MSEL
Modelling in Science Education and Learning
Modelling in Science Education and Learning
Volume 6(3), No. 5, 2013.
Instituto Universitario de Matemática Pura y Aplicada

Encriptación óptica empleando llaves Weierstrass-Mandelbrot

Fernando Giménez, Juan A. Monsoriu
Universitat Politècnica de València
fgimenez@mat.upv.es, jmonsori@fis.upv.es

John Fredy Barrera
Universidad de Antioquia

Walter D. Furlan
Universitat de València
walter.furlan@uv.es

Myrian Tebaldi, Néstor Bolognini, Roberto Torroba
Universidad Nacional de La Plata (Argentina)
myrianc@ciop.unlp.edu.ar, nestorb@ciop.unlp.edu.ar, rtorroba@gmail.com

Abstract

En este trabajo se presenta la generación de llaves de encriptación aprovechando el carácter local oscilatorio y variable de las sumas parciales de la función fractal Weierstrass-Mandelbrot. Bajo este esquema, la llave de seguridad puede replicarse si se conocen los parámetros usados para su obtención. Por lo tanto, en lugar de enviar la llave de seguridad, se envían los parámetros que le permiten al usuario generarla en la estación desencriptadora. Este procedimiento permite reducir la cantidad de información a ser enviada y se evita la posible interceptación de la llave, además la llave no sufre pérdidas o contaminación. La efectividad de las llaves Weierstrass-Mandelbrot se demostró mediante simulaciones computacionales en un sistema óptico de encriptación 4f y la técnica de codificación de doble máscara de fase. Estas llaves permiten encriptar información y recuperarla, lo que representa la prueba de su efectividad para el manejo seguro de datos. Además, se demuestra que en la eventualidad de que un atacante pueda obtener el dato encriptado, éste no podrá acceder a la información si no posee la llave de seguridad.

This paper presents the generation of encryption keys using the local oscillating properties of the partial sums of Weierstrass-Mandelbrot fractal function. In this way, the security key can be replicated if the parameters used to obtain it are known. Therefore, these parameters can be sent instead of sending the key. This procedure reduces the amount of information to be sent and prevents possible interception of the key. Moreover, the key can not be affected by data loss or pollution. The effectiveness of the Weierstrass-Mandelbrot keys were demonstrated by computer simulation in a 4f optical encryption system and the double random phase encoding technique. These keys allow us to encrypt and to retrieve the information, which is the evidence of their effectiveness for data security. Furthermore, it is shown that if the encrypted data is obtained under an attack, it is not possible to access the information without the security key.

Keywords: Encriptación óptica, fractal, llave, doble máscara.
Optical cryptography, fractal key, double-masked.

1 Introducción

En la complejidad del mundo actual el uso de elementos de identificación y la necesidad de validar dichos elementos se ha incrementado notablemente, de manera que la seguridad en la información se ha convertido en parte de nuestra vida cotidiana. En las más triviales transacciones se requiere la utilización de una identificación segura, ya sea un pasaporte, un código, una tarjeta bancaria, etc. Las empresas invierten miles de millones de dólares alrededor del mundo para evitar el fraude en la información, sin contar otros tipos de fraudes más tradicionales como lo es la falsificación de dinero. Esto evidencia que la seguridad en el manejo de la información ha entrado a formar parte del quehacer diario de las personas y las empresas.

En la actualidad, la posibilidad de reproducir copias exactas de patrones de alto grado de complejidad, ha ido en aumento debido a los grandes avances que se han presentado en la computación y en la tecnología de escáneres e impresoras, lo que ha generado una carrera entre los que proveen los sistemas de seguridad y los que intentan quebrantarlos. Las comunicaciones electrónicas y el almacenamiento de datos en computadores están bajo el mismo riesgo, dado que las comunicaciones en línea y a través de redes inalámbricas pueden ser interceptadas. El riesgo aumenta debido a la alta capacidad de procesamiento de los computadores, capaces de reducir el tiempo requerido para codificar y decodificar mensajes.

En este sentido, debe tenerse en cuenta que la gran mayoría de los sistemas de codificación digitales que en un momento se pensaron totalmente seguros, finalmente fueron vulnerados [1]. A medida que los proveedores de seguridad generan nuevos sistemas digitales para la protección de datos, en esa misma medida, otras personas trabajan en la búsqueda de formas para quebrantar estos sistemas. Es por esto, que aunque los sistemas de encriptación comerciales que se usan en la actualidad son digitales, la encriptación óptica representa una atractiva y potencialmente poderosa herramienta para el manejo seguro de datos, debido principalmente a su gran número de grados de libertad y velocidad de procesamiento [2].

En este contexto, se han propuesto e implementado varios sistemas ópticos para el cifrado de datos, los cuales han demostrado que el procesamiento óptico permite una manipulación segura de la información. Entre ellos, los sistemas ópticos más usados y desarrollados son los que usan dos máscaras aleatorias de fase para cifrar información [3]. En las contribuciones presentadas en los últimos diez años, y en especial los últimos cinco, se ha mostrado la confiabilidad [4], versatilidad [5, 7] y aplicabilidad de los sistemas ópticos de encriptación de doble máscara de fase [8]; asimismo se ha evaluado [9] y mejorado la seguridad de algunas técnicas [10]. Con esta motivación, varias compañías están construyendo prototipos de dispositivos que permiten mejorar algunos de los procedimientos utilizados en la encriptación óptica de información. Cabe destacar el empeño de la compañía Bayer, que ha tomado la iniciativa de la fabricación de un sistema óptico de encriptación con el fin de comercializarlo [11]. Como consecuencia de todo lo anterior, actualmente la encriptación óptica concentra los esfuerzos de muchos investigadores en diferentes laboratorios alrededor del mundo, donde unos de los objetivos primordiales de las investigaciones es el diseño de dispositivos ópticos que posean un alto grado de seguridad.

En lo que respecta a la implementación práctica de los sistemas de encriptación, estos poseen un elemento conocido como llave de seguridad, el cual permite encriptar la información y a su vez recuperarla a partir de la imagen encriptada. Para acceder a la información, el usuario autorizado debe tener acceso a la llave de seguridad y la información encriptada.

La llave que presentamos en este trabajo está generada a partir de una de las funciones más sorprendentes del mundo de las matemáticas: la función de Weierstrass. Se trata de un "mons-

truo" del análisis matemático por ser continua en la recta real pero no diferenciable en ningún punto. Mandelbrot considera a la curva generada como el primer ejemplo de fractal.

En este trabajo se propone e implementa un esquema de seguridad donde en lugar de enviar la llave de seguridad, se envía un conjunto de parámetros que le permiten al usuario generar dicha llave. Este procedimiento permite eliminar las contingencias por pérdidas o contaminación que en la etapa transmisora puede sufrir la llave; y además evita la interceptación de la llave, lo que incrementa la seguridad del proceso. Una ventaja adicional es la disminución en la cantidad de información enviada, lo que ayuda a optimizar el envío y recepción de la información.

2 Codificación óptica de información

A los diferentes procedimientos ópticos usados para cifrar información se les conocen como "métodos de encriptación", y a los usados para recuperar la información oculta se les conoce como "métodos de desencriptación". El código con el cual se oculta la información se conoce como llave de seguridad, lo que implica que la información sólo puede ser recuperada si el usuario autorizado posee esta llave. Los sistemas ópticos de encriptación más usados son los que emplean dos máscaras aleatorias de fase, los cuales son usualmente llamados "sistemas de encriptación de doble máscara de fase", esto debido a que la representación de códigos de seguridad como patrones de fase los tornan prácticamente imposibles de ser leídos o copiados por medios ópticos o electrónicos convencionales. Adicionalmente, la seguridad del sistema es proporcionada por una máscara aleatoria, lo que significa que la posibilidad de construir una máscara para tratar de violar el sistema de encriptación sería un trabajo infructuoso, pues existen millones de combinaciones que se deben probar para poder violar el sistema.

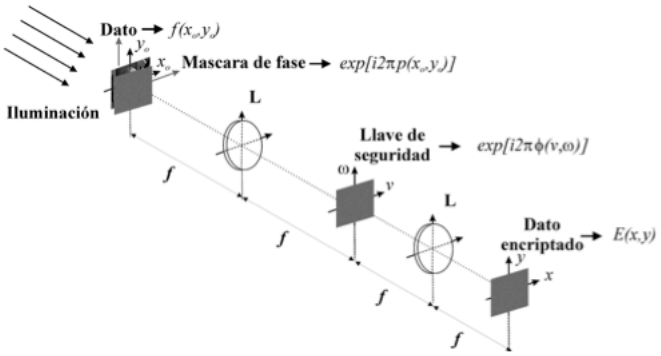

Figura 1: Representación del sistema óptico de encriptación.

En el sistema de encriptación de doble máscara de fase el dato a encriptar $f(x_0, y_0)$ se pone en contacto con una máscara aleatoria de fase $\exp\big(2\pi i p(x_0, y_0)\big)$ (ver la Figura 1). Luego se genera la transformada de Fourier de este producto y en el plano de Fourier se multiplica por la llave de seguridad $\exp\big(2\pi i \phi(v, \omega)\big)$, que es también una máscara aleatoria de fase. Finalmente se genera otra transformada de Fourier para obtener el dato encriptado $E(x, y)$ [4],

$$E(x, y) = \big(f(-x, -y) \exp\big(2\pi i p(-x, -y)\big) \otimes F_{x,y}\big(\exp\big(2\pi i \phi(v, \omega)\big), \tag{1}$$

donde $\otimes$ representa la convolución, $F_{x,y}\big(\cdot\big)$ la operación transformada de Fourier y las funciones $p(x_0, y_0)$ y $\phi(v, \omega)$ son aleatorias e independientes con valores en el intervalo $[0, 1]$. Donde

(x_0, y_0) denotan las coordenadas del plano de entrada y (v, ω) las coordenadas del primer plano de Fourier.

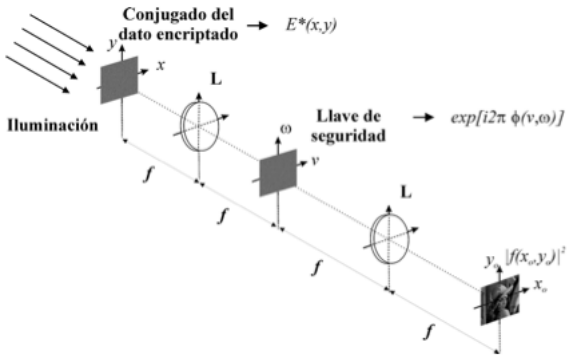

Figura 2: Representación del sistema óptico de desencriptación.

Para recuperar el dato se genera el complejo conjugado de la transformada de Fourier de la imagen encriptada [3, 5], se multiplica por la llave de seguridad y al generar una segunda transformada de Fourier se obtiene (ver la Figura 2):

$$d(x_0, y_0) = f^*(x_0, y_0) \exp\big(-2\pi i p(x_0, y_0)\big). \tag{2}$$

El paso final es obtener el módulo cuadrado del dato desencriptado $\big|d(x_0, y_0)\big|^2$ para recuperar la información del dato $\big|f(x_0, y_0)\big|^2$. Experimentalmente se aprovecha la posibilidad de: generar la transformada de Fourier con una lente positiva, obtener el complejo conjugado de un campo óptico empleando un cristal fotorrefractivo [3] y almacenar el módulo cuadrado del campo por una cámara CCD [7]. Lo anterior implica que cuando es un dato de amplitud, no es necesario poseer la información de la máscara que se situó en el plano de entrada durante la encriptación, pues la contribución de esta máscara es eliminada al registrase el modulo cuadrado del campo óptico. Mientras que para datos complejos, en el plano de salida debe multiplicarse por la máscara aleatoria $\exp\big(-2\pi i p(x_0, y_0)\big)$ [10].

3 Función fractal de Weierstrass-Mandelbrot

A principios del siglo XIX muchos matemáticos creían que una función continua tenía derivada en un conjunto significativo de puntos. Karl Weierstrass en 1872 sorprendió a la comunidad científica construyendo la función

$$f(x) = \sum_{n=0}^{\infty} a^n \cos(b^n \pi x) \tag{3}$$

La función tiene la particularidad de que es continua en todos los puntos de la recta real pero no es diferenciable en ninguno siempre que $0 < a < 1$, b sea un entero impar mayor que 1 y $ab > 1 + 3\pi/2$. A este tipo de funciones patológicas se las considera "monstruos" del análisis real. Su aspecto puede verse en la Figura 3. Esta función la presentó Weierstrass en una conferencia en la Real Academia de Ciencias de Berlín, pero el resultado no fue publicado hasta 1875 por Paul du Bois-Reymond [13]. La curva generada por la función anterior fue considerada por Mandelbrot como el primer fractal conocido.

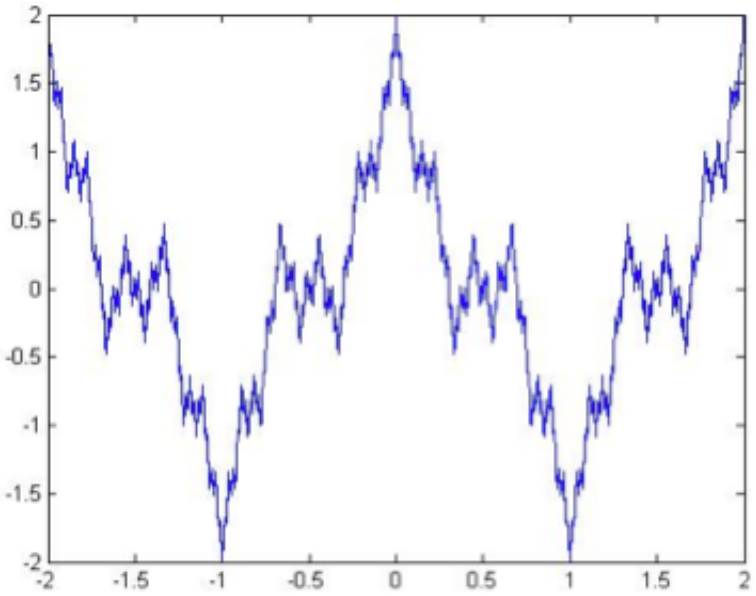

Figura 3: Función de Weierstrass para $a = 0.5$ y $b = 3$.

Considérese la siguiente modificación de la función de Weierstrass debida a Mandelbrot:

$$f(x) = \sum_{n=0}^{\infty} \omega^{-n\alpha}\big(1 - \cos(\omega^n \pi x)\big), \qquad \omega > 1, 0 < a < 1. \tag{4}$$

Esta función tiene las siguientes propiedades:

- Posee un escalado autoafín, esto es, toda la función $f(x)$ se puede reconstruir a partir de su valor en el intervalo $[x_0, \omega x_0[$. Así, por ejemplo, $f(x)$ en los intervalos $[\omega x_0, \omega^2 x_0[$ y $[x_0/\omega, x_0[$ son versiones aumentadas y disminuidas respectivamente de $f(x)$ en el intervalo $[x_0, \omega x_0[$. Es pues invariante frente al cambio de escala.

- Es autosimilar.

- Si ω es impar entonces $f(x)$ es periódica de periodo 2.

- Es hölderiana de orden α, esto es, se cumple que $|f(x) - f(y)| \leq C|x - y|^\alpha$ para una cierta constante $C > 0$.

Para apreciar el carácter fractal que tiene la curva de Weierstrass-Mandelbrot basta con considerar las sumas parciales

$$S_n(x) = \sum_{i=0}^{n} \omega^{-i\alpha}\big(1 - \cos(\omega^i \pi x)\big). \tag{5}$$

En la Figura 4 se puede apreciar la gráfica correspondientes a las cuatro primeras sumas parciales para el caso $\alpha = 0.5$ y $\omega = 3$.

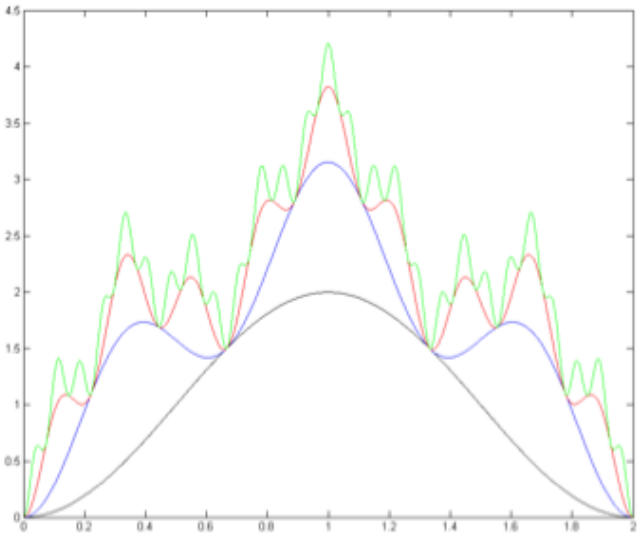

Figura 4: Gráficas de S_0 (negro), S_1 (azul), S_2 (rojo) y S_3 (verde) para $\alpha = 0.5$ y $\omega = 3$.

Podemos observar que sobre el lóbulo correspondiente a la gráfica de S_0 se sitúan los tres lóbulos correspondientes a S_0 y sobre cada uno de éstos los correspondientes a S_2, etc. Además podemos observar que el máximo absoluto de todas las sumas parciales se alcanza en un único punto $x = 1$.

En la Figura 5 se presenta el caso $\alpha = 0.5$ y $\omega = 4$, donde se puede apreciar que el máximo absoluto de las sumas parciales se alcanza en dos puntos.

En general el número de lóbulos de S_n se corresponde con el valor de ω^n y coincide también con el número de máximos locales para los valores de ω enteros. Este máximo para S_n es

$$\sum_{i=0}^{n} 2\omega^{-i\alpha} = \frac{1-\omega^{-(n+1)\alpha}}{1-\omega^{-\alpha}} < \frac{1}{1-\omega^{-\alpha}} = \frac{\omega^{\alpha}}{\omega^{-\alpha}-1}. \tag{6}$$

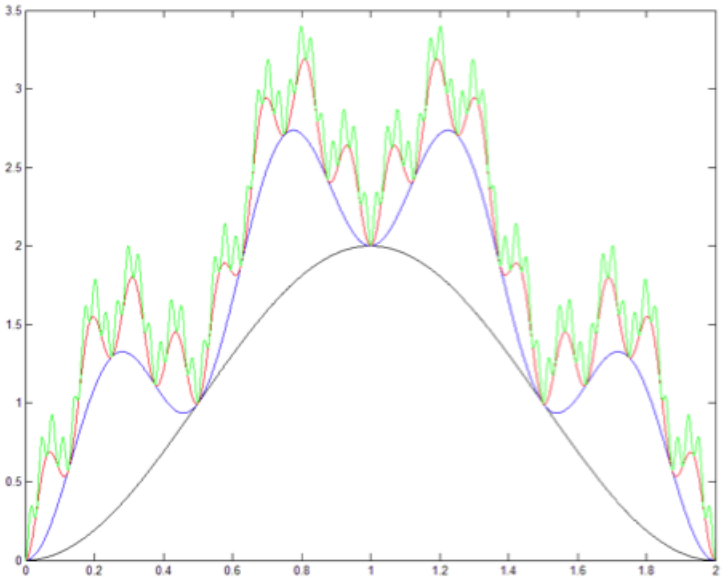

Figura 5: Gráficas de S_0 (negro), S_1 (azul), S_2 (rojo) y S_3 (verde) para $\alpha = 0.5$ y $\omega = 4$.

4 Generación de llaves de seguridad Weierstrass-Mandelbrot

La llave de seguridad en los sistemas ópticos de encriptación es un elemento de fase que se puede representar como una matriz $C = (c_{ij})$ de $N \times N$ entradas [10]. Cada entrada puede tomar valores entre 0 y 255. Las máscaras de fase serán creadas asignando como valor de cada píxel, un valor de fase proporcional a su nivel de gris siendo esta distribución de fase la que se emplea como llave de seguridad. Para esta asignación se utiliza la relación de proporcionalidad de $C = 2\pi/255(c_{ij})$.

Para generar la llave a partir de las sumas parciales de la función de Weierstrass-Mandelbrot primero se define un intervalo inicial $[a, b]$ y se luego se divide en $N^2 - 1$ subintervalos de longitud $h = (b - a)/(N^2 - 1)$. En este caso los nodos correspondientes se denotan por $x_j = a + jh,\ j = 0, 1 \ldots, N^2 - 1$. En segundo lugar, a partir de los nodos se construyen valores $z_{ij} = 10^r S_n(x_{N(i-1)+j})$ para $i, j = 1, \ldots, N$, donde r es un entero positivo dado. Finalmente, la llave de seguridad se define por la matriz,

$$C_{ij} = E\big(256(z_{ij} - E(z_{ij})\big), \tag{7}$$

en donde $E(\,\cdot\,)$ representa la parte entera. El valor de $z_{ij} - E(z_{ij})$ coincide con el número decimal en el intervalo $[0, 1[$ que resulta de eliminar la parte entera y los r primeros decimales de la suma parcial $S_n(x_{N(i-1)+j})$. Esto permite aprovechar el carácter local oscilatorio y variable de las sumas parciales S_n, de manera que al aumentar el valor de r se consigue que aumente la aleatoriedad de la matriz C, lo cual es deseable para obtener llaves que permitan asegurar la seguridad de los sistemas.

De acuerdo a este procedimiento, es evidente que la llave queda determinada cuando se define el intervalo $[a, b]$ y los parámetros de ω, α, n, N y r. En la Figura 6 se pueden observar las llaves generadas para valores de N igual a: (a) 10 y (b) 40. En la Figura 6(b) es evidente la aleatoriedad de la máscara, propiedad que asegura su utilidad como llave en un sistema de encriptación para el manejo seguro de información

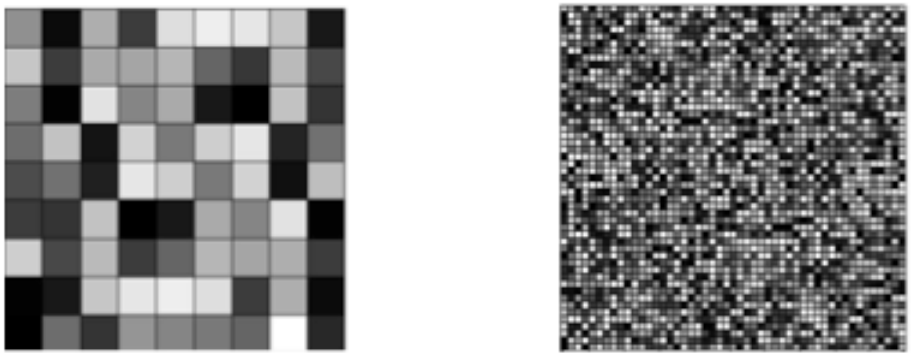

Figura 6: Llaves de seguridad para el intervalo $[0, 2]$, $\omega = 3$, $\alpha = 0.5$, $n = 40$, $r = 5$ y para N igual a: (a) 10 y (b) 40.

5 Resultados de los procesos de encriptación y desencriptación

Se verifica a partir de simulaciones computacionales que las matrices obtenidas a partir de la función fractal Weierstrass-Malderbrot representan llaves de seguridad adecuadas para el sistema óptico de encriptación de doble máscara de fase. La ventaja de generar estas matrices es que, a diferencia de las máscaras aleatorias convencionales, las matices C son reproducibles conocidos sus 6 parámetros de construcción, por lo tanto en lugar de enviar la llave solo se envían estos parámetros.

Esto implica que la matriz C reemplaza la función $\phi(v,\omega)$ en los procesos de encriptación y desencriptación descritos en la sección 3. En las Figuras 7(a), (b) y (c) se incluyen tres objetos y sus respectivos pares encriptados en las Figuras 7(d), 7(e) y (f), respectivamente. Los resultados demuestran que las llaves Weierstrass-Mandelbrot permiten encriptar información, pues aunque cada objeto encriptado contiene la información de su respectivo objeto, a partir de éste no se puede reconocer la existencia de información.

Los datos se pueden recuperar si en el proceso de desencriptación se usa la llave correcta (Figuras 7(a), (b) y (c)), mientras que no se puede acceder a la información cuando se utilizan llaves diferentes (Figuras 8(d), (e) y (f)). Como se evidencia en este caso, si se modifica uno de los parámetros en la construcción de la llave, no se puede recuperar la información original y por lo tanto se puede afirmar que la llave permite asegurar la fiabilidad del método.

Figura 7: Objetos a encriptar: (a), (b) y (c), y sus correspondientes objetos encriptados empleando llaves con un intervalo $[0,2]$, y usando los parámetros $\omega = 3$, $\alpha = 0.5$, $N = 512$, $r = 5$ y para n igual a: (d)40, (e) 60 y (f)80, respectivamente.

Figura 8: (a), (b) y (c) objetos recuperados empleando las llaves correctas. Desencriptación con llaves generadas con el mismo intervalo $[a, b]$ y los mismos valores de los parámetros α, n, N y r para cada caso, pero con un valor de ω igual a: (d) 4, (e) 5 y (f) 6, respectivamente.

6 Conclusiones

En esta contribución se demuestra que a partir de las sumas parciales de la función fractal Weierstrass-Mandelbrot se pueden generar matrices que actúan como llaves de seguridad en un sistema óptico de encriptación de doble máscara de fase bajo arquitectura 4f. Los resultados de los procesos de encriptación y desencriptación validan la aplicabilidad del método. Además, se mostró que al cambiar uno de los parámetros de la llave se evita la recuperación de los datos. Se vislumbra el uso las llaves Weierstrass-Mandelbrot para la manipulación segura de muchos datos.

Agradecimientos

Este trabajo fue realizado con el apoyo de los siguientes subsidios: Sostenibilidad 2011-2012 y CODI (Universidad de Antioquia-Colombia), CONICET No. 0863/09 and No. 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I168 (Argentina), Ministerio de Economía y Competitividad, España (programa FIS2011-23175) y Universitat Politècnica de Valencia, España (programas PAID-05-11 y PAID-02-11).

Referencias

[1] N. Camp-Winget, R. Housley , D. Wagner. Security flaws in 802.11 data links protocols, Commun. ACM, **46**, 35–39 (2003).

[2] O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, B. Javidi. Optical Techniques for Information Security, Proceedings of the IEEE, **97**, 1128-1148 (2009).

[3] J. F. Barrera , R. Henao, M. Tebaldi, R. Torroba, N. Bolognini. Multiplexing encryption-decryption via lateral shifting of a random phase mask, Opt. Commun., **261**, 29–33 (2009).

[4] B. Javidi, A. Esmail, G. Zhang. Optical security system using Fourier plane encoding, U.S. patent 7,684,098 B2 (March 23, 2010).

[5] F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, R. Torroba. All-optical encrypted movie, Opt. Express, **19**, 5706–5712 (2011).

[6] F. Mosso F., M. Tebaldi, J. F. Barrera, N. Bolognini, R. Torroba. Pure optical dynamical color encryption, Opt. Express, **19**, 13779-13786 (2011).

[7] J. F. Barrera, E. Rueda, C. Ríos, M. Tebaldi, N. Bolognini, R. Torroba. Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality, Opt. Commun., **284**, 4350–4355 (2011).

[8] J. F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, R. Torroba. Experimental multiplexing of encrypted movies using a JTC architecture, Opt. Express, **20**, 3388–3393 (2012).

[9] J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, N. Bolognini. Known-plaintext attack on a joint transform correlator encrypting system, Opt. Lett., **35**, 3553–3555 (2010).

[10] J. F. Barrera, R. Torroba. Efficient encrypting procedure using amplitude and phase as independent channels to display decoy objects, Appl. Opt., **48**, 3121–3129 (2009).

[11] Bayer company, Optical encryption ensures maximum data security: Keeping a keen eye on security, www.research.bayer.com (2005).

[12] P. du Bois-Reymond. Versuch einer Classification der willk¨urlichen Functionen reeller Argumente nach ihren Aenderungen in den kleinsten Intervallen, J. Reine. Angew. Math., **79**, 21–37 (1875).

[13] M. V. Berry, Z. V. Lewis. On the Weierstrass-Mandelbrot fractal function, Proc. R. Soc. Lon. A, **37**, 459–484 (1980).