CIFRADO DE IMÁGENES BASADOS EN SISTEMAS DINÁMICOS

MARTÍNEZ ÁVILA, Saúl[1], MURGUÍA IBARRA, José Salomé[2], MARTÍNEZ RODRIGUEZ, Veronica[3],

[1]*Universidad Autónoma de San Luis Potosí, Facultad de Ciencias. Av. Dr. Salvador Nava s/n C.P. 78290, San Luis Potosí, S.L.P.* ondeleto@uaslp.mx
[2]*Universidad Autónoma de Querétaro, Facultad de Ingeniería-Campus, Aeropuerto Carr. a Chichimequillas s/n C.P. 76140, Querétaro, Qro.* sasa.97@live.com
[3]*Instituto Tecnológico Superior de Monclova, Carretera No. 57Los 90´s C.P 25733 Monclova, Coah.Mexico.* vero@monclova.tecnm.mx

International Identification of Science - Technology and Innovation

ID 1er Autor: Saúl, MARTÍNEZ ÁVILA (ORC ID 0000-0001-6365-1293)
ID 1er Coautor: José Salomé, MURGUÍA IBARRA (ORC ID 0000-0002-4458-9014)
ID 2er Coautor: Veronica, MARTÍNEZ RODRIGUEZ (ORC ID 0000-0003-0242-4815)

Resumen — En este trabajo se presenta la implementación numérica de un sistema de cifrado de imágenes, el cual utiliza un mapeo unidimensional caótico para decorrelacionar las imágenes, y una caja de sustitución que junto con el mapeo caótico anterior realizan la etapa de confusión. El sistema de cifrado propuesto es aplicado a imágenes en escala de grises donde los resultados obtenidos muestran que tal propuesta presenta un buen desempeño, además de ser resistente a ciertos ataques.

Palabras clave — Sistema de cifrado, mapeo caótico, caja de sustitución.

Abstract — In this work the numerical implementation of an image encryption system is presented, which employs an unidimensional chaotic system to decorrelate the images, a substitution box that together with the previous chaotic map perform the confusion stage. The proposed encryption system analysis is applied to gray scale images and the obtained results illustrate that the proposal presents a good performance, besides its resistance to some attacks.

Keywords — Encryption system, chaotic map, substitution box.

I. INTRODUCCIÓN

Con el rápido avance y crecimiento de la tecnología, la transmisión de grandes cantidades de información (imagen, video o de cualquier tipo) se ha vuelto cada vez más habitual, donde una de las principales prioridades es la protección de la misma y evitar que agentes externos puedan intervenir y hacer mal uso de tal información. Debido a las vulnerabilidades que pueden presentar los sistemas de información, surge la necesidad de decodificarla y protegerla frente a terceros. Desde décadas pasadas se han utilizado diferentes métodos de cifrado, pero sobre todo en señales de imágenes se cuenta con algunos sistemas de cifrado menos eficientes que otros.

Actualmente, una alternativa para el cifrado de imágenes es el uso de sistemas que presentan dinámica caótica, ya que dichos sistemas poseen propiedades interesantes como lo son la alta dependencia a las condiciones iniciales, la no periodicidad, entre otros, haciendo que estos sistemas sean una herramienta auxiliar eficiente en el proceso de cifrado de una imagen [1-2].

De forma general, un sistema de cifrado se compone de los procesos de cifrado y descifrado de la información, además de una llave que no es más que una expresión que contiene números o letras y que sirve como mecanismo para poder realizar dichos procesos. El sistema de cifrado utilizado en este trabajo hace uso de un mapeo caótico unidimensional basado en la función beta; tal mapeo caótico nos proporciona una seria de ventajas como lo son el fuerte comportamiento caótico, un amplio rango de parámetros de bifurcación, así como un alto número de parámetros, los cuales nos proporcionan un alto grado de seguridad. Asimismo, con la finalidad de que el sistema tenga una relación confusa entre el cifrado y la llave, se considera utilizar una caja de sustitución ya establecida en conjunción del mapeo anterior.

II. MARCO TEÓRICO

A. Mapeo caótico unidimensional

El mapeo caótico unidimensional considerado utiliza como parte fundamental a la función beta la cual es definida por la Ec. (1) [3].

$$Beta(x;p,q,x_1,x_2) =. \begin{cases} \left(\frac{x - x_1}{x_c - x_1}\right)^p \left(\frac{x_2 - x}{x_2 - x_c}\right)^p & \text{para } x \in [x_1, x_2] \\ 0 \quad \text{para otros valores} \end{cases} \tag{1}$$

donde $p, q, x_1, x_2 \in R$, $x_1 < x_2$ y $x_c = \frac{p\,x_1 + q\,x_1}{p+q}$

En la figura 1 se ilustran diversas gráficas muy parecidas a las funciones trapezoidal, triangular y Gaussiana, respectivamente.

El mapeo caótico basado en la función beta se define matemáticamente con la Ec. (2).

$$x_{n+1} = k \times Beta(x_n;p,q,x_1,x_2) \tag{2}$$

donde los valores de los parámetros son $p = b_1 + c_1 \times a$, y $q = b_2 + c_2 \times a$ con b_1, c_1, b_2 y c_2 son constantes seleccionadas de forma adecuada, k es un parámetro que multiplica el mapeo caótico con la finalidad de controlar la amplitud del mapeo caótico y a denota el parámetro de bifurcación.

Cabe resaltar que a pesar de la simplicidad de la ecuación anterior presentada, con la variación de sus parámetros se obtienen diferentes comportamientos caóticos produciendo graficas totalmente diferentes. Tales características nos ayudan a producir un cifrado más eficiente y resistente a la mayoría de los ataques.

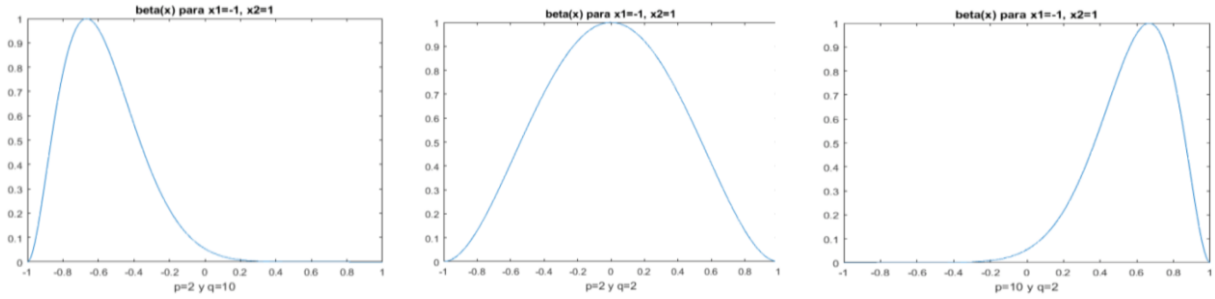

Fig 1. Gráficas resultante de la función beta con diferentes valores de parámetros.

B. Caja de sustitución (S-box)

Una de las principales características de los cifradores de bloques es que cumplan con la propiedad de confusión, término acuñado por Claude Shannon en 1949. Dicha propiedad permite que las propiedades estadísticas entre el texto cifrado y la llave se obscurezcan tanto como les sea posible.

Lo anterior se logra con una caja de sustitución (S-box), la cual es un componente no-lineal básico del sistemas de cifrado. En general, una S-box toma un número de entrada y lo transforma en otro número. En muchas ocasiones podría parecer sencillo que una S-box puede ser fácilmente implementada debido a que se puede considerar como una tabla fija de consulta. Sin embargo no lo es. En este trabajo se utilizó la S-box implementada en el trabajo de Aboytes-González *et al* [4], el cual se recomienda para una mejor descripción de la misma.

III. METODOLOGÍA

El sistema de cifrado implementado consta de 3 etapas, en el cual se usa una llave de 4 condiciones iniciales y un conjunto de parámetros que se utilizaran a lo largo del proceso de cifrado.

a) En la primera etapa se realiza el proceso de permutación en la cual se cambia el orden de los renglones y columnas con el fin de generar una imagen de carácter aleatoria.

b) La segunda etapa se realiza el proceso de difusión en el cual se hace uso de una caja de sustitución que de forma general este proceso toma el valor de un pixel y lo sustituye por otro valor, con el fin de ocultar la relación entre la clave y la imagen cifrada.

c) Por último se aplican una serie de operaciones a la imagen resultante del proceso anterior con el fin de obtener una imagen cuyo histograma muestre una distribución uniforme. Con lo cual se obtendría una imagen donde las redundancias fueron ocultadas.

El sistema de cifrado propuesto se muestra en la figura 2.

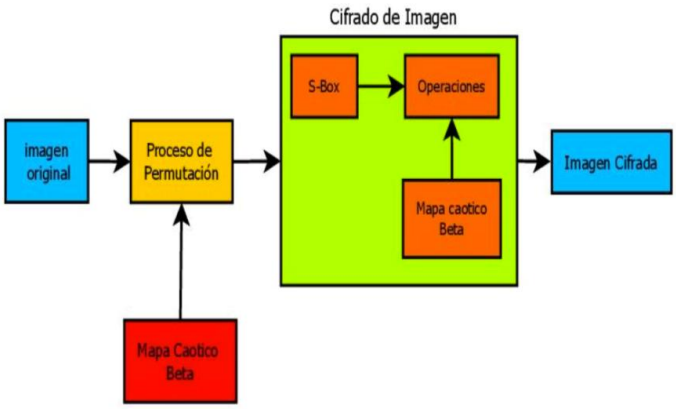

Fig. 2. Sistema de cifrado propuesto.

El algoritmo para realizar el proceso de cifrado es el siguiente:

1. Considerar una imagen de dimensión M×M.
2. Generar 2 secuencias de carácter caótico usando las primeras dos condiciones iniciales de la llave, una vez obtenidas dichas secuencias, reacomodar cada secuencia en una matriz de M×M obteniendo las matrices Q1 y Q2.
3. Se realiza el proceso de permutación de la siguiente manera:
   a. Ordenar los renglones de Q1 y Q2 de menor a mayor con el fin de obtener el orden de los índices de cada renglón de dichas matrices.
   b. Las matrices de índices M1 y M2 servirán para indexar la imagen de la siguiente manera:
      i. Se usara la matriz M1 para reacomodar los renglones de la imagen original.
      ii. Una vez modificados los renglones de la imagen se prosigue a reacomodar las columnas usando la matriz de índices M2.
4. Una vez obtenida la matriz permutada se hace pasar por la caja de sustitución para obtener la matriz P.
5. Por último se obtienen otras dos matrices como en el punto número 1usando las dos condiciones iniciales restantes de la llave, para obtener las matrices Q3 y Q4, a dichas matrices se les aplica $p_n = floor(Q_{n+2} \times 10^{14})\%256$, para $n=1,2$, con el fin de obtener las nuevas matrices p_1 y p_2.
6. Se realiza las siguientes operaciones a la matriz P (resultante de la caja de sustitución) de forma consecutiva para obtener a si la imagen cifrada Ic, es decir, $w = P\ xor\ p_3$, e $Ic = (w + p_4)\%256$.

Una vez obtenida la imagen cifrada, para obtener la imagen original sólo basta con realizar las operaciones inversas así como la llave.

IV. RESULTADOS

Con la finalidad de verificar la seguridad del sistema de cifrado propuesto, se aplicaron algunas pruebas estadísticas, las cuales son usadas para obtener la relación que hay entre la imagen original y la imagen cifrada. Una de las pruebas es la del histograma, en el que la imagen cifrada debe presentar una distribución uniforme. Los resultados se muestran en la figura 3, donde se ilustra que la imagen original y su versión permutada presentan el mismo histograma, mientras que la imagen cifrada presenta un histograma con distribución uniforme.

Además, se consideró la prueba de correlación adyacente de la imagen original y la cifrada, donde se puede observar que la imagen original presenta una fuerte correlación entre cada uno de los pixeles adyacentes, mientras que la imagen cifraba tiene muy poca correlación entre cada pixel adyacente lo cual prueba que el sistema de cifrado es fuerte (ver figura 4).

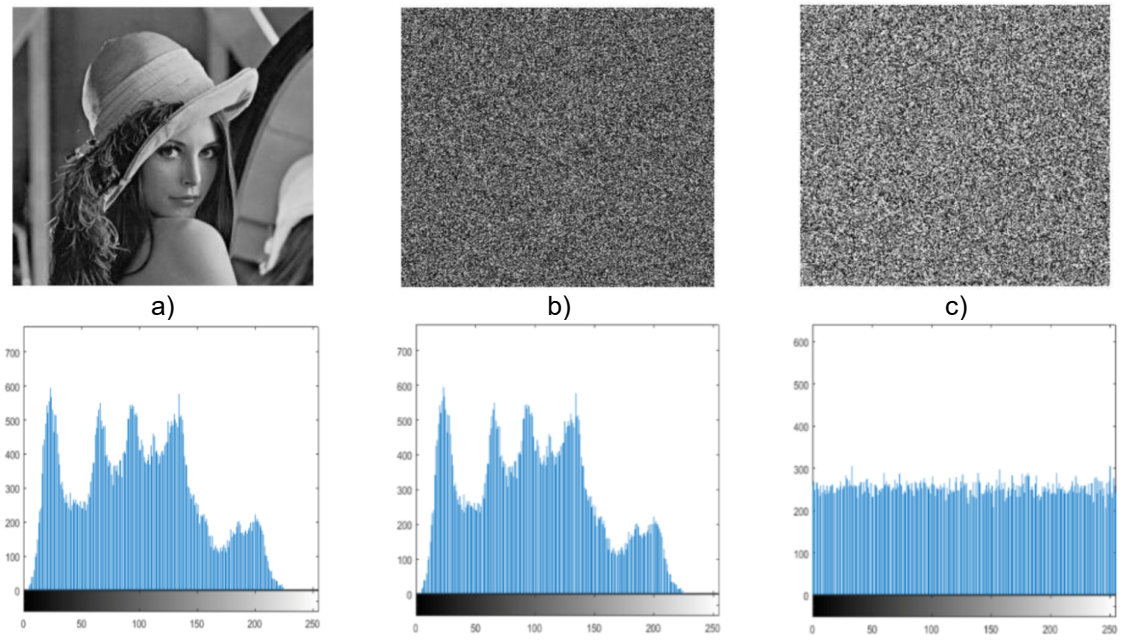

Fig. 3. a) Imagen de prueba, b) Imagen permutada y c) Imagen cifrada. d), e) y f) corresponden a sus respectivos histogramas.

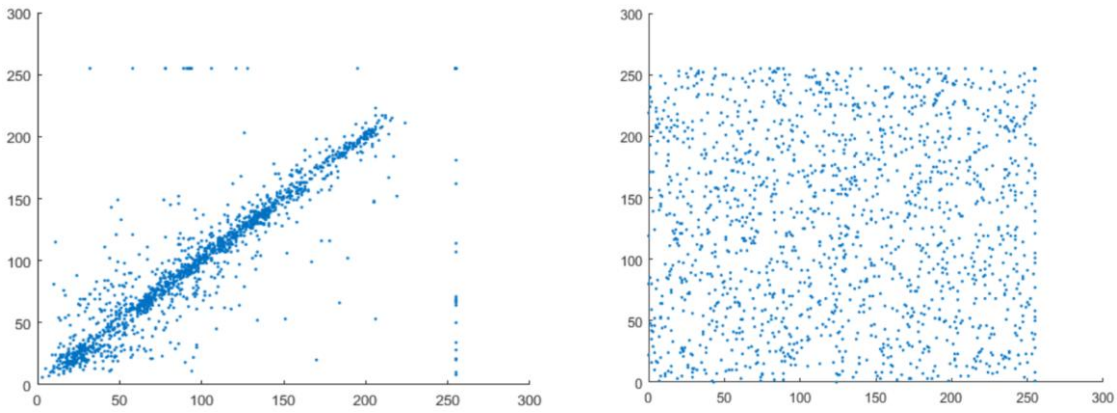

Fig. 4. Correlación de imagen a) original y b) cifrada.

Asimismo, para evadir algunos ataques de tipo estadístico se realizaron las pruebas del número de tasa de cambio de píxeles (NPCR), de la intensidad cambiante media unificada (UACI), de entropía (E) , análisis de correlación adyacente horizontal (CH), vertical (CV) y diagonal (CD), entre otros. Los resultados obtenidos son: NPCR = 99.5987, UACI = 30.6047, E = 7.9933, CH = 0.0422, CV = -0.0756 y CD = -0.1128. Además, el PSNR entre la imagen original y la cifrada fue de 8.5673 y el MSE de 9043.8. Los resultados anteriores fueron muy parecidos con los de otros autores [3,5], lo cual nos indica de una buena seguridad de la imagen cifrada.

V. CONCLUSIONES

En este proyecto se propuso y realizó la implementación de un sistema de cifrado a imágenes en función de un mapeo caótico unidimensional, el cual decorrelacionar las imágenes, y una caja de sustitución que junto con el mapeo caótico anterior realizaron la etapa de confusión.

Con la finalidad de evaluar la seguridad del sistema de cifrado propuesto se realizó un análisis con un conjunto de pruebas estadísticas tales como el análisis de histograma, el de correlación adyacente, entre otras. Los resultados obtenidos mostraron un buen desempeño comparados con la de otros trabajos por lo que el sistema de cifrado propuesto en general es seguro a cierto tipo de ataques.

VI. RECONOCIMIENTOS

Expreso mi agradecimiento a la Universidad Autónoma de Querétaro y al CONACyT por las facilidades y el apoyo otorgado para la realización de la estancia de verano.

REFERENCIAS

[1] C. Para, J. Pelzl, *Undersanding Cryptography: A Textbook for Students and Practitioners*, Ed. Springer-Verlag. Berlin Heidelberg, 2010.

[2] K. Kaya, C (Editor) *Cryptographic Engineering*, Ed. Springer Science+Business Media, LLC, 2009.

[3] R. Zahmoul, R. Ejbali, M. Zaied, “Image encryption based on new Beta chaotic maps”, *Optics and Lasers in Engineering*, Vol. 96, pp. 39-49. 2017.

[4] J. A. Aboytes-González, J. S. Murguía, M. Mejía-Carlos, et al., “Design of a strong S-box based on a matrix approach”, *Nonlinear Dynamics*, Disponible en https://doi.org/10.1007/s11071-018-4471-z [consultado en 2018].

[5] M. T. Ramírez-Torres, J. S. Murguía, M. Mejía Carlos, “Image encryption with an improved cryptosystem based on a matrix approach” *Int. J. Mod. Phys. C*, No. 10, Vol. 25, [1450054], 2014.