Bistua: Revista de la Facultad de Ciencias Básicas
Universidad de Pamplona
revistabistua@unipamplona.edu.co
ISSN (Versión impresa): 0120-4211
COLOMBIA

2005
Jorge Enrique Rueda / Ana Ludia Romero / Lina Mireya Castro
CRIPTOGRAFÍA DIGITAL BASADA EN TECNOLOGÍA ÓPTICA
Bistua: Revista de la Facultad de Ciencias Básicas, Julio, año/vol. 3, número 002
Universidad de Pamplona
Bucaramanga, Colombia
pp. 19-25

ISSN 0120 - 4211 Bistua Vol. 3 No. 2

CRIPTOGRAFÍA DIGITAL BASADA EN TECNOLOGÍA ÓPTICA

Jorge Enrique Rueda[1]
Ana Ludia Romero*
Lina Mireya Castro*

[1]Universidad de Pamplona, Facultad de Ciencias Básicas
Departamento de Física y Matemáticas
Grupo de Investigaciones en Optica&Plasma
E-Mail: jruedap2003@unipamplona.edu.co
* Semillero de Investigación del GIOP

.

RESUMEN

En este trabajo presentamos los resultados de la implementación de un algoritmo para cifrado digital de imágenes; el sistema está basado en un arreglo de filtrado espacial usando la transformada de Fourier y una llave de cifrado de solo fase. Se determinó los valores óptimos de distribución de la fase de la llave.

ABSTRACT

In this work, we present the results of the implementation of an algorithm of digital coding of images; the system is based on an arrangement of space filtrate using the Fourier transform and a coding phase only key. It was determined the optimal phase distribution values of the coding key.

INTRODUCCIÓN

El fraude y ataques a los sistemas informáticos son cada vez de mayor preocupación, siempre que las pérdidas por tales prácticas ilícitas implican incalculables pérdidas económicas, tanto a usuarios de sistemas financieros como a la banca misma, a estamentos gubernamentales, y en general a todas las empresas que manejan bases de datos a través de la Internet o cualquier otro medio de transporte de la misma. En el mundo de hoy, donde los avances tecnológicos en hardware y software para procesar imágenes y la alta resolución de los dispositivos periféricos de entrada y salida de datos de un ordenador digital, ha permitido que sea un problema simple reproducir cuadros, insignias, símbolos, billetes, tarjetas inteligentes, documentos de identidad, obras de arte, claves de acceso a base de datos privados, etc.

Actualmente, las tarjetas de crédito, licencias de conducción, cédulas de identidad, marcas de productos y los pasaportes utilizan hologramas como mecanismo de seguridad, pero la verificación la realiza el sistema de visión de un humano, que a pesar de su alta capacidad de proceso, es un sistema fácilmente vulnerable debido a que su funcionamiento es subjetivo, motivando a que un alto porcentaje de las copias falsas no sean detectadas y se mantengan en circulación.

Otra área donde la criptografía tiene impacto, es en las redes mundiales como la Internet y las redes telefónicas, a través de ellas se manejan grandes volúmenes de información confidencial: de tarjetas de crédito, de transacciones bancarias, corporativa y/o gubernamental, etc.

La implementación de sistemas de seguridad de la información, es un tema que cada día toma mayor importancia. Con la aparición de los ordenadores digitales, se inicia una amplia investigación, basada en la algoritmia matemática aplicada al cifrado de información; estas técnicas aun se mantienen en desarrollo y mejoramiento, pero las mismas se hacen vulnerables en la medida que los procesadores digitales se hacen cada vez más robustos, con capacidad para resolver problemas matemáticos de alta complejidad.

Desde la década de los noventa la tecnología óptica hace presencia en la construcción de arreglos de cifrado. En 1994 Javidi y Horner proponen el método para encriptación óptica de información que usa mascaras aleatorios de fase. A este trabajo han seguido otros que usan llaves ópticas aleatorios de fase en el plano de entrada y en el plano de Fourier, sistemas de encriptación cuando existe ruido y distorsión, patrones de speckle encriptados mediante máscaras de fase aleatorias y encriptación mediante conjugación de fase en un cristal fotorrefractivo (Javidi 1997; Tajahuerce 2000 - 2001; Rosen 2001; Mogensen 2001 - 2000; Matoba 2000; Nomura 2000; Sinha 2003; Rueda 2002), en entre otros; recientemente se presentó un método que usa la transformada wavelet (Linfei 2005).

MODELACION MATEMATICA

En la Fig.1 se muestra un diagrama de flujo de un sistema de cifrado óptico, en el cual basamos la modelación numérica. La implementación óptica se puede materializar mediante un arreglo de correlación Vander Lught (Goodman 1968; YU 1973 - 1996; Vander Lugt 1964).

El diagrama de flujo se describe matemáticamente como sigue:

Sea una función de valor real que representa la imagen que se quiere ocultar, entonces el proceso de encriptación convierte a esta función en ruido blanco y se realiza básicamente en tres pasos:

1. La imagen $f(x,y)$ se multiplica por una función de fase aleatoria $R(x,y)=\exp(i f(x,y))$, esto es: : $f(x,y)\cdot R(x,y)$.
2. La transformada de Fourier del producto anterior se multiplica por otra función de fase aleatoria $S(u,v)=\exp(i j(u,v))$ denominada la llave del proceso de encriptación, que es estadísticamente independiente de la primera función de fase aleatoria.
3. Cálculo de la transformada de Fourier inversa, así:

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

$f_c(x',y')$ representa una señal que lleva oculta la imagen de entrada $f(x,y)$. Las funciones $R(x,y)$ y $S(u,v)$ convierten a la imagen $f(x,y)$ en ruido blanco; el símbolo $*$ representa producto de convolución.

Etapa de decriptado de la imagen : $f(x,y)$:

1. Cálculo de la transformada de Fourier del conjugado de la señal encriptada $\{f_c(x',y')\}^*$, es decir:

$$F\left[\{f_c(x',y')\}^*\right]=F\{[f^*(x',y')\cdot R^*(x',y')]*S^*(x',y')\}=F[f^*(x',y')\cdot R^*(x',y')]\cdot F[S^*(x',y')] \quad (2)$$

2. Multiplicación del resultado Ec.(2) por la llave $S(u,v)$ utilizada en el proceso de encriptación:

$$F[f^*(x',y')\cdot R^*(x',y')]\cdot F[S^*(x',y')]\cdot S(u,v) \quad (3)$$

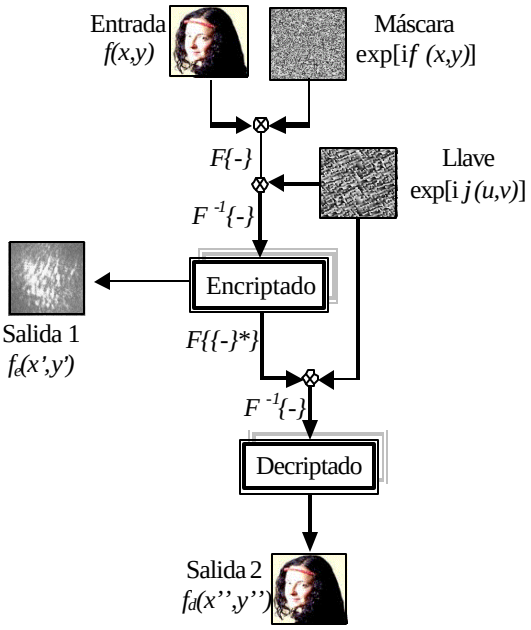


Figura 1. Flujograma de Encriptado-Decriptado mediante la Transformación de Fourier. {-}*: Complejo Conjugado; F{-}: Transformación de Fourier; F-1{-}: Transformación de Fourier Inversa;Ä: multiplicación.

3. Cálculo de la transformada de Fourier inversa del producto anterior Ec.(3):

$$f_d(x'', y'') = F^{-1}\{F[f^*(x', y') \cdot R^*(x', y')] \cdot F[S^*(x', y')] \cdot S(u, v)\} = [f(x'', y'') \cdot R^*(x'', y'')] * [S^*(x'', y'') \otimes S(x'', y'')] \quad (4)$$

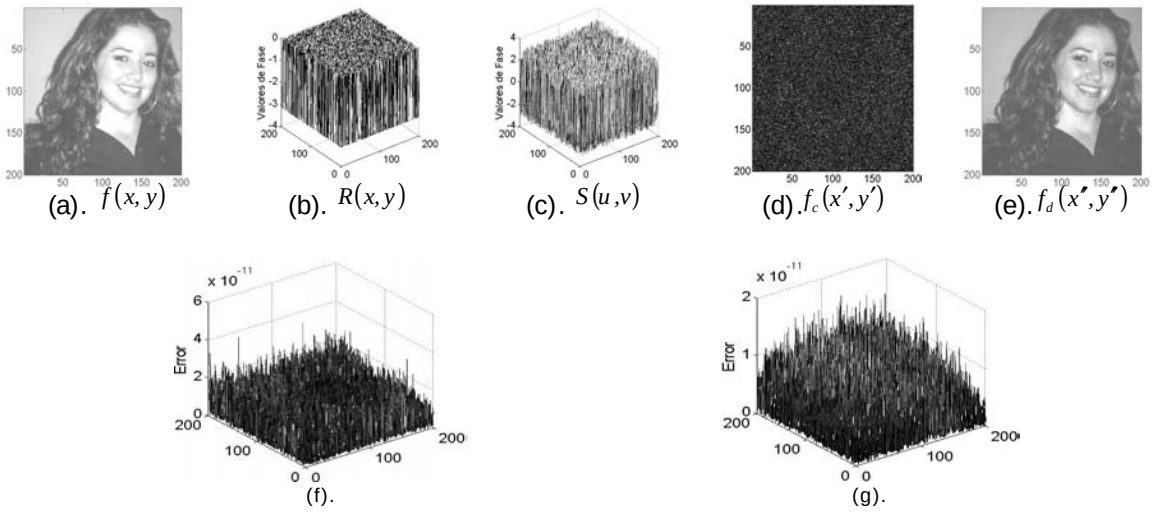
donde $\otimes$ significa producto de correlación. Si $f^*(x'', y'')$ es real, entonces $f^*(x'', y'') = f(x'', y'')$. Por otro lado, este resultado se interpreta como la recuperación de la señal $f(x'', y'')$, siempre que el factor de fase $R^*(x'', y'')$ desaparece en el momento de la detección, puesto que los sistemas de visualización son cuadráticos. Así que, finalmente se obtiene: $f_d(x'', y'') = [f(x'', y'') \cdot R^*(x'', y'')] * d(x'', y'')$ (5)

Se puede verificar que si la llave de decriptado es diferente a la de encriptado, digamos $\tilde{S}(u, v)$, entonces el resultado sería:

$$f_d'(x'', y'') = [f(x'', y'') \cdot R^*(x'', y'')] * [S^*(x'', y'') \otimes \tilde{S}(x'', y'')] \quad (6)$$

donde $\tilde{S}(x'', y'')$ es la transformada inversa de Fourier de $\tilde{S}(u, v)$. Es claro que el producto $S^*(x'', y'') \otimes \tilde{S}(x'', y'')$ genera una distribución de energía que produce una fuerte distorsión sobre la imagen $f(x, y)$ decriptada. Por otro lado, de estos resultados analíticos podemos verificar sin dificultad que este sistema de cifrado puede funcionar sin la mascara de entrada $R(x, y)$.

RESULTADOS Y DISCUSION



(a). $f(x, y)$ (b). $R(x, y)$ (c). $S(u, v)$ (d). $f_c(x', y')$ (e). $f_d(x', y')$ (f). (g).

Figura 2. Resultados de encriptamiento. (a). Imagen a encriptar; (b). Distribución de fase de la máscara; (c). Distribución de fase de la llave; (d). Imagen (a) encriptada; (e). Imagen (a) decriptada; (f) . Error en (e) multiplicando (a) por ruido blanco; (g). Error en (e) sin multiplicar (a) por ruido blanco.

El sistema de cifrado modelado matemáticamente se implementó en lenguaje Matlab. En las Figs.2-5 se muestran los resultados numéricos obtenidos. En las Figs.2-3 se presenta el resultado de encriptar y decriptar una imagen; la Fig.3.(f) corresponde al resultado de intentar decriptar la imagen de la Fig.3.(a) usando una llave diferente a la utilizada para encriptarla.

Por otro lado, se determinó que el sistema introduce alteraciones locales de intensidad en la imagen decriptada respecto a la imagen de entrada; este efecto se produce, con o sin el uso de ruido blanco multiplicando la entrada; las Figs.2.(f)-(g) y Figs.3.(g)-(h) muestran la distribución espacial del error introducido localmente en cada caso.

Los resultados de la Fig.4 corresponde a una prueba del sistema donde se demuestra que la máscara de ruido blanco multiplicando la imagen de entrada no es necesaria, siempre que la llave se construya con la distribución de fase apropiada. Ahora bien, el no uso de tal máscara se convierte en una ventaja desde el punto de vista de costos significativos, cuando estos sistemas se construyen óptimamente.

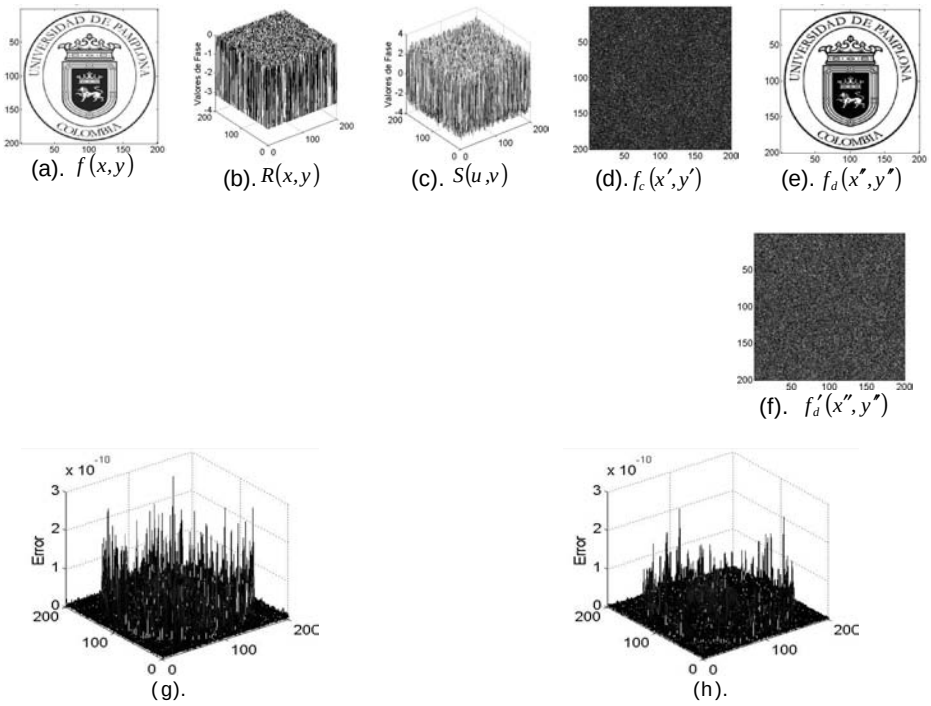


Figura 3. Resultados de encriptamiento. (a). Imagen a encriptar; (b). Distribución de fase de la máscara; (c). Distribución de fase de la llave; (d). Imagen (a) encriptada; (e). Imagen (a) decriptada; (f). Decriptado de la imagen (a) utilizando la llave de Fig.2.(c).; (g) . Error en (e) multiplicando (a) por ruido blanco; (h). Error en (e) sin multiplicar (a) por ruido blanco.

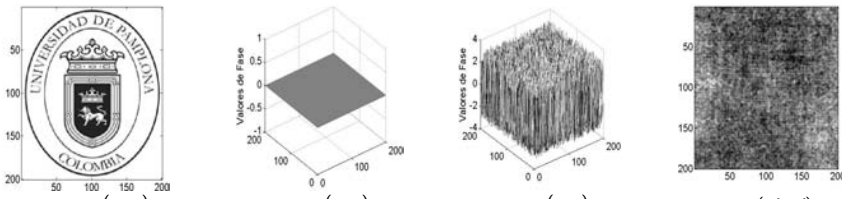


Figura 4. Resultados de encriptamiento. (a). Imagen a encriptar; (b). Distribución de fase de la máscara; (c). Distribución de fase de la llave; (d). Imagen (a) encriptada.

Se estudió la dependencia de los valores de fase de la llave, en función del factor seguridad en la fase de encriptado; en las Fig.5 se muestran algunos resultados de este estudio de cálculo óptimo de los valores de la distribución de fase de la llave; se determinó que los valores de esta distribución de fase están restringidos a valores cercanos a p. Obsérvese en las Figs.5.(d),(f) y (h), que el sistema no encripta la imagen de entrada, correspondiendo estos casos al uso de las llaves de las Figs.5.(c),(e) y (g), respectivamente, donde los valores de la fase son menores a p/4.

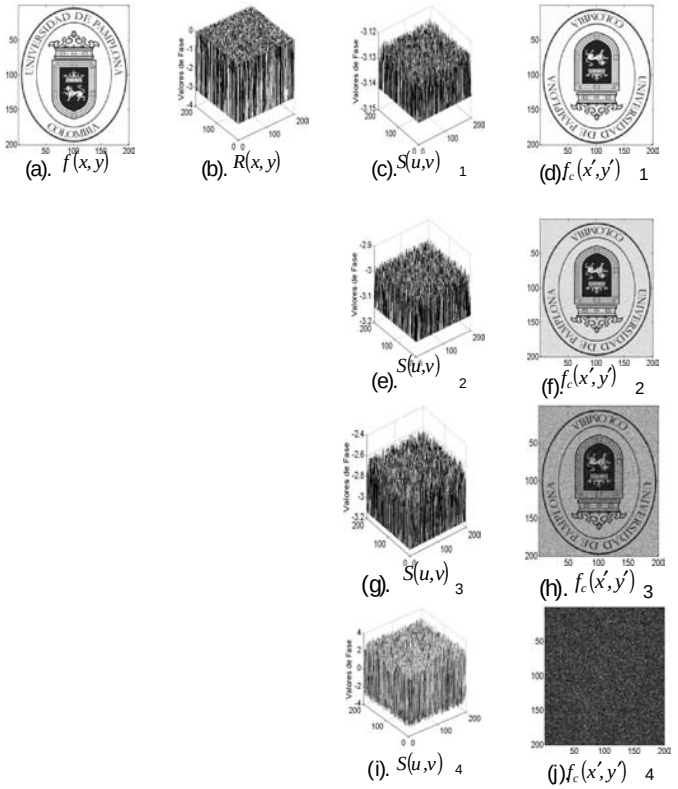


Figura 5. Resultados del estudio del nivel de cifrado del sistema en función de los valores de fase de la llave. (a). Imagen a encriptar; (b). Distribución de fase de la máscara ; (d).- (f).- (h).-(j). Imagen (a) encriptada con las llaves 1 a 4, respectivamente.

Los resultados de la Fig.5 se calcularon manteniendo para todos los casos la misma máscara ; el uso o no de la máscara, no genera diferencias significativas en los resultados obtenidos en este estudio.

CONCLUSIONES

Se modeló analíticamente y se implementó computacionalmente un algoritmo para cifrado digital de imágenes usando llaves de speckle de solo fase. El algoritmo modela el arreglo óptico de cifrado basado en la arquitectura de correlación Vander Lugt. Se demostró que este tipo de arreglo de cifrado puede funcionar sin el uso de la máscara , siendo esto una ventaja en disminución de costos, en el momento de una implementación óptica de este tipo de sistemas. Por otro lado, se comprobó que este sistema produce una respuesta con error, de un orden de magnitud difícilmente detectable a simple vista. Finalmente, se determinó que los valores de la distribución de fase de la llave están restringidos a valores cercanos a p, para que el sistema encripte el 100% de la imagen.

REFERENCIAS BIBLIOGRÁFICAS

A. Sinha and K. Singh, A technique for image encryption using digital signature, Optics Communications, 218, p.p.229-234, (2003)
A. Vander Lugt, Signal detection by complex spatial filtering. IEEE transactions on Information, Vol. 10, (1964), p. 139.
B. Javidi, G. S. Zhang, y J. Li, "Encrypted optical memory using double-random phase encoding", Appl. Opt. 36, 1054-1058, (1997).
C. Linfei, Z. Daomu, Optical image encryption based on fractional wavelet transform, Opt. Comm. Vol. 254 (2005) p.p. 361-367.
E. Tajahuerce and B. Javidi, Encrypting three Dimensional Information with Digital Holography, Journal of Applied Optics, vol. 39, pp. 6595-6601, December 10, (2000).
E. Tajahuerce, et al., Optical Security and Encryption with Totally Incoherent Light, Journal of Optics Letters, vol. 26, pp. 678-681, May 15, 2001.
E. Tajahuerce, et al., Optoelectronic information encryption using phase-shift interferometry, Journal of Applied Optics, Vol. 39, pp. 2313-2320, May 10, 2000.
F. Yu, and D. Gregory, Optical pattern recognition: architectures and techniques. Proc. IEEE, Vol. 84, (1996), p. 733.
F. YU, Introduction to diffraction, information processing, and holography. England : The MIT Press, 1973.
J. Goodman, Introduction to Fourier optics. New York: McGraw-Hill, 1968.
J. Rosen, and B. Javidi, Optical Encryption using Embedded Images, Journal of Applied Optics, accepted for publications, to appear, 2001.
J. Rueda, A. Salazar, y M. Lasprilla, Encriptación por conjugación de fase en un BSO utilizando señales ópticas de baja potencia, Rev. Col. Fís., Vol. 34, No.2, (2002), P.P.636-640.
O. Matoba, et al., Secure Optical Storage using fully phase encryption, Journal of Applied Optics, vol. 39, pp. 6689-6694, December 10, 2000.
P. Mogensen and J. Glückstad, A phase-based optical encryption system with polarisation encoding. Opt. Commun. (2000) 173, 177-183
P. Mogensen, and J. Glückstad, Phase-only optical decryption of a fixed mask. Appl. Opt. (2001) 40,1226-1235
P. Mogensen, J. Glückstad, Phase-only optical encryption. Opt. Lett. (2000) 25, 566-568
P. Mogensen, R. Eriksen, J. Glückstad, High capacity optical encryption system using ferro-electric spatial light modulators. J. Optics A. (2001) 3, 10-15
T. Nomura and B. Javidi, Optical encryption system using a binary key code, Journal of Applied Optics, vol. 39, pp. 4783-4787, September 10, (2000).