Criptoanálisis a Sistema de Cifrado de Imágenes Basado en Múltiples Cajas de Sustitución

Marco Tulio Ramírez-Torres
Coordinación Académica Región Altiplano Oeste
Universidad Autónoma de San Luis Potosí
Salinas de Hidalgo, México
tulio.torres@uaslp.mx

Gina Gallegos-García
Centro de Investigación en Computación
Instituto Politécnico Nacional
Ciudad de México, México
ggallegos@cic.ipn.mx

Jesús Agustín Aboyte-González
Centro de Investigación en Computación
Instituto Politécnico Nacional
Ciudad de México, México
agustin.aboytes@upslp.edu.mx

César Arturo Guerra-García
Coordinación Académica Región Altiplano Oeste
Universidad Autónoma de San Luis Potosí
Salinas de Hidalgo, México
cesar.guerra@uaslp.mx

Carlos Soubervielle-Montalvo
Facultad de Ingeniería
Universidad Autónoma de San Luis Potosí
San Luis Potosí, México
carlos.soubervielle@uaslp.mx

***Abstract*— Debido a las necesidades actuales de seguridad, diversos autores han propuesto varios sistemas de cifrado, basados en diferentes principios de funcionalidad y aplicados a diferentes tipos de información. Las cajas de sustitución han demostrado ser una herramienta importante en los sistemas de cifrado simétrico como parte de las operaciones de confusión. Actualmente hay propuestas de sistemas de cifrado que incluyen el uso de múltiples cajas de sustitución, así como las llamadas cajas de sustitución dinámicas. Sin embargo, es importante analizar a profundidad los sistemas de seguridad que se encuentran publicados antes de ser implementados o tomados como referencia. En este trabajo se analiza un sistema de cifrado para imágenes, propuesto por Majid Khan, donde con estadística y ataques criptoanáliticos se ha podido verificar la calidad del cifrado, utilizando el ataque chosen-plain image attack. El sistema es quebrado con este ataque, revelando la información original sin conocer la llave de cifrado, utilizando solo dos imágenes arbitrarias. Este trabajo trata de explicar a detalle la forma de realizar un criptoanálisis, para que a futuro las personas que diseñen un sistema de seguridad contemplen estas pruebas.**

Keywords—criptoanálisis, caja de sustitución, cifrado de imágenes.

I. Introducción

En la actualidad, debido a la demanda de seguridad de todos los procesos que requieren trabajar en línea, y el almacenamiento seguro de información confidencial, se han propuesto diversos algoritmos criptográficos con diferentes enfoques, entre ellos los de enfoque caótico. Esto debido a propiedades que tienen como ergodicidad y la sensibilidad a condiciones iniciales.

Por otra parte, el cifrado de contenido multimedia ha requerido el desarrollo de nuevos sistemas de cifrado, debido a que esta información requiere seguridad criptográfica y seguridad perceptual [1]. Para explicar esto, un ejemplo pueden ser las imágenes digitales, las cuales pueden contener una gran cantidad de datos, una alta redundancia y correlación adyacente. Para cifrar una imagen no solo se requiere proteger la información modificando su contenido de una forma segura (seguridad criptográfica), si no que la versión cifrada debe evitar revelar patrones de la imagen original (seguridad perceptual). Un ejemplo de cuando no se considera la seguridad perceptual se puede ver en la Fig. 1.

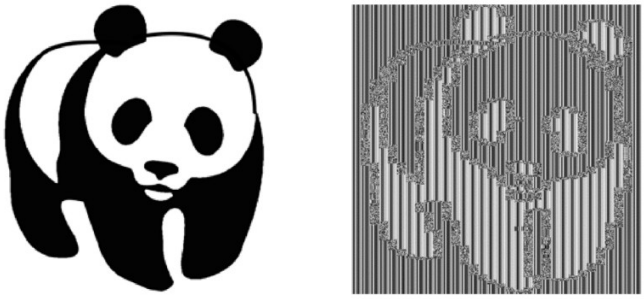

Fig. 1. a) Imagen original de dos tonos, b) versión cifrada de a) con el sistema AES en modo ECB.

Sin embargo, en muchas ocasiones estos nuevos sistemas presentan debilidades ante ataques de criptoanálisis y/o criptoanálisis diferencial. Provocando la fuga de información confidencial. Por ejemplo, en [2] utilizan una secuencia pseudoaleatoria generada por un sistema hipercaótico para cifrar las imágenes, utilizando la operación XOR y la suma modular. Este sistema fue analizado en el trabajo [3] y se encontraron debilidades al momento de aplicar el ataque Chosen-Plain Image

Attack (CPIA). Por otra parte, en [4] se propone un método de cifrado y de generación de cajas de sustitución basado en caos. Sin embargo, en 2018 en [5], Zhu junto con otros autores publicaron las debilidades del sistema propuesto por Çavuşoğlu et. al, bajo el ataque Chosen-Plaintext Attack (CPA). En [6] los autores proponen un algoritmo de cifrado de imágenes caótico, basado en la entropía de la información. En el mismo año, Li et. al, en [7] revelan los problemas de seguridad que presenta dicho sistema contra ataques diferenciales. Por lo que se puede ver, es necesario un análisis más profundo con diferentes escenarios para poder validar un nuevo sistema de cifrado.

En este trabajo se analiza una propuesta hecha por Majid Khan en [8], la cual presenta una debilidad ante el ataque CPIA. El sistema utiliza los parámetros iniciales de un sistema caótico como llave secreta para generar cajas de sustitución. Estas cajas son también llamadas S-box, en este sistema las emplean para cifrar imágenes sustituyendo los valores de los coeficientes de los píxeles. En el artículo original presentan una validación del sistema, principalmente basada en pruebas estadísticas y con poca variedad de imágenes. Por lo que, en esta investigación se busca describir a detalle el ataque, su justificación y referencia, para que en futuras propuestas contemplen una mayor variedad de pruebas de forma justificada.

Este artículo tiene la siguiente estructura, en la sección 2 se describe el sistema propuesto por Khan, tanto la generación de las cajas de sustitución como el algoritmo de cifrado. La sección 3 muestra el criptoanálisis aplicado paso a paso. Y finalmente, en la sección 4 se incluyen las conclusiones.

II. Descripción del sistema de cifrado

El sistema de cifrado propuesto por Khan [8] utiliza sistemas caóticos que suelen ser empleados en criptografía debido a su ergodicidad y a que son sensibles a condiciones iniciales. Dicho esquema está basado en un sistema caótico multi-paramétrico, utilizando la combinación de los sistemas de Lorenz y Rossler. El autor afirma que este sistema es altamente no lineal y tiene comportamiento caótico. El conjunto de ecuaciones de este sistema se muestra a continuación:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x) - y - z, \\ \frac{dy}{dt} &= rx - y - 20xz + x + ay, \\ \frac{dz}{dx} &= 5x - bz + \delta + x(x - c). \end{aligned} \tag{1}$$

Para el sistema de ecuaciones (1) se establecen los parámetros δ, r, a, b y c que son los que gobiernan las características de salida y los valores generados por el sistema.

El algoritmo de cifrado de imágenes es descrito a continuación:

1. Las trayectorias son generadas en el sistema caótico multi-paramétrico, seleccionando las condiciones iniciales.

2. Se colectan las muestras de la trayectoria de datos caóticos.

3. Aplicando una transformación afín, las muestras de la salida son ajustadas en un rango de 0 a 255.

4. Se conforma la S-box como una matriz de 16×16, utilizando las muestras ajustadas en el paso anterior.

5. Los píxeles de las imágenes que serán los datos de entrada a la S-box, son convertidos a números binarios de ocho bits.

6. Dicho número binario debe ser separado en dos bloques de cuatro bits, también llamados nibbles y convertidos nuevamente a base decimal.

7. La imagen cifrada se obtiene al usar los dos números (de cuatro bits) del paso 6 provenientes del coeficiente del pixel. Estos dos números serán usados como coordenadas de reglón y columna en la S-box. El número de los cuatro bits más significativos señala en la S-box, el renglón del valor de sustitución. Mientras que el número de los cuatro bits menos significativos señala la columna. El número localizado en la S-box se utiliza para sustituir el coeficiente del pixel en la imagen original. Este paso se repite hasta cifrar toda la imagen.

Para explicar con más detalle el paso 7 del algoritmo, suponga el caso de un píxel cuyo coeficiente es 21 (hex). En la Fig. 2 se puede ver una sección de la S-box del sistema AES. Los bits más significativos del valor de entrada 21 (hex), señalan el renglón 2, mientras que los menos significativos la columna 1. Por lo tanto, el valor 21 (hex) se sustituye por fd (hex).

Estos son todos los pasos que abarca el esquema de cifrado diseñado por Khan. Consta únicamente de una función de confusión que intercambia los valores de entrada (los coeficientes de píxel) por los valores de la caja de sustitución. El resto del artículo original lo dedica a validar el cifrado con pruebas estadísticas y criptoanálisis diferencial.

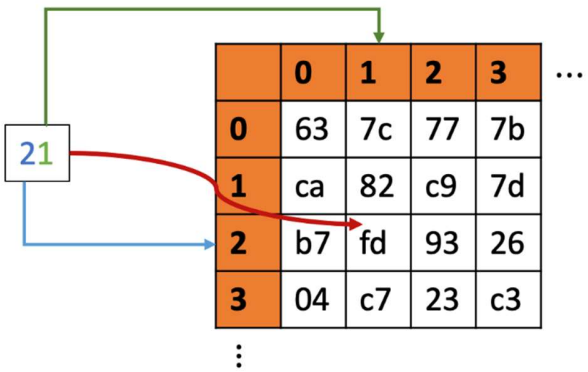

Fig. 2. Sustitución del valor 21 (hex) utilizando la caja de sustitución del sistema AES.

III. Criptoanálisis propuesto

Antes de comenzar a describir el ataque que se emplea en esta investigación, es importante definir lo que es una debilidad o ruptura en un sistema de cifrado. En [9] el autor define romper un método de cifrado, como encontrar una debilidad que puede ser explotada con menor complejidad que por fuerza bruta. Por lo tanto, es necesario aclarar que quizás se requieran cantidades irreales de conjuntos de textos conocidos o escogidos por el

atacante. Así como considerar que el adversario tiene habilidades que tal vez no sean posibles en el mundo real.

El ataque utilizado en este criptoanálisis es el Chosen Plain-Image Attack (CPIA), es una versión específica para imágenes del ataque Chosen Plaintext Attack, que ha sido utilizado en otros criptoanálisis, por ejemplo en [10] y [11]. En este ataque el adversario es capaz de escoger las imágenes en claro a la entrada del sistema, y obtener las respectivas imágenes cifradas. En este ataque el adversario tratará de encontrar alguna debilidad en el sistema sin conocer la llave secreta, utilizando únicamente las imágenes en claro y cifradas.

Debido a que es parte del propósito de este artículo servir como una explicación detallada de las pruebas de criptoanálisis, es conveniente aclarar que una vez especificadas las consideraciones del ataque, la forma en que se llevará a cabo no es única. Se pueden hacer diferentes usos con la información disponible, diferentes pruebas y análisis. Así como la selección de las imágenes en claro pueden tener diferentes propósitos. Por lo tanto, repetir un ataque tal cual como es reportado en algún artículo, para un nuevo sistema puede no ser concluyente para medir la calidad del cifrado. Antes de replicar algo, se debe analizar el porqué de las condiciones y si cumplen con los supuestos del ataque.

Una vez explicado esto, se procede a realizar el ataque. Las imágenes seleccionadas por el atacante son de 8 bits, de 256*256 pixeles y se muestran en la Fig. 3.

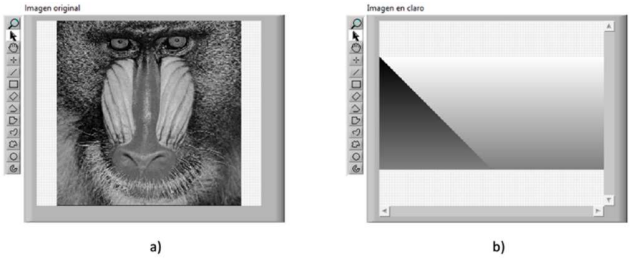

Fig. 3. Imágenes en claro. a) Imagen de mandril, ampliamente utilizada en el procesamiento de imágenes. b) Imagen hecha con todos los colores de la escala de grises de 8 bits.

La Fig. 3b) es en escala de grises a 8 bits (0 a 255), fue diseñada para aportar dos tipos de información en este ataque. Se sabe la localización y cantidad de píxeles con un valor de coeficiente específico. Es decir, cada color se repite un número único de veces. La imagen tiene dimensiones de 128×257, bajo el siguiente patrón:

$$\begin{bmatrix} 0 & 255 & 255 & \cdots & 255 \\ 1 & 1 & 254 & \cdots & 254 \\ \vdots & & \ddots & & \vdots \\ 127 & 127 & \cdots & 128 & \cdots & 128 \end{bmatrix} \quad (2)$$

Donde el primer renglón está formado por un píxel con el valor de 0 y 256 píxeles con el valor de 255. El segundo renglón contiene dos píxeles con el valor de 1 y 255 píxeles con el valor de 254. Así sucesivamente en cada renglón, un lado aumenta el número de píxeles de un valor, mientras que el número de píxeles del otro lado disminuye. El histograma es un gráfico para representar distribuciones de frecuencias de los valores de los píxeles, hecho con los valores de la Fig. 3b), el cual se ve de la siguiente manera:

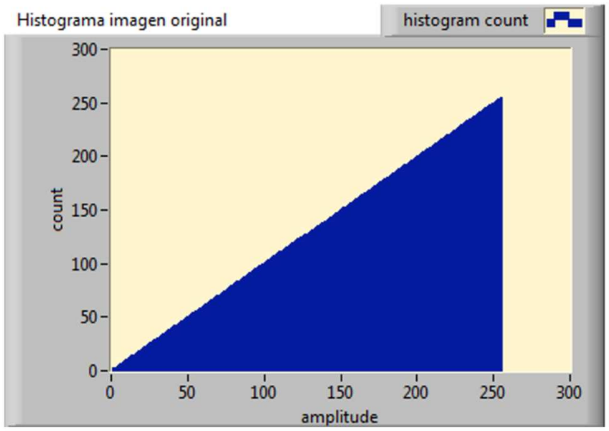

Fig. 4. a) Histograma de los coeficientes de los píxeles de la Fig. 3b).

Se pudo haber utilizado una imagen más sencilla, como la de la Fig. 5, que es igual a la imagen seleccionada en el criptoanálisis [12]. Es un barrido de todos los valores de 0 a 255. Sin embargo, pensando en más casos, nuestra propuesta serviría para sistemas de cifrado similares, incluso si estos tuvieran una operación de permutación. Las operaciones de permutación sirven para cambiar de posición a los píxeles, como por ejemplo las funciones de mapeo. Si el sistema propuesto por Khan o el sistema propuesto en [13], agregaran alguna función de mapeo, el criptoanálisis propuesto en [12] con la Fig. 5, no funcionaría ya que los pixeles se repiten en la misma frecuencia.

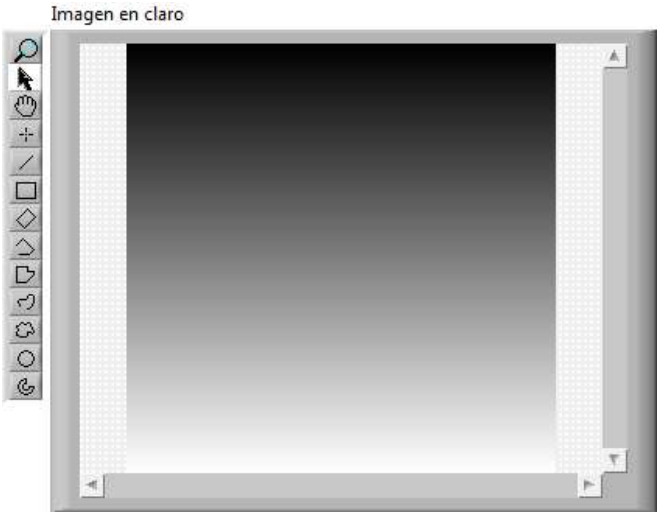

Fig. 5. Imagen en escala de grises de 256*256 pixeles, hecha con los valores de 0 a 255, un valor diferente por cada renglón.

Siguiendo con el ataque se seleccionan los parámetros iniciales del sistema caótico para poder generar la caja de sustitución. Para una mejor descripción se utilizará la caja de

sustitución reportada en el artículo por el autor, la cual se muestra a continuación

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	74	3	93	16	37	8B	5B	E1	A2	94	F2	14	77	2A	2B	F9
1	7D	C	9C	1C	32	7C	25	C2	A8	9F	D4	1A	7F	B	F7	52
2	85	15	A5	22	2D	6E	13	B9	AE	AA	D2	34	8F	6	72	66
3	8E	1E	AD	2C	20	5F	1	B0	B4	AF	D0	3A	90	23	69	DC
4	97	27	B6	31	19	4F	EF	A7	C1	BD	C9	48	89	33	58	9D
5	A0	30	BE	35	11	3F	DD	8C	CF	CA	C0	56	87	64	50	7E
6	A9	39	C6	3D	0	2F	CC	86	E4	D1	B7	5D	62	96	F	45
7	B2	43	CE	41	F6	1F	BA	81	F3	D5	B5	65	5C	FB	51	26
8	BB	4C	DE	44	EC	E	88	76	18	D8	B1	91	4E	D	6B	7A
9	C4	55	E6	46	E2	FD	78	73	2E	DB	AC	B8	47	17	95	FF
A	CD	5E	ED	49	D7	EB	68	71	36	E3	AB	4	FE	29	F5	63
B	D6	67	F4	4A	CB	DA	59	6F	53	E5	A3	21	D3	9A	9B	83
C	DF	70	FC	4D	BF	C8	3B	6D	5A	E7	A1	28	BC	57	D9	24
D	E8	79	2	4B	B3	A4	12	6C	61	E9	C3	42	98	38	F3	1D
E	F1	82	9	40	A6	92	5	84	75	EE	C7	54	1B	A	E0	9E
F	FA	8A	10	3C	99	80	F8	8D	7B	F0	8	6A	3E	60	C5	7

Fig. 6. Caja de sustitución reportada en [8].

Ambas imágenes en claro son cifradas con la misma caja de sustitución. El resultado se muestra en la Fig. 7.

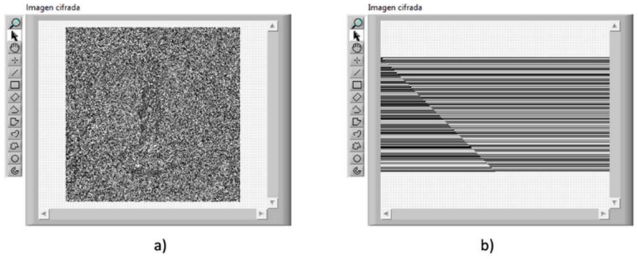

Fig. 7. Imágenes cifradas. a) Imagen del mandril cifrada. b) Imagen 3b) cifrada.

Si además analizamos el histograma de la Fig. 7b), obtendríamos la siguiente gráfica:

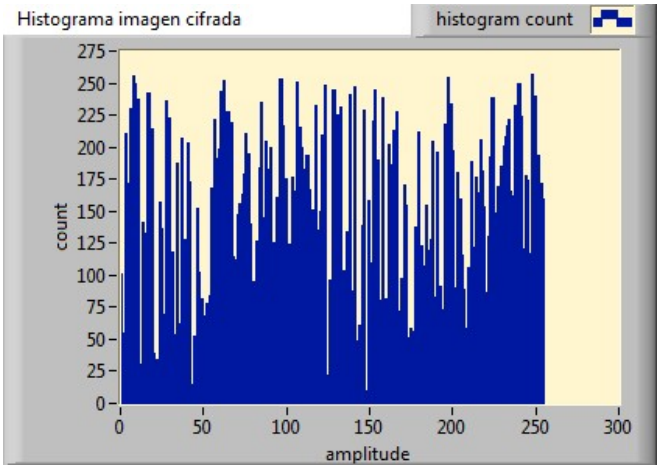

Fig. 8. Histograma de la Fig. 7b).

Como se puede ver, el sistema de cifrado no es capaz de ocultar la redundancia de la imagen original, solo intercambia los valores. Un buen sistema de cifrado arrojaría un histograma uniforme, sin importar la imagen de entrada. Esta debilidad nos permite romper el sistema, aquí se analizan dos formas, donde se podrían calcular una caja de sustitución inversa. La primera forma 1) Acorde a su posición en la imagen original. La Fig. 3b) sirve como referencia para saber la posición original de cada valor, mientras que en la imagen cifrada, Fig. 7b), permite analizar los nuevos valores de los píxeles, y acorde a su posición deducir el valor por el cual se intercambiaron los números de entrada 0, 1, 2, hasta 255. La segunda forma, 2) Haciendo un análisis de histograma. Utilizando el histograma de la imagen cifrada Fig. 7b) es posible deducir los valores por los cuales se intercambiaron los coeficientes de píxel. Esto debido a que se conoce el número de píxeles de cada valor en la imagen original, Fig. 3b). Por ejemplo, el valor que solo tenga un píxel originalmente era el valor de 0, el valor que tenga 2 píxeles era el valor 1 y así sucesivamente.

Utilizando las imágenes de las Fig. 3b) y 7b), y en caso de que se requiera, el histograma de la Fig. 8, es posible recuperar la Fig. 3a) a partir de la Fig. 7a) con un porcentaje del 100% de igualdad, sin conocer la llave de cifrado. El resultado se puede ver en la Fig. 9.

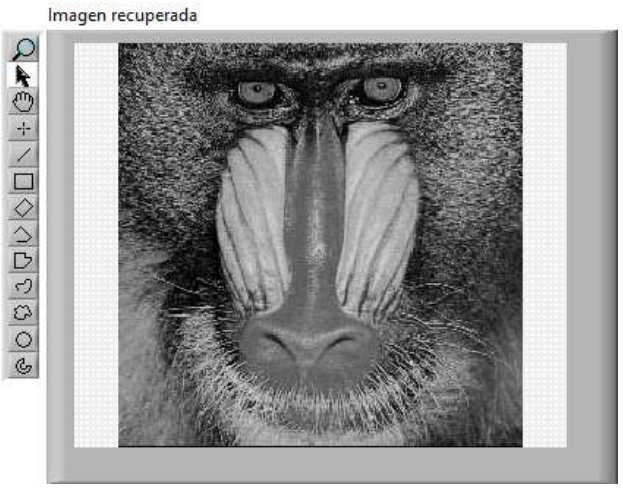

Fig. 9. Imágen recuperada de la Fig. 7b).

Como se puede ver, la imagen original del mandril se puede recuperar sin conocer la llave secreta. Se necesita solo una imagen conocida que contenga todos los valores de la codificación y se conozcan sus posiciones. Hay más ataques y vectores que podrían quebrar este sistema, por ejemplo si continúa con la Fig. 5, en la Fig. 10 podemos ver su versión cifrada. Esta imagen permite calcular la S-box inversa ya que la información no cambia de lugar, solo se sustituyen los valores. Por lo tanto el valor de renglón revela el valor original.

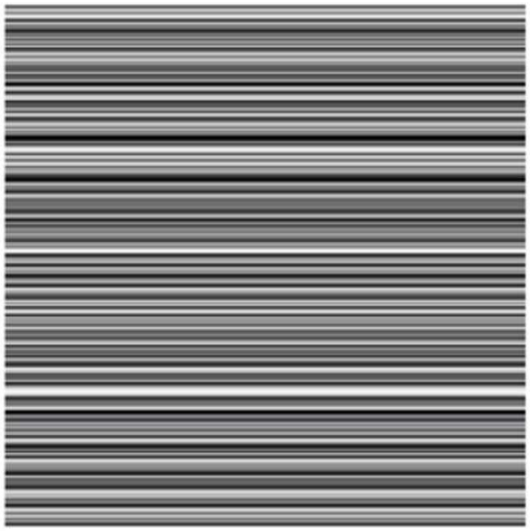

Fig. 10. Versión cifrada de la imagen 3b).

Otro vector de ataque es introducir 256 imágenes sólidas, es decir de un solo color, y con esa información calcular la S-box inversa. Incluso el sistema de cifrado también sería vulnerable al ataque Chosen Ciphertext Attack, al pasar la imagen de la Fig. 3b) por la operación de descifrado.

La condición de que ambas imágenes se cifraron con la misma caja de sustitución, o dicho de forma más general, que ambas imágenes fueron cifradas con la misma condición inicial, son parte de los aspectos que, si el sistema de cifrado no limita en sus pasos es válido aplicar de esta manera en el criptoanálisis. Como se mencionó anteriormente, en los criptoanálisis las reglas son un poco más flexibles, permitiendo considerar que el adversario puede hacer este tipo de acciones de cifrar con la misma condición inicial, como seleccionar las imágenes en claro, etc. Prueba de la utilidad de esto, es que los sistemas de cifrado avanzados pueden pasar estas pruebas, bajo las mismas consideraciones en los ataques.

IV. Conclusiones

En esta investigación se presenta un criptoanálisis a un sistema de cifrado para imágenes, basado en la generación de múltiples de cajas de sustitución a partir de un sistema caótico. El sistema de cifrado presenta una debilidad ante el ataque Chosen Plain-Image Attack, lo que implicaría que presenta debilidades ante otro tipo de ataques. Si el sistema hubiera sido evaluado con imágenes más simples, no hubiera pasado las pruebas estadísticas que reporta el autor en el artículo, desde la inspección visual. Otro problema que se puede señalar es que las cajas de sustitución generadas por el sistema caótico no son evaluadas. Cuando se propone un método de generación de cajas de sustitución, éstas se deben pasar por diversas pruebas, para confirmar que las cajas cumplen con ciertas propiedades. En la ref. [14] se puede consultar un trabajo de esa área donde se propone un método y se explican las pruebas a las que se someten las cajas.

Si se analizan los sistemas de cifrado que están bien establecidos como el AES (Advanced Encryption Standard), se puede ver que utilizan varias rondas con operaciones de confusión y difusión, incluyendo cajas de sustitución. Por lo tanto, la recomendación en el caso de diseño de sistemas de cifrado de imágenes, es hacer sistemas más robustos y combinar diversas operaciones para poder romper la alta correlación y la correlación adyacente.

Otra recomendación que se puede dar con este trabajo es que, al momento de diseñar sistemas de cifrado, se usen imágenes solidas que son el caso más simple, porque son de un solo color Si el sistema es bueno, será capaz de ocultar la alta redundancia de las imágenes en el cifrado. Esto se puede analizar calculando los histogramas.

Esperamos que este trabajo sirva de referencia para diseñadores de criptosistemas, y de esta manera contemplen aspectos de seguridad necesarios para poder pasar pruebas y ataques. Es muy importante evitar simplemente repetir punto a punto pruebas que se encuentran en la literatura, sin interpretar su porqué y si es aplicable al nuevo sistema que se esté diseñando.

References

[1] S. Lian, *Multimedia Content Encryption: Techniques and Applications*. Boca Raton, FL: CRC Press, 2008.

[2] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, Jan. 2012.

[3] C. Li, Y. Liu, T. Xie, and M. Z. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 2083–2089, Feb. 2013.

[4] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92–101, Feb. 2017.

[5] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box," *Symmetry*, vol. 10, no. 9, p. 399, Sep. 2018.

[6] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 01, p. 1850010, Jan. 2018.

[7] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[8] M. Khan, "A novel image encryption scheme based on multiple chaotic S-boxes," *Nonlinear Dynamics*, vol. 82, no. 1, pp. 527–533, Apr. 2015.

[9] B. Schneier, "A self-study course in block-cipher cryptanalysis," *Cryptologia*, vol. 24, no. 1, pp. 18–33, Jan. 2000.

[10] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 167, p. 107286, Jan. 2020.

[11] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, no. 8, pp. 1035–1039, Jul. 2009.

[12] M. Ahmad, M. N. Doja, and M. S. Beg, "Cryptanalysis and improvement of an image encryption scheme using Fourier series," *3D Research*, vol. 8, no. 4, pp. 1–11, Dec. 2017.

[13] M. Khan, "A novel image encryption using Fourier series," *Journal of Vibration and Control*, vol. 21, no. 16, pp. 3450–3455, Nov. 2015.

[14] J. A. Aboytes-González, J. S. Murguía, M. Mejía-Carlos, H. González-Aguilar, and M. T. Ramírez-Torres, "Design of a strong S-box based on a matrix approach," *Nonlinear Dynamics*, vol. 94, no. 3, pp. 2003–2012, Nov. 2018.