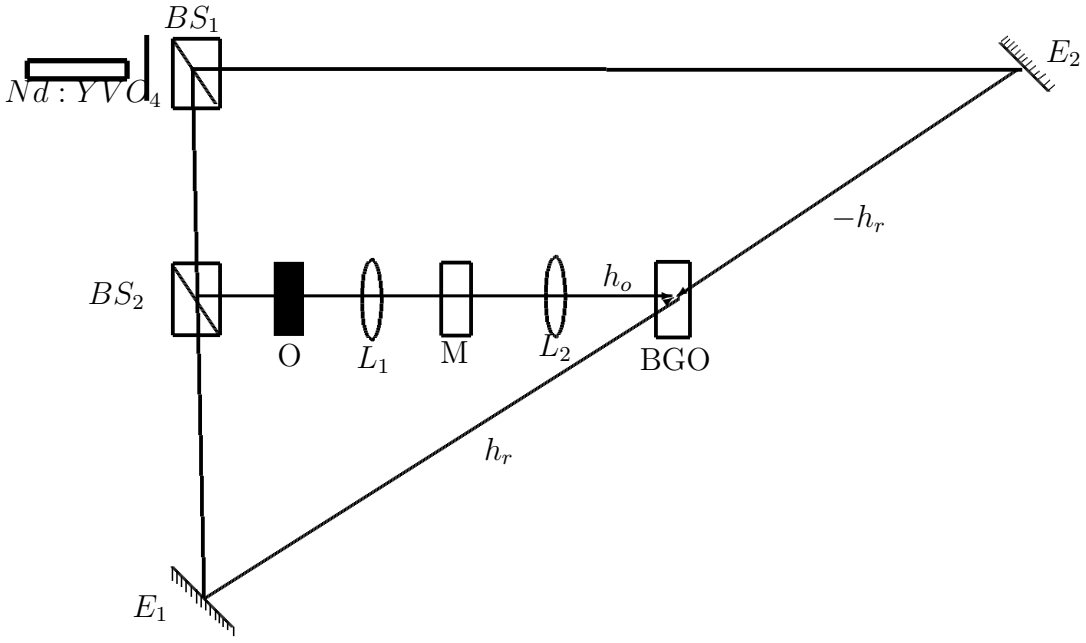


Figura 2.1: Configuración óptica para Encritación-Decriptación

los elementos ópticos involucrados en esta configuración son: BS_1 y BS_2 : Divisores de haz. L_1 y L_2 : Lentes.

E_1 y E_2 : Espejos.
h_o : Haz objeto.
h_r : Haz de referencia.
$-h_r$: Haz de referencia viajando en sentido opuesto.
O : Objeto.
M : Máscara de fase aleatoria.
BGO: Cristal fotorrefractivo de Óxido de Germanio y Bismuto($Bi_{12}GeO_{20}$).
CCD: Cámara.

Uno de los elementos más importantes en un proceso de encriptación son las llaves. En este trabajo las máscaras de fase fueron implementadas de dos maneras, una primera forma se efectúa modulando el índice de refracción de un dispositivo con base en un *Spatial Light Modulator*(SLM), con el cual se cambia la fase del frente de onda de forma aleatoria pero de manera determinista. Esto se logra haciendo uso de un ordenador en el cual se calcula previamente las máscaras usando un generador de numeros aleatorios. El hecho de que pueda direccionarse el SLM, que en este caso se trata de un cristal liquido, va a permitir reproducir cada vez que se desee una mascara de fase previamente calculada. El uso de este tipo de dispositivos permite generar un banco de llaves dinámico.

La segunda forma de obtener las llaves fue usando materiales transparentes que permitan modular la fase de un frente de onda de forma aleatoria como función del espesor. Específicamente se usa como máscara de fase aleatoria un material de plástico y un material a base de acetato. La desventaja que presentan estos elementos comparados con los LCD es que no se conoce con exactitud el rango de fase que introducen, ya que no fueron fabricados para este tipo de aplicaciones, además de no poderse reproducir cada vez que sea necesario, convirtiéndose en llaves estáticas.

Como medio de registro se usa un cristal fotorrefractivo de BGO**??**.

2.1. Especificaciones de la configuración óptica

En la configuración óptica se usaron los siguientes elementos:

- ‡ Láser $Nd:YVO_4$ a $532nm$ de $50mW$ de potencia.
- ‡ Láser $He-Ne$ a $632nm$ de $5mW$ de potencia.
- ‡ El ángulo entre h_o y h_r es $\theta = 25°$.
- ‡ Ordenes fraccionales usados $\alpha = \beta = 0{,}6960$, con $z = 18{,}9cm$.
- ‡ Se usa como medio de registro un cristal fotorrefractivo de BGO que opera sin campo externo aplicado. De este cristal solo se conocen sus dimensiones y sus ejes cristalográficos, ver figura 2.2. De este cristal no se tienen específicaciones técnicas, en la tabla 2.1 se registran algunas
características generales de este tipo de cristales.

Estos cristales son aislantes en el espectro visible y forman parte de la familia de los Silenitas. Esta familia cristaliza en el sistema cúbico con simetría $2-3$ y consta de una doble estructura de $Bi_{12}XO_{20}$ por celda unidad.

Este cristal no ha sido caracterizado, por tal razón para ésta aplicación fue necesario hacer una medida del ángulo de registro.

‡ Cámara CCD JVC 500 policromática.

‡ Televisor a color de $25'$.

‡ Cámara digital Canon PowerShot $A200$, de 2,1 Mega píxeles.

‡ Los divisores de haz son cubos 50/50.

‡ Las lentes son corregidas, con una distancia focal de $35cm$.

‡ Cristal liquido $XGA4$ de CRL-OPTO, ver especificaciones en la tabla 2.1 y en la figura 2.3.

‡ Material de Acetato y material de Plástico.

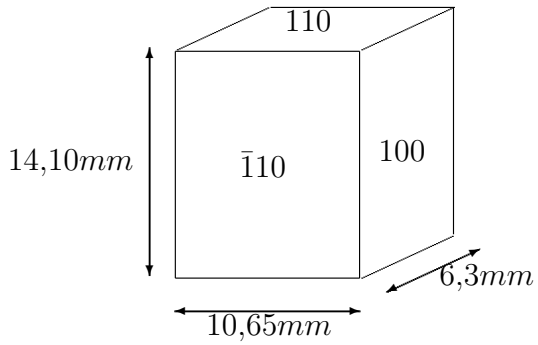


Figura 2.2: Ejes cristalográficos y dimensiones del cristal

$\lambda(\mu m)$	$\rho(deg/mm)$ BGO
0,50	41,5
0,55	30,8

Cuadro 2.1: Actividad Óptica

type	Active matrix TFT transmission mode panel using twisted nematic liquid crystal material.
Spatial resolution	1024 (horizontally) by 768 (vertically) monochrome pixels.
Pixel pitch	$14\mu m(H)$ x $14\mu m$ (V).
Pixel dimensions	$11\mu m$ (H) x $8{,}5\mu m$ (V).
Panel dimensions	Active area $14{,}33mm$ (H) x $10{,}75mm$ (V).
Transmission	14 % typical at $600nm$
Fill factor	40 % with opaque metal mask between pixels.
Contrast ratio	$> 100 : 1$

Cuadro 2.2: Especificaciones técnicas del cristal liquido

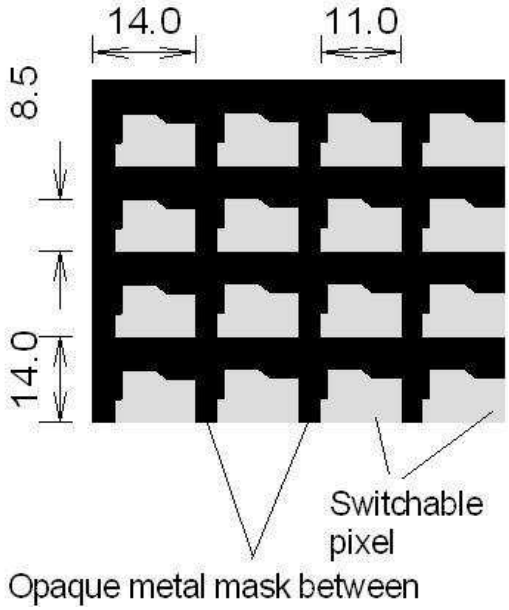


Figura 2.3: Dimensiones de los píxeles en μm

2.2. Inconvenientes en la configuración óptica

En la configuración óptica se presentaron tres problemas:

1. **Problema Energético**
   El origen del problema enérgetico está en que no se cuenta con un filtrado espacial apropiado para el $Nd : YVO_4$ de $50mW$ a $532nm$, el cual después de pasar por el filtrado espacial usado en la configuración emerge con una energía aproximadamente del 15 % de la energía efectiva de este láser.

   Teniendo en cuenta los esquemas de encriptación-decriptación por conjugación de fase, se tiene que la energía de los dos haces que intervienen en la etapa de registro es aproximadamente del 4 % de la energía incidente. Esto trae como consecuencia una baja sensibilidad

fotorrefractiva.

2. **Máscaras de fase aleatorias**
   Como consecuencia del problema enérgetico no pudo usarse el LCD para desplegar las máscaras de fase aleatoria debido a la alta absorción de este material, lo cual hace que se debilite aún más la energía de uno de los haces que interviene en el registro haciendo prácticamente nula la sensibilidad fotorrefractiva. Bajo estas condiciones se usan como mascaras dos materiales diferentes, uno de plástico y otro de Acetato.

3. **Adquisición de los datos**
   Debido a la baja energía presente en la configuración óptica, a la hora de adquirir el objeto recuperado por conjugación de fase, el sistema de adquisición con el que se cuenta no tiene la sensibilidad para detectar estas energías, por tal motivo fue necesario usar un televisor el cual tiene un sistema de amplificación que hizo posible ver la información recuperada. Para poder registrar la información se tomó una fotografía a la imagen desplegada en el televisor usando una cámara digital. Debido a esto no se puede calcular un error para de esta forma cuantificar los resultados obtenidos.

2.3. Encriptación

Para obtener la señal encriptada según la figura 2.4, es necesario llevar a cabo dos transformaciones de Fourier fraccional, una de orden α sobre el objeto O y otra de orden β sobre el producto $f_\alpha(O)$ y la máscara de fase aleatoria M, obteniéndose a la salida la señal encriptada (P_β).

Para registrar la señal encriptada en el cristal fotorrefractivo es necesario hacer interferir el haz objeto h_o con el haz de referencia h_r, siendo h_o el haz que lleva la información de la señal encriptada y h_r una onda plana que incide sobre el cristal con un ángulo θ.

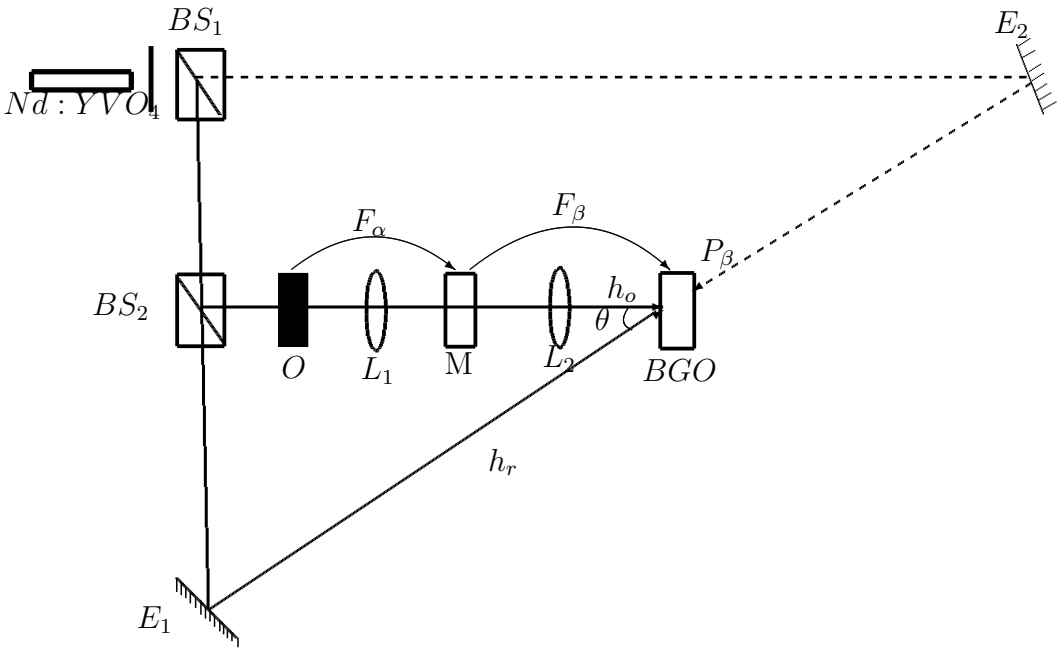


Figura 2.4: Configuración óptica para encriptación

2.4. Decriptación

Después de crearse la red en el cristal fotorrefractivo, por la interferencia de h_o y h_r, se procede a recuperar la información registrada iluminando el cristal con el haz conjugado $-h_r$, como en la figura 1.6. Siguiendo la evolución del campo conjugado el haz que se difracta en la dirección objeto sufre una transformación de Fourier fraccional de orden $-\beta$, luego es multiplicado por la máscara de fase aleatoria M y por último una transformación de Fourier fraccional de orden $-\alpha$. Con la ayuda de SLM se recupera el conjugado del objeto O^* sobre la CCD.

De las configuraciones ópticas para encriptación-decriptación, se aprecia que el sistema óptico opera en dos direcciones, de izquierda a derecha funciona como sistema de encriptación y de derecha a izquierda funciona como sistema de decriptación. Esto ocurre como consecuencia de lo demostrado en la ecuación 1.27.

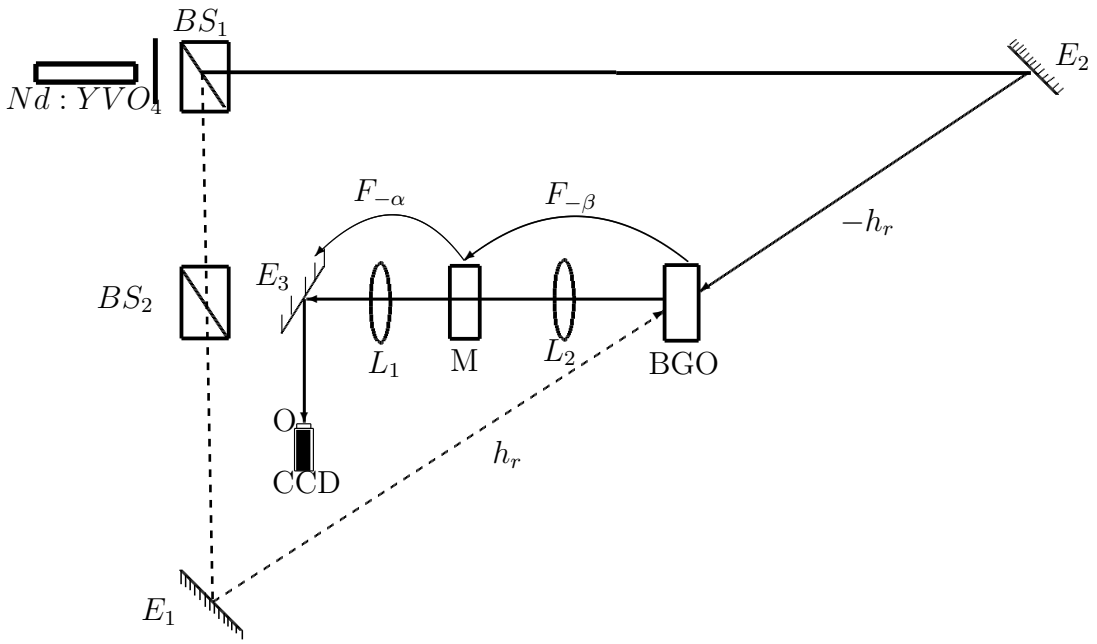


Figura 2.5: Configuración óptica para decriptar

Capítulo 3

Resultados

En este capitulo se presentaran los resultados obtenidos, de la siguiente manera:

‡ Resultados análisis máscaras de fase aleatorias.

- Simulaciones.
- Resultados Experimentales.
- Análisis de Histogramas de cada una de las máscaras.
- Cálculo de Error para las máscaras respectivas.

‡ Resultados del sistema de encriptación-decriptación por conjugación de fase.

- Simulaciones teniendo en cuenta la existencia de la transformación de Fourier fraccional inversa.
- Resultado del sistema óptico por conjugación de fase sin usar máscaras.
- Resultados experimentales proceso de Encriptación-Decriptación.
- Objetos no recuperados en el proceso de Encriptación-Decriptación.

3.1. Simulación de Máscaras de fase aleatorias

El objetivo de este estudio es definir de forma apropiada las máscaras de fase aleatorias a usar en las configuraciones ópticas de encriptación-decriptación. Con tal fin se emplea un mecanismo para verificar si la máscaras de fase aleatorias logran cambiar la información proveniente del objeto hasta el punto de no reconocerse este como tal. Dicho mecanismo consiste en verificar que en el plano imagen del objeto la información se encuentre encriptada, garantizando de esta forma que en ningún otro plano se obtenga información del objeto.

Para crear las máscaras de fase aleatorias se usa el generador de números seudo-aleatorios de *Matlab*, el cual permite adicionar diferentes tipos de ruido, y así seleccionar las máscaras de fase que ofrezcan mejores resultados según el mecanismo propuesto.

En la simulación se usó ruido de tipo *speckle*, *gausiano*, y ruido de tipo *rand*, este ruido es uniformemente distribuido con valores positivos entre 0 y 1, el orden fraccional empleado en la simulación es de 0.7.

3.1.1. Primer Conjunto de Máscaras

Para mostrar los resultados correspondientes a cada conjunto de máscaras, al lado izquierdo de cada figura encuentran las máscaras con sus respectivos valores de varianza V y al frente de cada una se encuentra la imagen encriptada.

Para este set de figuras se ha usado una función de ruido conocida como *speckle*, este tipo de función admite dos parámetros, varianza V y valor medio M, su forma explícita es:

$$J = I + n * I$$

I: Imagen a la cual se le adiciona ruido.
n: Numero aleatorio uniformemente distribuido con media M cero y varianza V.

Las mascaras de fase se generan usando este ruido al cual se le ha variado V de 1 hasta 10. En la figura 3.2 se muestran los resultados obtenidos ubicándose en el plano imagen del objeto para evaluar de esta forma la efectividad de las máscaras.

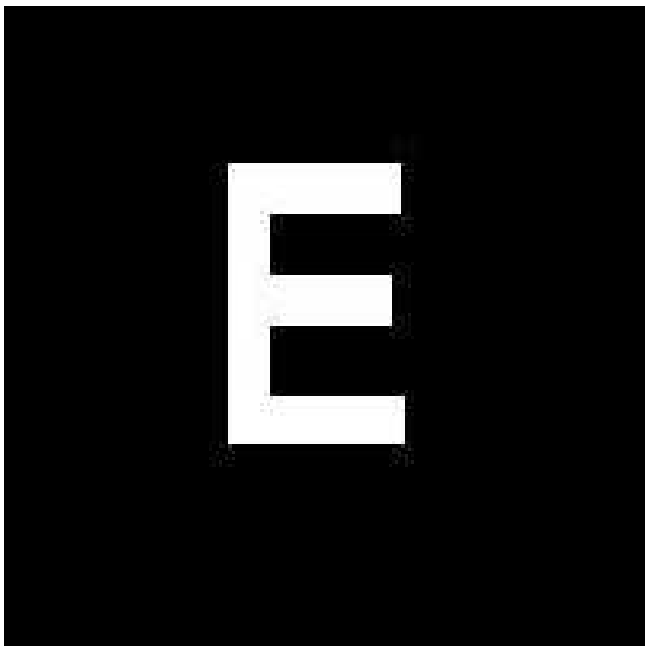


Figura 3.1: Objeto usado en el proceso de simulación.

3.1.2. Segundo Conjunto de Máscaras

En este set de máscaras se usa ruido del tipo speckle, variando el parámetro de varianza V de 0.1 hasta 1.0. Los resultados mostrados en la figura 3.3, corresponden a valores de varianza de

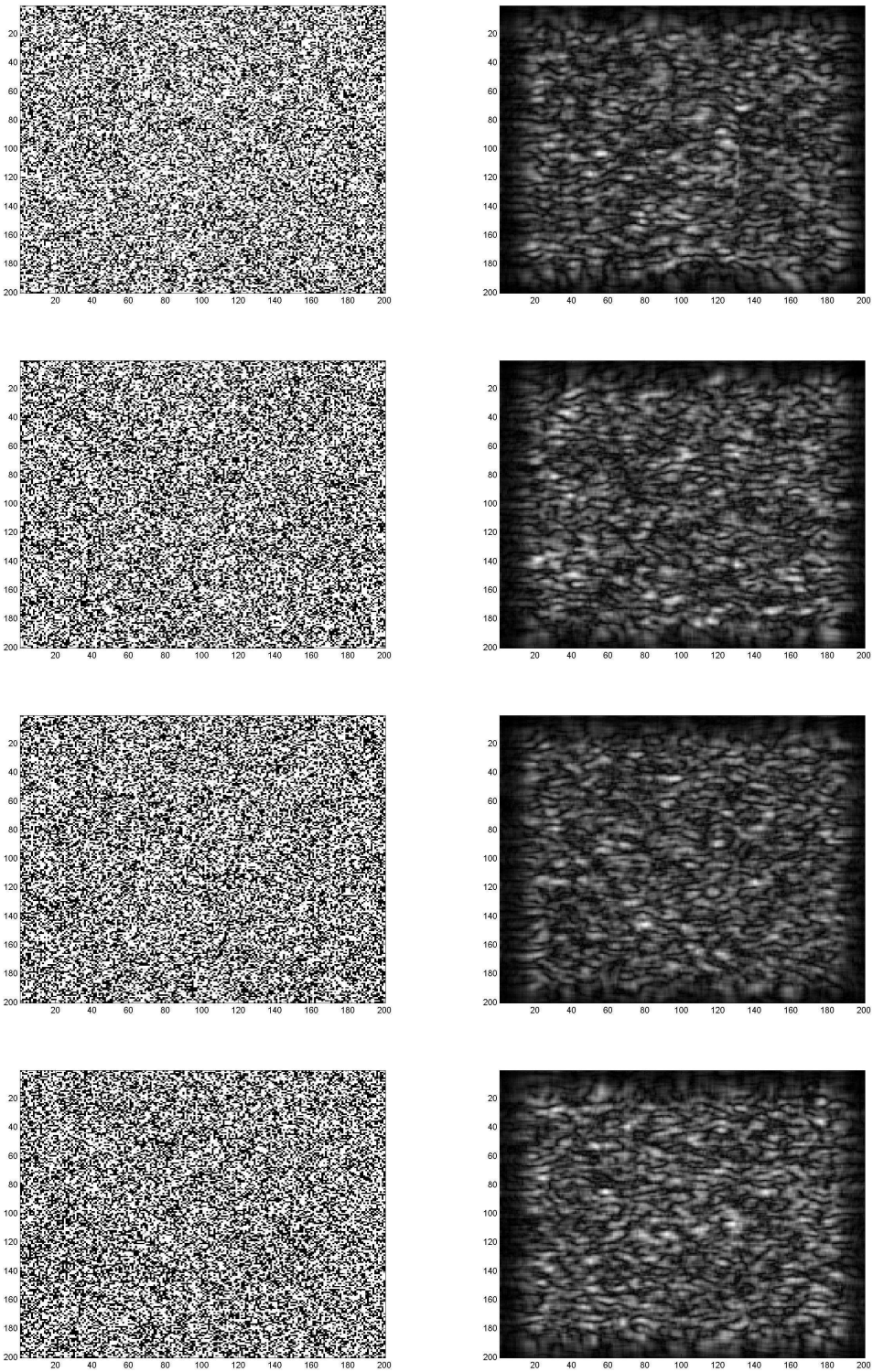


Figura 3.2: Al lado izquierdo se muestra la máscara y al lado derecho se muestra la imagen encriptada.

0.2, 0.5, 0.7, y 1.0.

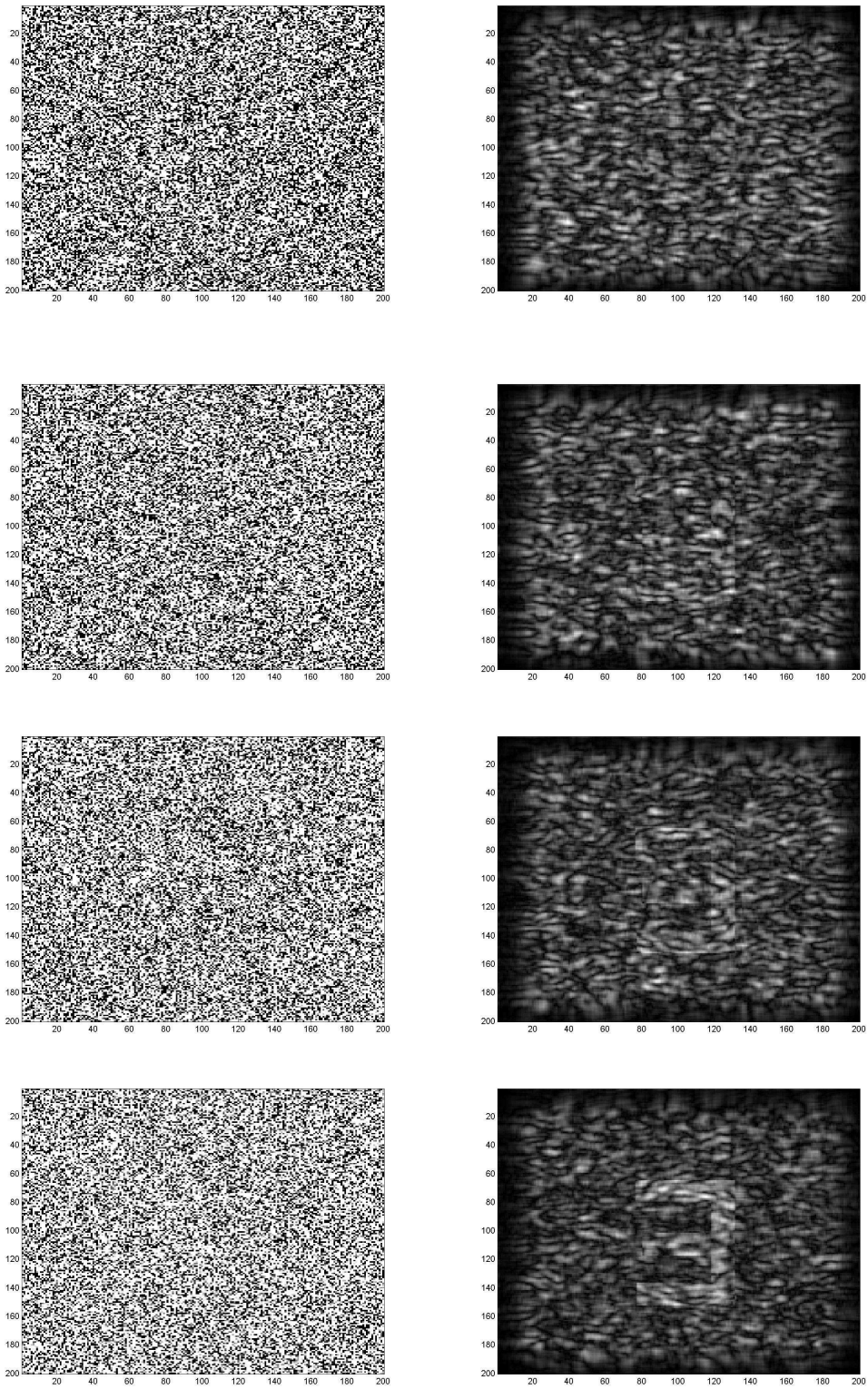


Figura 3.3: A la izquierda de la figura se muestra la máscara y al lado derecho la imagen encriptada.

3.1.3. Tercer Conjunto de Máscaras

Las mascaras aleatorias se generan usando la función *rand*. Esta función genera numeros aleatorios positivos entre 0 y 1 uniformemente distribuidos. Los resultados se muestran en la figura 3.4.

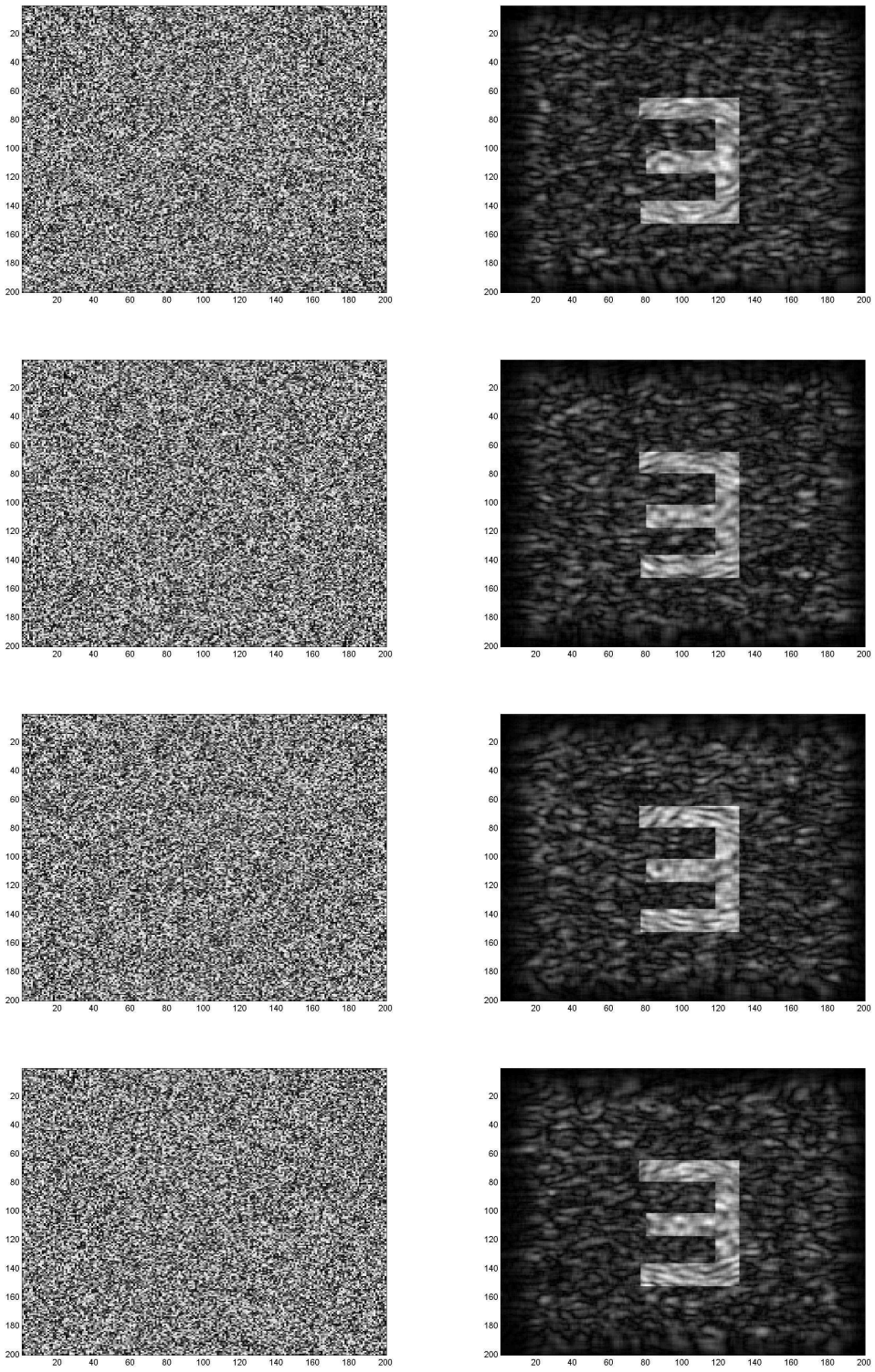


Figura 3.4: Máscaras usando la función *rand* de *Matlab*

3.1.4. Cuarto Conjunto de Máscaras

En este set se ha usado ruido tipo *Gausiano*. Esta función admite dos parámetros, valor medio M y varianza V, para este grupo de imágenes se usa el valor de $M = 0$ y se varia V de 1 hasta

10, ver figura 3.5, los valores de la figura corresponden a varianzas 2.0, 5.0, 7.0 y 10.

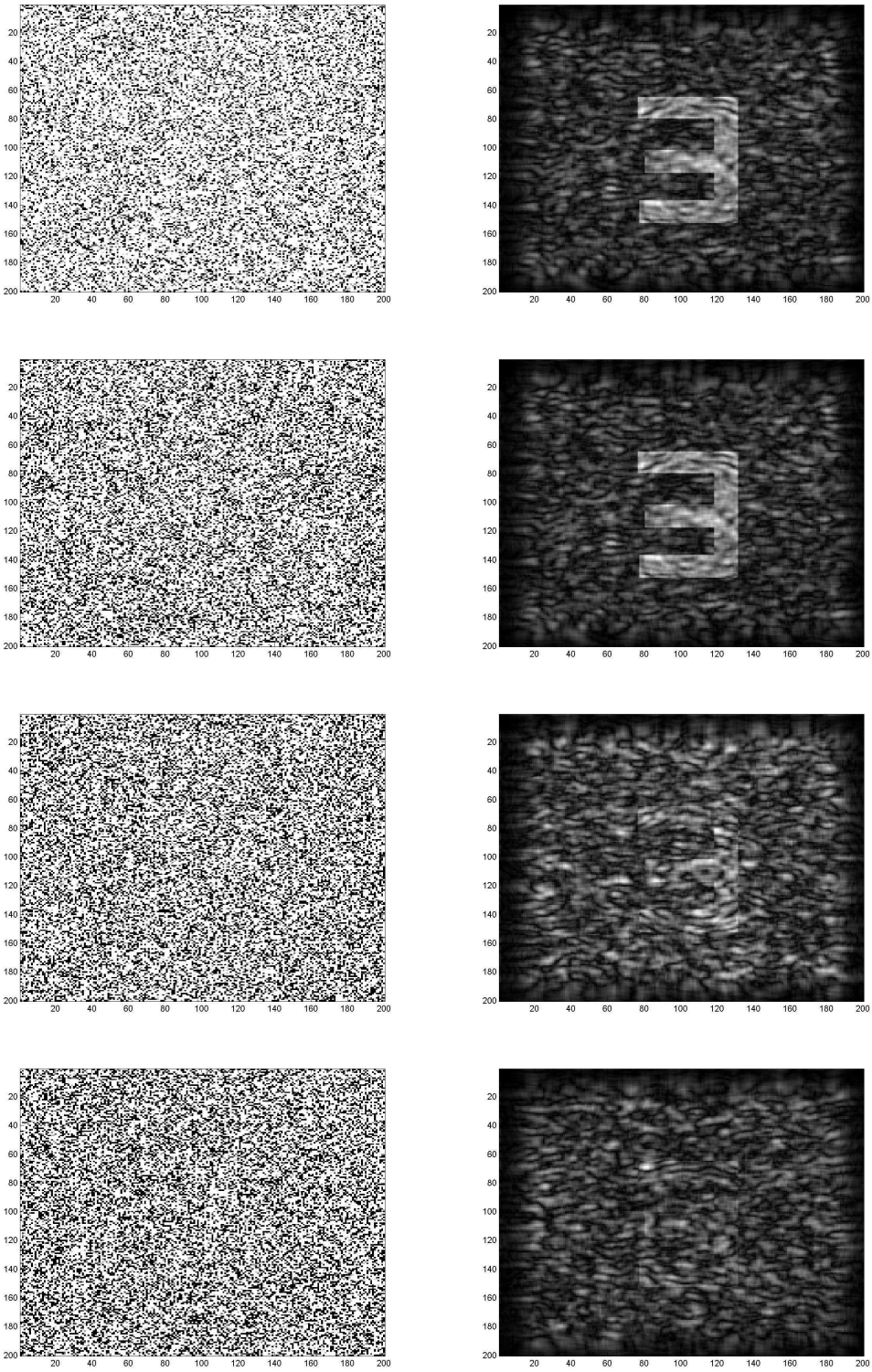


Figura 3.5: Al lado izquierdo de la figura se encuentra la máscara y al lado derecho la imagen encriptada.

3.1.5. Conclusiones proceso de simulación de máscaras

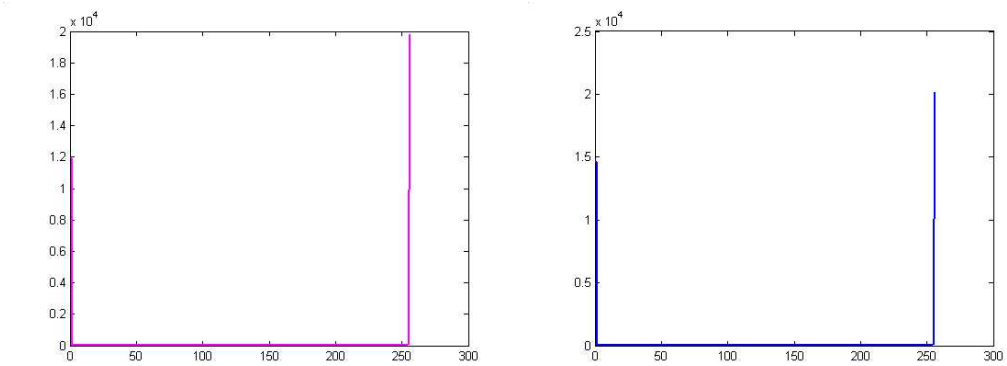
Los resultados arrojados por la simulación indican que no es indistinto el uso de las mascaras de fase aleatorias.

Se hace un análisis de histograma para ver que diferencia hay en la distribución de niveles de gris.

3.1.6. Histogramas

El objetivo de estudiar los histogramas de los diferentes tipos de mascaras es justificar por que sólo algunas máscaras responden adecuadamente según el tipo de función que se use para generarlas.

La parte izquierda de la figura 3.6, muestra los histogramas de las máscaras generadas usando ruido del tipo *speckle* con V igual a 2, 5, 7 y 10, en este orden, el lado derecho corresponde al histograma de las máscaras con valores de V igual a 0.2, 0.5, 0.7, 1.



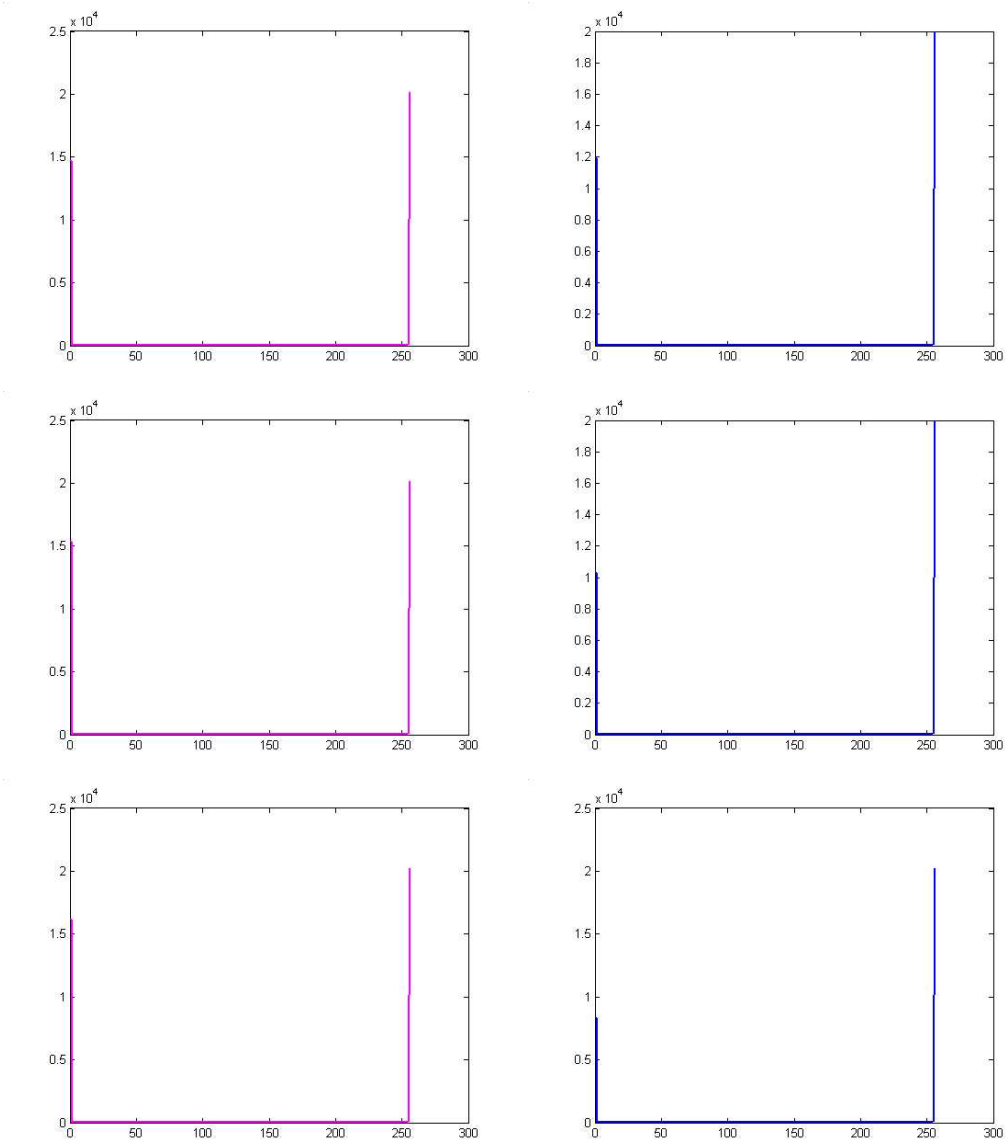


Figura 3.6: Histogramas de mascaras tipo *speckle*

En la tabla 3.6 se muestran los resultados arrojados por los histogramas de las mascaras generadas usando la función *speckle*.

Como se había mencionado en la sección 3.2.4 las máscaras que ofrecen mejor respuesta son las generadas usando ruido del tipo *speckle* con valores de $V = 5, 7, 10$. La razón de este comportamiento es que este tipo de máscara es prácticamente una máscara aleatoria binaria. Este mismo comportamiento también lo exhibe la máscara con $V = 0.2$, lo cual lleva a concluir que una máscara que obedezca a este comportamiento siempre va a permitir encriptar la información.

En la tabla 3.1.6 se muestra el numero de veces que se encuentra en la máscara el nivel de gris 0 y 255.

Número de histograma	Varianza	Nivel de Gris 0 Número de veces presente en la imagen $*10^4$	Nivel de Gris 255 Número de veces presente en la imagen $*10^4$
1	2	1,2	1,9798
2	0,2	1,4687	2,0
3	5	1,5	2
4	0,5	1,2	2
5	7	1,5	2,0
6	0,7	1,0334	1,9891
7	10	1,6227	2,0
8	0,1	0,8	2,0

Cuadro 3.1: Resultados histogramas para máscaras *speckle*

3.1.7. Histogramas correspondientes a máscaras de tipo *gausiano*

La figuras 3.7 corresponden a histogramas de las mascaras generadas con la función *gaussian* de *matlab* con valores de varianza V igual a 2,5,7 y 10.

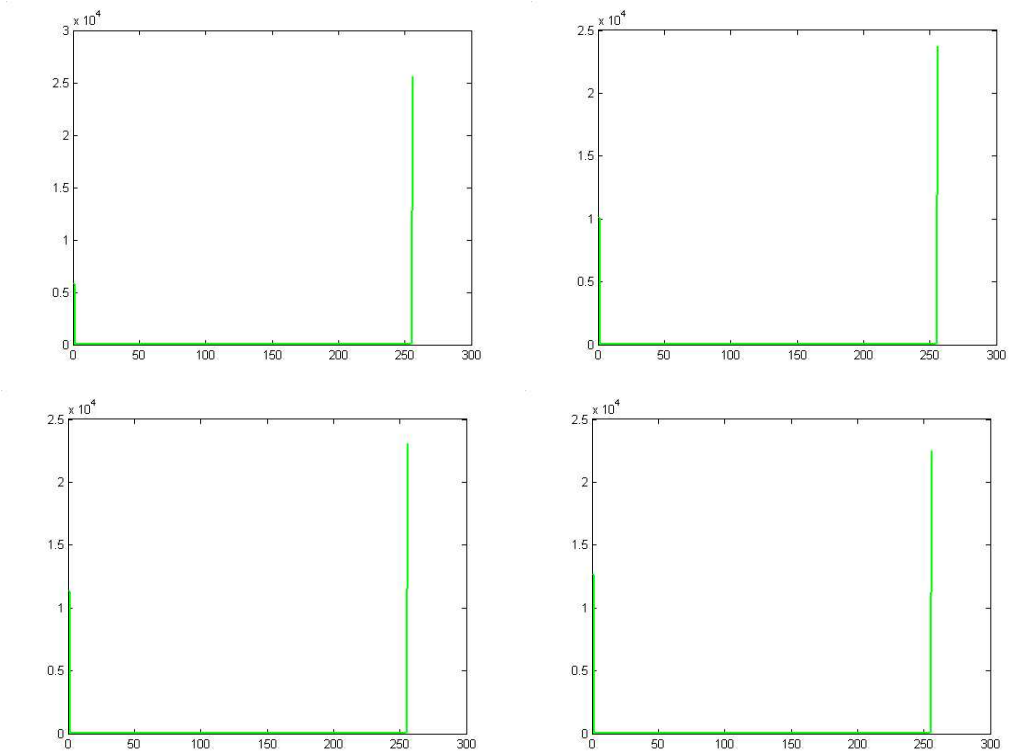


Figura 3.7: Resultados histogramas para máscaras usando la función *gaussian*

Con base en estos histogramas y en los valores reportados en la tabla 3.1.7 se aprecia que para

valores de $V = 2$ y 5 hay una alta contribución del nivel de gris 255 en la mascara, lo cual indica que estas máscaras no son binarias. Caso contrario ocurre para el valor de $V = 10$ donde hay una alta contribución tanto del nivel de gris 0 como del 255, hecho que concuerda con las simulaciones. Esto corrobora lo expuesto en el análisis de histograma para máscaras del tipo *speckle*.

Número de histograma	Varianza	Nivel de Gris 0 Número de veces presente en la imagen	Nivel de Gris 255 Número de veces presente en la imagen
1	2	5875	25560
2	5	1009	23691
3	7	11382	23048
4	10	12716	22448

Cuadro 3.2: Resultados histogramas para máscaras usando la función *Gaussian*

3.1.8. Histogramas correspondientes a máscaras usando la función *rand* de *Matlab*

Estos histogramas muestran que en la máscaras todos los niveles de gris de 0 a 255 están presentes en la imagen con igual probabilidad de ocurrencia. Por tal razón en la figura 3.8 se muestra un histograma como ejemplo.

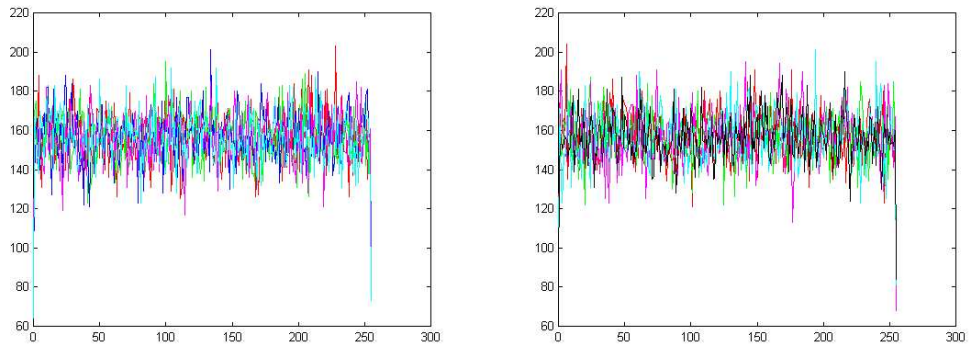


Figura 3.8: histogramas usando la función *rand*

Una de las razones que permite que las máscaras generadas usando ruido *speckle* permitan encriptar la imagen es la variación de V. La variación de este parámetro permite de cierta forma que en las máscaras haya una mayor ocurrencia del nivel de gris 0 y 255, cosa que no ocurre con las máscaras generadas usando la función *rand*, debido a que esta función no se le puede variar ningún parámetro.

3.2. Cálculo de Error

Se calcula el error cuádratico medio entre la imagen de entrada y la imagen encriptada, en función de la Varianza y del orden fraccional para las mascaras generadas con ruido del tipo *speckle* y *gausiano*. Para las mascaras del tipo *rand* se calcula el error en función del orden fraccional. De acuerdo a estos resultados de error se puede establecer un rango en el cual se obtiene la información encriptada.

3.2.1. Curvas de error para máscaras generadas usando ruido del tipo *speckle*

Para cada valor de varianza de 0.1-10, se realiza una curva de Error cuádratico medio Vs. Orden fraccional, este último se varia de $0-1$, en la parte superior de la figura 3.9 se muestran dos curvas: una con varianza 0,6 y la otra con varianza de 0.7. En la parte inferior izquierda de esta misma figura se muestra una curva de Error promedio Vs. Varianza y al lado derecho la gráfica Varianza Vs. Orden fraccional. De esta última curva se obtiene el rango en el cual la información se encripta. Para realizar esta curva se tiene en cuenta a partir de que orden

fraccional se empieza a obtener la imagen encriptada hasta el orden en el cual deja de estar encriptada, ver figura 3.9.

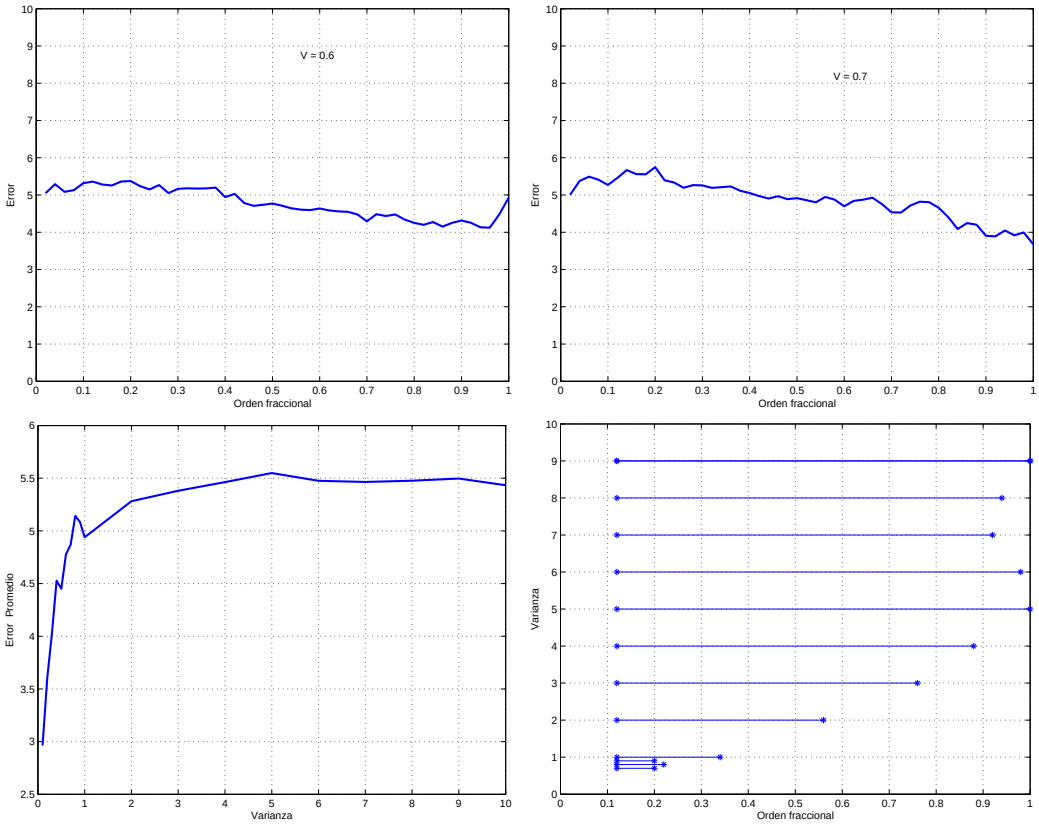


Figura 3.9: Curvas de error para ruido del tipo *speckle*

La curva de la parte superior izquierda corresponde a una varianza de 0.6; el comportamiento de esta curva es muy similar a las obtenidas para varianzas de 0.1 hasta 0.5; ya que para estas varianzas no se obtiene la imagen encriptada para ningún orden fraccional. La curva de la parte superior derecha corresponde a una varianza de 0.7. Es a partir de esta curva que se empieza a obtener un rango de ordenes fraccionales para los cuales se tiene la imagen encriptada.

De la curva inferior izquierda se aprecia el efecto de la varianza en el error, para una varianza de 5.0 se obtiene el máximo en el error promedio y a partir de este valor de varianza el comportamiento de la curva se mantiene prácticamente constante, lo cual indica que para este rango de varianzas se puede obtener la imagen encriptada, que se corrobora en la curva inferior izquierda, comportamiento que se había predicho usando los histogramas.

En la figura inferior derecha se muestra el rango de ordenes fraccionales para los cuales se obtiene la imagen encriptada, se aprecia que para valores de varianza de 5, 9 y 10 se obtiene un amplio rango dinámico de ordenes fraccionales para los cuales se obtiene la imagen ecriptada.

3.2.2. Curvas de error para máscaras generadas usando la función *gaussian* de *Matlab*

Para realizar estas curvas se toman valores de varianza de $1-10$, para cada uno de estos valores se gráfrica el error cuádratico medio Vs. orden fraccional, para la otra curva se calcula el error cuádratico promedio Vs. varianza, ver figura 3.11.

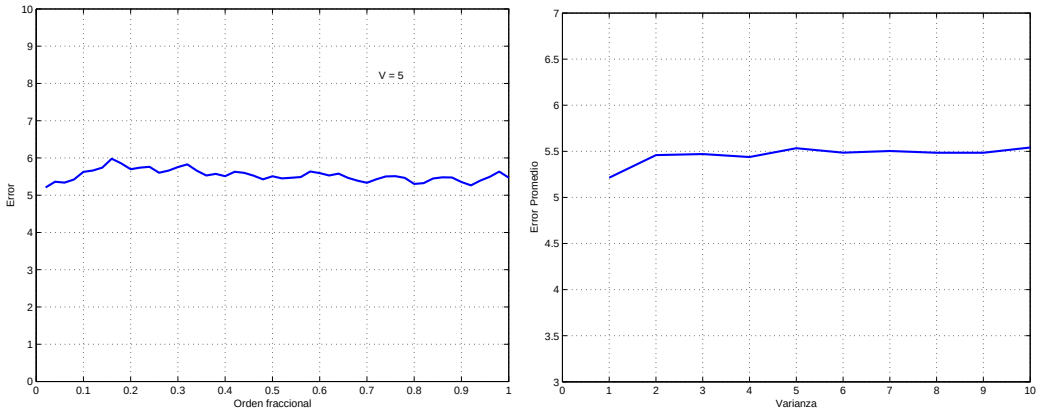


Figura 3.10: Curvas de error para ruido del tipo *gaussian*

Las curvas de error Vs. orden fraccional para cada una de las varianzas son de forma similar a la curva del lado izquierdo de la figura. A pesar de que los errores reportados por estas curvas se encuentran son similares a los obtenidos en las curvas de error usando ruido del tipo *speckle*, no es posible obtener la imagen encriptada en ningún orden fraccional.

3.2.3. Curvas de error para máscaras generadas con ruido del tipo *rand* de *Matlab*

Estas curvas se obtienen generando 10 mascaras usando ruido del tipo *rand*. Para cada una de estas curvas se calcula el error cuádratico medio Vs. orden fraccional, ver debajo 3.11.

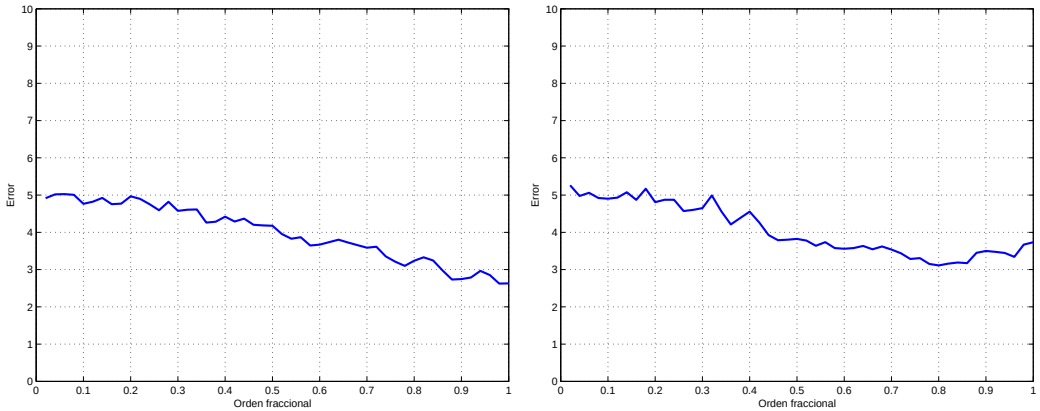


Figura 3.11: Curvas de error para ruido del tipo *rand*

Estas curvas indican que para ordenes fraccionales cercanos a cero es cuando tienen el máximo valor de error, lo cual implica que para estos ordenes hay la posibilidad de obtener la imagen encriptada, pero no hay un rango de ordenes fraccionales para los cuales se obtenga la imagen encriptada.

3.3. Resultados experimentales del uso de las máscaras de fase aleatorias

En este experimento se busca corroborar lo simulado respecto al uso de las máscaras de fase aleatorias, usando el mismo citerio empleado en las simulaciones para verificar la efectividad de las máscaras.

En el experimento se usa una pantalla de cristal líquido (LCD), marca $CRL - OPTO$ modelo $XGA4$, la cual interfasada con un PC permite desplegar las máscaras de fase aleatorias calculadas en la sección 3.1.

El objeto usado en el experimento es una letra E, transformada un orden fraccional 0.68, y multiplicada en el dominio fraccional por cada una de las máscaras usadas en la simulación, ver figuras 3.12 a 3.14. Para las máscaras del tipo speckle se usaron valores de varianza de 0.2, 0.5, 0.7 y 1.0, para las máscaras de tipo gausiano se usan valores de varianza V de 0.2, 0.5, 0.7 y 1.0. Para cada una de las máscaras se muestra el plano imagen.

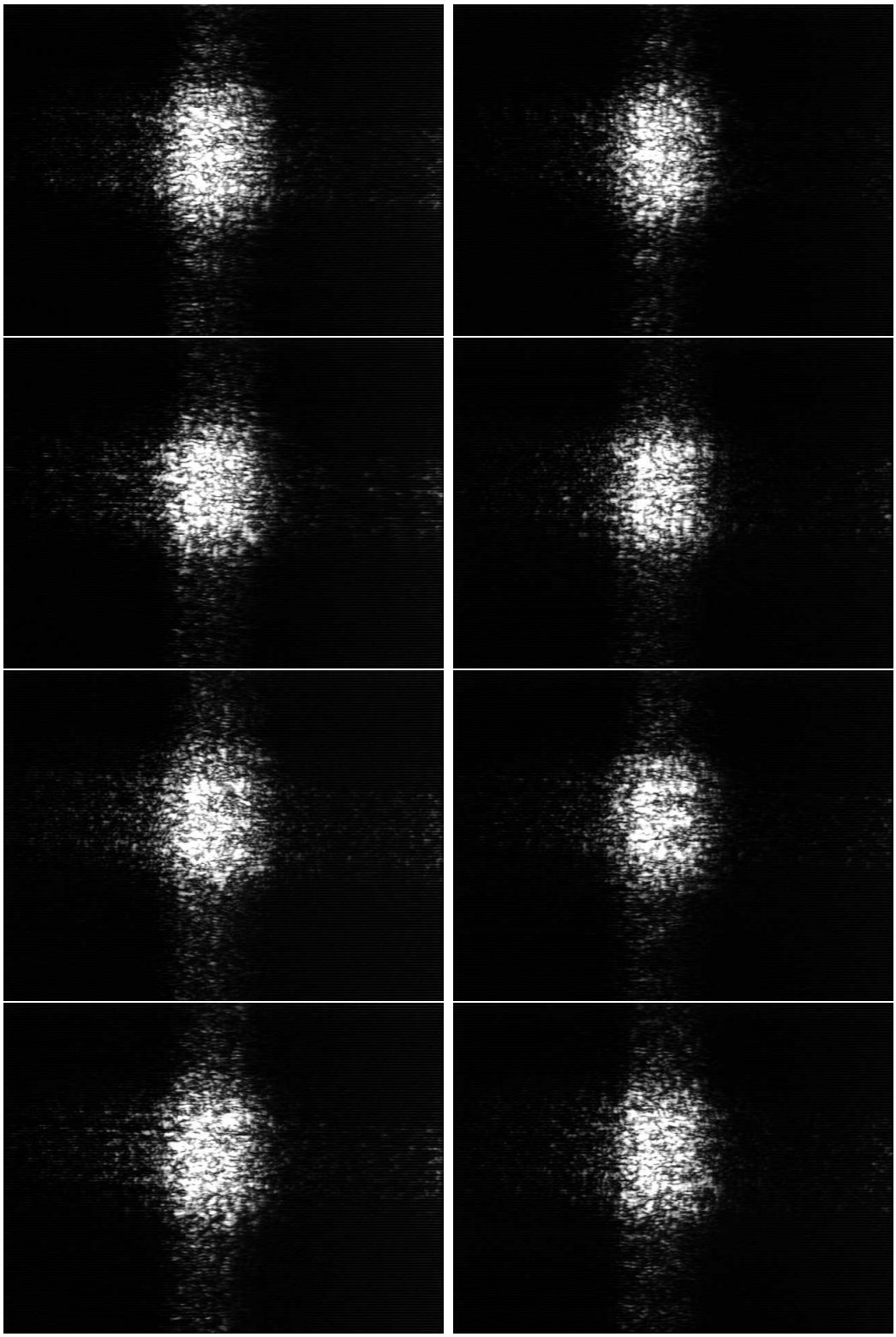


Figura 3.12: Ruido *speckle*: lado izquierdo V = 2-10, al lado derecho con V = 0.2-1

En estos resultados experimentales las máscaras que mejor funcionan son las generadas usando

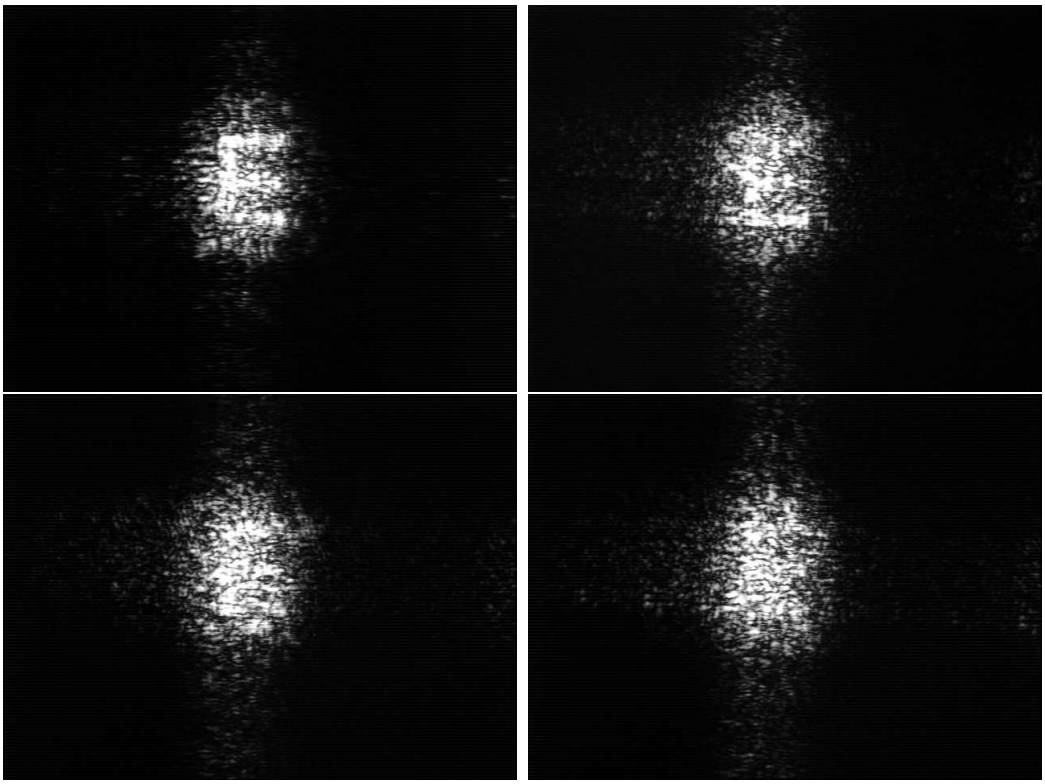


Figura 3.13: Plano imagen máscaras tipo *Gauss*

la función *speckle* con valores de $V = 5, 7, 10$. La fase que introducen este tipo de máscaras es suficiente para cambiar la información del objeto, para las máscaras generadas con otros ruidos no se logra encriptar el objeto.

Las simulaciones y el tratamiento experimental concuerdan en gran medida, por lo tanto se corrobora que la naturaleza de las máscaras obedece a lo ya visto en la simulaciones, es decir, que su elección no puede ser arbitraria.

3.4. Simulación Digital del comportamiento en Conjugación de Fase

Con base en el resultado obtenido en la ecuación (1.27) se realiza una simulación numérica para verificar lo demostrado.

Se toma una letra de $200 * 200$ píxeles, la cual es transformada un orden fraccional $p_1 = 0{,}5$, el resultado se multiplica por una máscara de fase aleatoria y al resultado de este producto se le efectúa una transformación de Fourier fraccional de orden $p_2 = 0{,}7$, por último se toma el conjugado de este resultado y se procede a recuperar el objeto.

En la parte superior izquierda de la figura 3.15 se muestra el objeto de interés, en la parte derecha se muestra la máscara de fase aleatoria, en el lado inferior izquierdo se muestra el objeto encriptado conjugado y al lado derecho se muestra el objeto recuperado.

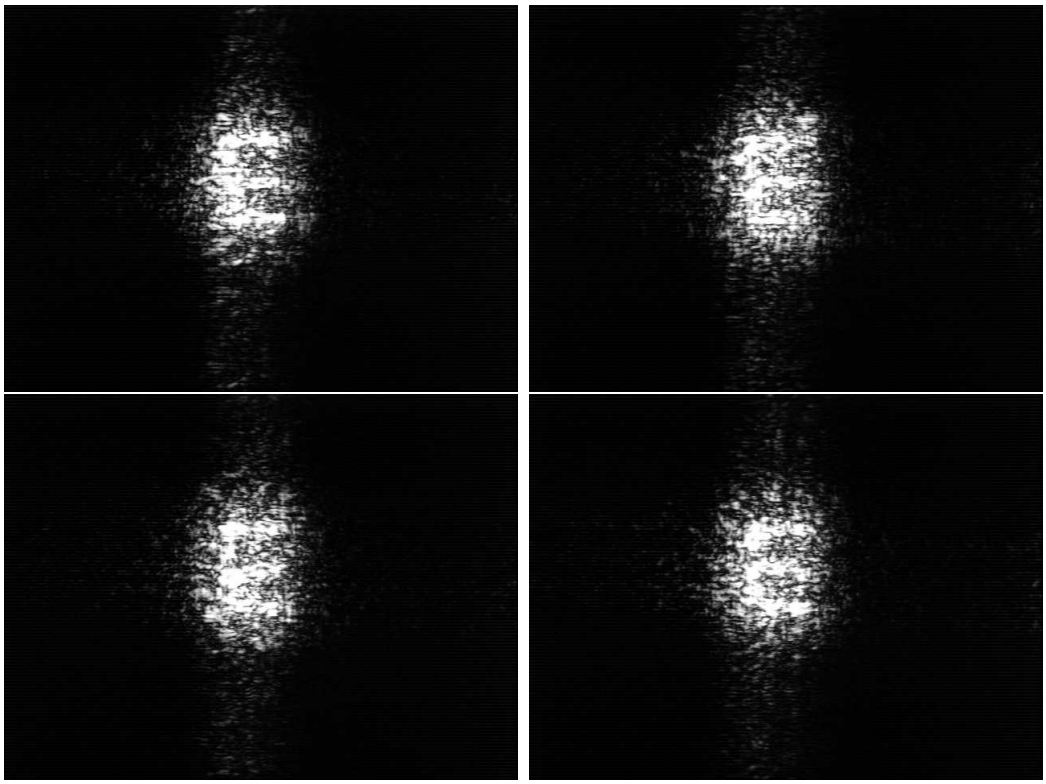


Figura 3.14: Plano imagen máscaras tipo *rand* de Matlab

El algoritmo digital que se usa para calcular las transformadas de Fourier fraccional se basa en la configuración Lohmann Tipo I.

El resultado de la simulación concuerda con lo predicho teóricamente, hecho que garantiza la realización de transformaciones de Fourier fraccional inversas. El error cuádratico medio entre el objeto de entrada y el objeto recuperado es igual a 0.6151. Con base en esto se propuso y se realizó la configuración óptica que lleva a cabo tanto el proceso de encriptación como el de decriptación ver la figura 2.1.

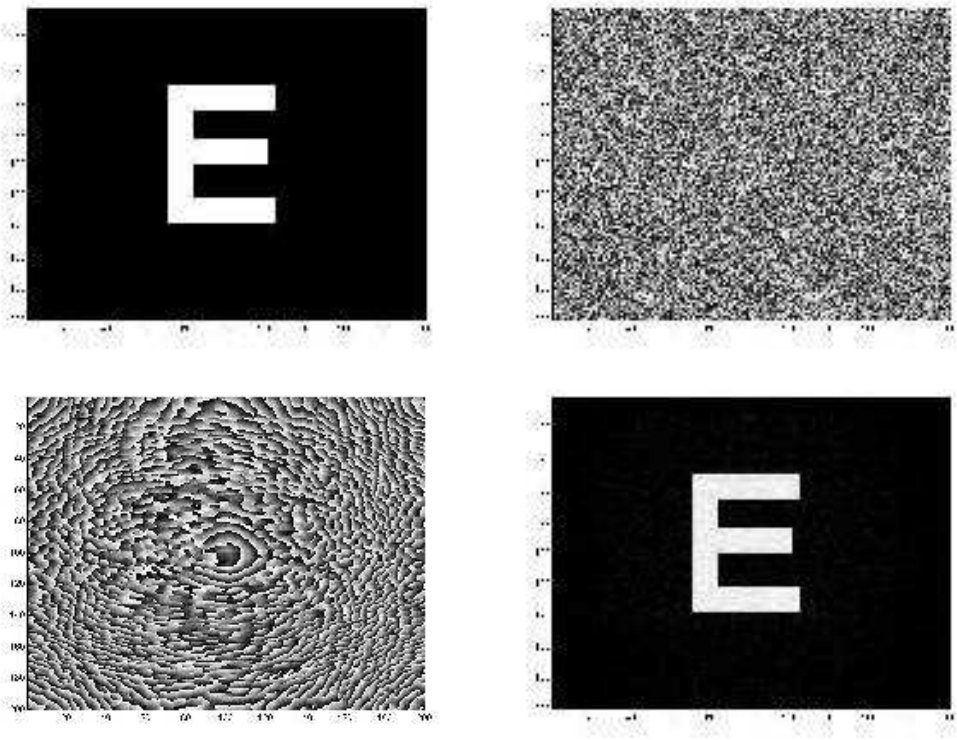


Figura 3.15: Simulación del comportamiento en conjugación de fase.

3.5. Respuesta del sistema por conjugación de fase

Se registra la imagen de una letra E sobre el cristal fotorrefractivo y luego se recupera por conjugación de fase, los resultados obtenidos se muestran en la figura 3.16.

De estas figuras se puede ver que se logra recuperar la información almacenada sobre el cristal por conjugación de fase.
En las figuras se aprecia un rayado", esto se debe a que las caras del cristal fotorrefractivo no están bien pulidas, este tipo de defectos se presentan en este cristal de BGO porque no fue fabricado industrialmente, dicho material fue fabricado por estudiantes hace más de 20 años.

3.6. Resultados del proceso de Encriptación-Decriptación

Teniendo en cuenta los esquemas ópticos propuestos en las figuras 2.4 y 2.5, se muestran los resultados de un letra A encriptada y su recuperación por conjugación de fase, ver figura 3.17. Con base en estos resultados se puede decir que la fase introducida por el material usado como máscara, en este caso material de Acetato, no alcanza a cambiar completamente la información del objeto [20].

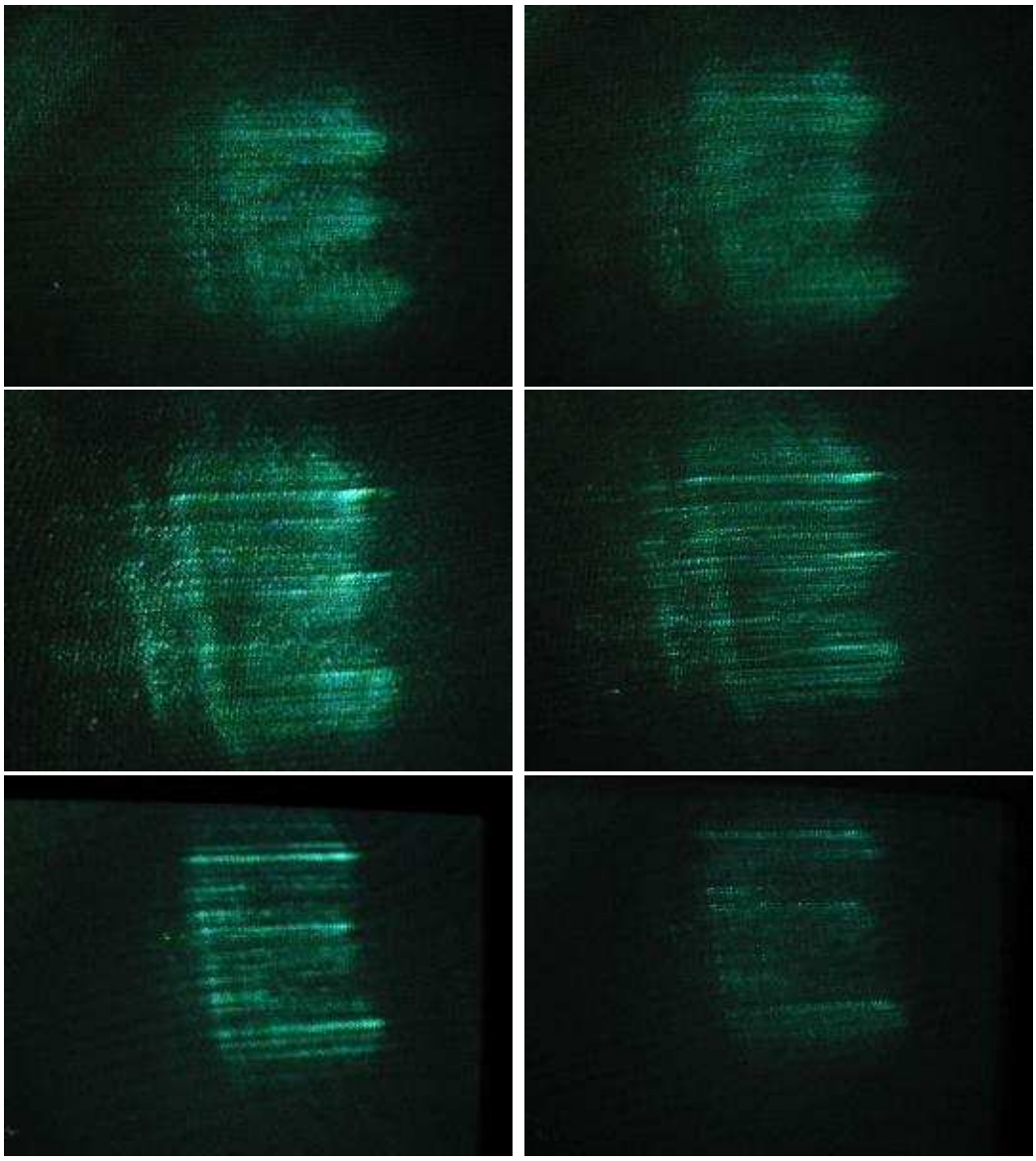


Figura 3.16: Lado izquierdo: Objeto no encriptado registrado sobre el cristal de BGO. Lado derecho: Objeto recuperado por conjugación de fase.

3.7. Ejemplos

El registro y recuperación de estos objetos en diferentes direcciones se hace con el fin de mostrar la fiabilidad del sistema, ver la figura 3.18. Para estos ejemplos se usó como máscara de fase el mismo material de Acetato usado en la sección precedente. La recuperación del objeto compuesto de tres letras es alentador, teniendo en cuenta el grado de dificultad que este representa debido a la información que contiene.

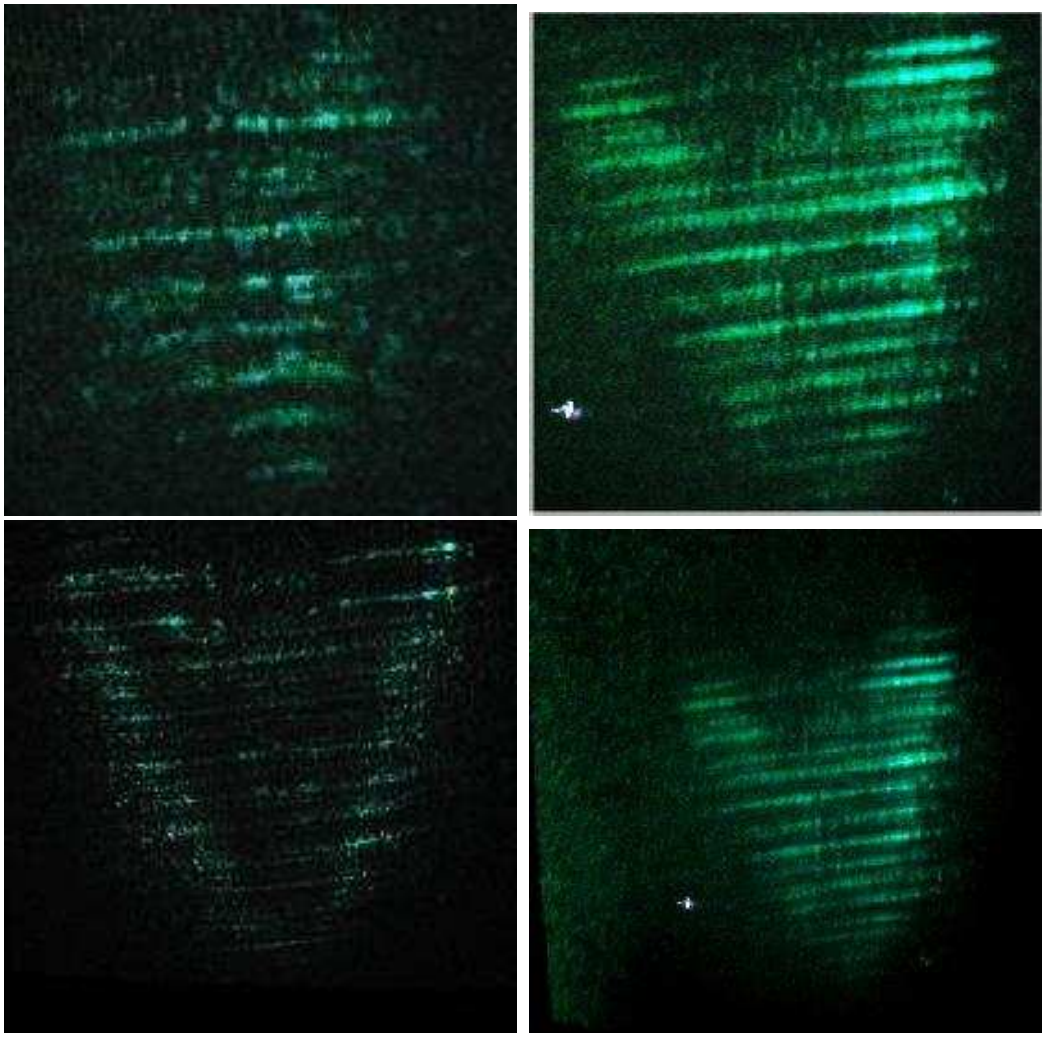


Figura 3.17: Lado izquierdo: Objeto Encriptado. Lado derecho: Objeto recuperado

3.8. Objetos no recuperados

En la parte superior izquierda de la figura 3.19 se muestra el objeto a encriptar, en la parte derecha de esta misma figura se muestra la imagen encriptada y en la parte inferior dos intentos de recuperación del objeto por conjugación de fase.
Teniendo en mente que el uso de las máscaras de fase aleatorias no es arbitrario de acuerdo al estudio realizado en la sección 3,3, se procede a probar con materiales que introduzcan cambios de fase aleatorios y además que sean transparentes. Es por esto que en estos ejemplos se usó como máscara de fase un material de plástico.
Por simple inspección de las figuras se concluye que el material usado como máscara de fase logra cambiar completamente la información del objeto. El objeto no se puede recuperar por conjugación de fase porque el material usado como máscara se comporta como un elemento difusor.

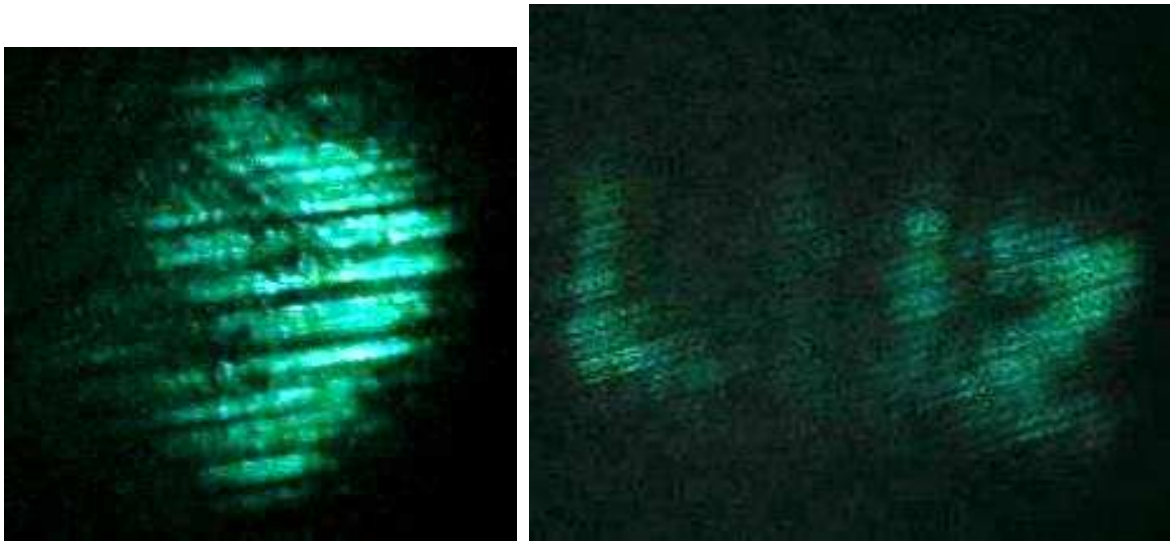


Figura 3.18: Recuperación de objetos con diferentes orientaciones

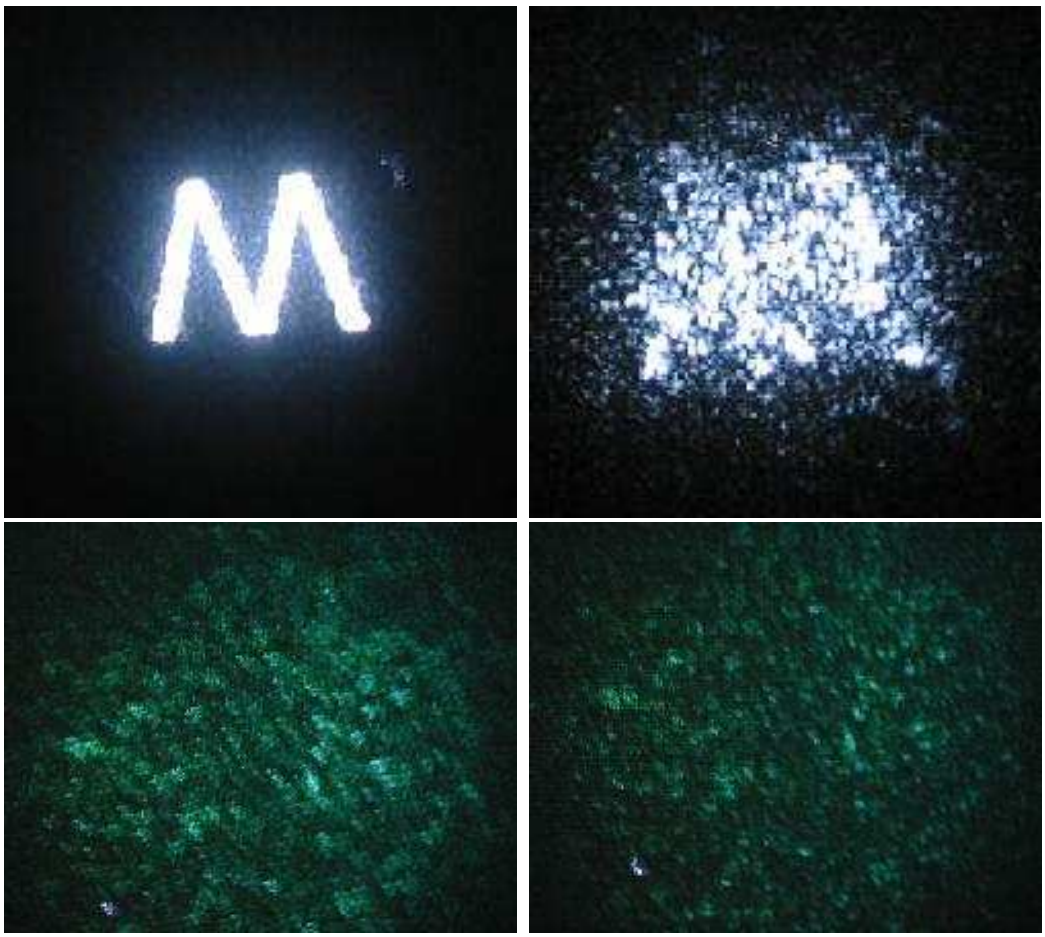


Figura 3.19: Ejemplo de intento de recuperación con otro tipo de máscara para encriptar.

Capítulo 4

Conclusiones

‡ En esta tesis se logra establecer que es muy importante la adecuada selección de las llaves para encriptación de señales en aplicaciones de seguridad.

‡ Se propone y se aplica un mecanismo para verificar la efectividad de las mascaras de fase, garantizando con esto que la imagen encriptada no pueda recuperarse en otro dominio fraccional.

‡ Usando el fenómeno de conjugación de fase se han realizado transformaciones inversas de Fourier fraccional ópticas.

‡ Con base en las transformaciones inversas se obtiene una misma configuración óptica que realiza el proceso de encriptación-decriptación.

‡ El Teorema del Escalamiento y del Corrimiento adicionan un grado de complejidad a sistemas de encriptación óptica.

4.1. Perspectivas

‡ Este tipo de sistemas de encriptación pueden aplicarse en comunicaciones ópticas creando un dispositivo óptico integrado que realice el proceso de encriptación y otro que realice el proceso de decriptación. Cada uno de estos dispositivos integrados se ubicarían a la salida de los ordenadores de los usuarios interesados en compartir información. Este sistema tendría una característica muy importante *los usuarios que comparten información no tendrían conocimiento de las llaves, simplemente comparten la informacíon sin ni siquiera saber que fue encriptada.*

‡ Buscar una técnica que permita establecer criterios contundentes que permitan dar un perfil de máscaras a usar en un proceso de encriptación. Un posible tratamiento es usar correlación.

Bibliografía

[1] S. Liu, L. Yu, B. Zhu, *Optical image encryption by cascaded fractional Fourier transfors with random phase filtering*, Optics Communications, Vol. 187, 57–63 (2001).

[2] B. Zhu, S. Liu, *Optical image encryption based on the generalized fractional convolution operation*, Optics Communications, Vol. 195, 371–381 (2001).

[3] Y. Zhang, C. Zheng, N. Tanno, *Optical encryption based on iterative fractional Fourier transform*, Optics Communications, Vol. 202, 277–285 (2002).

[4] Z. Lizarazo, R. Torres, Y. Torres, *Transformada de Fourier fraccional aplicada a la encriptación de señales*, VII Simposio de Tratamiento de Señales Imágenes y Visión Artificial, Bucaramanga (2002).

[5] N. Towghi, B. Javidi, Z. Luo, *Fully phase encrypted image processor*, J. Opt. Soc. Am. A, Vol.16, N°8, 1915–1927 (1999).

[6] P. Refregier, B. Javidi, *Optical image encryption based on input plane and Fourier plane random encoding*, Opt. Lett., Vol. 20, N°7, 767–769 (1995).

[7] L. Gonçalves, Y. Sheng, *Optical implementation of image encryption using random phase encoding* , Opt. Eng., Vol.35, N°9, 2459–2463 (1996).

[8] B. Javidi, G. Zhang, *Experimetal demostration of the random phase encoding technique for image encryption and security verification* , Opt. Eng., Vol.35, N°9, 2506–2512 (1996).

[9] B. Javidi, A. Sergent, G. Zhang, L. Guibert, *Fault tolerance properties of a double phase encoding encryption technique*, Optical Engineering, Vol. 36, N° 4, 992–998 (1997).

[10] B. Javidi, E. Ahouzi, *Optical security system with Fourier plane encoding*, Applied Optics, Vol. 37, N° 26, 6247–6255 (1998).

[11] Victor Namias, *The Fractional Fourier Tranform and it's aplication to quantum mechanics.* J. Inst. Maths Applics, **25**, 241–265, (1980).

[12] H. Ozaktas, Z. Zalevsky, M. Kutay, *The Fractional Fourier Transform*, Jhon Wiley & Sons Ltd, (2001).

[13] D. Mendlovic, H. Ozaktas, *Fractional Fourier transform and their optical implementetion: I*, J. Opt. Soc. Am. A., **10**, 1875–1881 (1993).

[14] H. Ozaktas, D. Mendlovic, *Fractional Fourier transform and their optical implementetion: II*, J. Opt. Soc. Am. A., **10** 2522–2531 (1993).

[15] A. Lohman, *Image rotation, Wigner rotation, and the fractional Fourier transform*, J. Opt. Soc. Am. A., **10**, 2181–2186 (1993).

[16] P. Pellat-Finet, G. Bonnet, Fractional order Fourier transform and Fourier optics, Opt. Comm, **111**, 141-154, (1994).

[17] P. Yeh, *Introduction to photorefractive nonlinear optics*, New York: John Wiley & Sons, Inc., (1993).

[18] L. Solymar, D. Webb, A. Grunnet-Jepsen, *The physics and applications of photorefractive materials*, New York: Oxford-University Press Inc., (1996).

[19] G. Unnikrishnan, J. Joseph, K. Singh, *Optical encryption system that uses phase conjugation in a photorefractive crystal*, Applied Optics, **37**, 8181–8186, (1998).

[20] Z. Lizarazo, Y. Torres, *Encriptación de Imagenes usando la transformada de Fourier fraccional*, Revista Colombiana de Fisica, 396-399, (2003).

[21] Z. Lizarazo, J. Cornejo, M. Sotaquirá, O. Gualdrón, *Métricas de desempeno para diferentes filtros en arquitecturas de correlación digital*, Revista Colombiana de Fisica, 400-402, (2003).