Algoritmo de Encriptamiento Basado en Sincronización de Sistemas Caóticos

Juan J. Montesinos García, Rafael Martínez-Guerra* y Sergio M. Delfín Prieto

Departamento de Control Automático, CINVESTAV-IPN, Av. IPN 2508, Col. San Pedro Zacatenco, C.P. 07360, Ciudad de México, México. (e-mail: jmontesinos, rguerra, sdelfin@ctrl.cinvestav.mx)

Resumen: En este artículo se propone el uso de la sincronización de sistemas caóticos de Liouville para el encriptamiento de imágenes. El algoritmo de encriptamiento aprovecha los beneficios de los algoritmos por bloques y evita sus desventajas como son la necesidad de mensajes de tamaños fijos y pequeños, también elimina la vulnerabilidad a ataques de mensaje escogido (*chosen-plaintext attack*) y mensaje conocido (*known-plaintext attack*), todo esto se logra al usar las propiedades de los sistemas de Liouville en combinación con fractales como los conjuntos de Julia.

1. INTRODUCCIÓN

La sincronización de sistemas caóticos ha tenido grandes avances por sus usos potenciales L. O. Chua (1992), Ö. Morgül (1996), en especial se han conseguido importantes resultados en comunicaciones seguras M. F. Hassan (2014), G. Alvarez (2006). En este campo el objetivo es encriptar datos usando señales obtenidas de algún oscilador caótico, para esto, una de las soluciones más comunes es diseñar el receptor como un observador de estados con el cual se genera la sincronización de los estados del oscilador y de este modo recuperar la información que fue encriptada con sus estados R. Martínez-Guerra (2015), J. Castro-Ramírez (2015). El algoritmo de encriptamiento que se propone en este artículo usa la sincronización en el esquema maestro-esclavo, de modo que el transmisor es el sistema maestro y el esclavo será el receptor, este último debe reconstruir las trayectorias del maestro a partir de una señal dada por el maestro para así recuperar el mensaje cifrado.

Los algoritmos de encriptamiento por bloques dependen de dos etapas básicas: una de difusión (*diffusion*) y otra de mezcla (*shuffling*), en la primera etapa la información es combinada con datos aleatorios dados por un oscilador caótico y en la segunda los lugares que ocupan los datos de la etapa previa son mezclados a partir de datos provistos por el oscilador, sin embargo, estas operaciones no garantizan que el mensaje se mantenga seguro y muchos de estos algoritmos son vulnerables a ataques de mensaje conocido y mensaje escogido, también este tipo de algoritmo requiere que los mensajes sean de tamaño fijo facilitando aún más la implementación de criptoanálisis. El algoritmo presentado tendrá las ventajas de los algoritmos de bloques pero será resistente a este tipo de ataques permitiendo que el proceso de encriptamiento sea rápido aún si el mensaje es considerablemente grande y sin importar las dimensiones de éste. Estas propiedades se obtienen al tomar las ventajas que da trabajar con sistemas de Liouville para la reconstrucción de estados y usando las propiedades de los fractales para modificar los números pseudo aleatorios obtenidos del oscilador para reducir la viabilidad de realizar criptoanálisis.

Este artículo está organizado de la siguiente manera: en la Sección 2 se presenta el algoritmo de encriptamiento. En la Sección 3 se da una explicación detallada de los receptores y cómo desencriptar el mensaje. En la Sección 4 se presentan resultados numéricos. En la Sección 5 se plantea la posible vulnerabilidad del algoritmo. Finalmente en la Sección 6 se dan las conclusiones.

2. ENCRIPTAMIENTO

2.1 Generación de números pseudo aleatorios

La clase de sistema que será introducido en la siguiente definición será necesaria para la elección del sistema caótico.

Definición 1. Un sistema es denominado de Liouville si sus variables de estados pueden ser descritos como una expresión en términos de integrales o exponenciales de integrales de la salida y algunas de sus derivadas temporales.

Para ejemplificar esta definición, considere el siguiente sistema.

Ejemplo. Las ecuaciones que describen al oscilador de Colpitts están dadas como:

$$\begin{aligned} \dot{x}_1 &= x_2 - f(x_3) \\ \dot{x}_2 &= -x_1 - bx_2 - x_3 \\ \dot{x}_3 &= x_2 - d \\ y &= x_2 \end{aligned} \tag{1}$$

donde:

$$f(x_3) = \begin{cases} -a(x_3+1) & x_3 < -1 \\ 0 & x_3 \geq -1 \end{cases}$$

[1] *Corresponding author.

El transmisor basado en el oscilador de Colpitts puede ser descrito como sigue:

$$\begin{aligned} x_1 &= -\dot{y} - by - \int (y-d) \\ x_2 &= y \\ x_3 &= \int (y-d) \end{aligned} \tag{2}$$

Mostrando así que este sistema caótico es de Liouville.

Para comunicaciones seguras, es necesario generar una secuencia de números, y los osciladores caóticos son una fuente de números pseudo aleatorios, en este caso el oscilador de Colpitts será usado ya que es un sistema de Liouville, pero también tiene propiedades para encriptamiento como una dinámica acotada y estable, además que depende en gran medida de las condiciones iniciales.

2.2 Algoritmo de encriptamiento

El proceso de encriptamiento consiste en la difusión y mezcla de la imagen plana, estas etapas dependerán de la llave y el mensaje causando que los ataques del tipo mensaje conocido o mensaje escogido sean difíciles de implementar. En la descripción del algoritmo, el mensaje será asumido como una imagen a color RGB, este algoritmo no está limitado a imágenes sino también puede ser aplicado a mensajes de texto. Considere la imagen RGB dada por $P \in \mathbb{Z}^{m\times n\times 3}$ compuesta por las tres matrices P_r, P_g y P_b de tamaño $m \times n$.

La llave es un conjunto de caracteres hexadecimales, suficientemente largo para obtener la información requerida para el proceso de encriptamiento, la llave será compuesta como se muestra a continuación:

$$K_{ey} = K_1 - K_2 - K_3 - K_4 - \cdots - K_l$$

Cada segmento de la llave será identificada como $K_i = ABCD$ con $1 \leq i \leq l$. Todo segmento de la llave contiene información sobre el proceso de encriptamiento, tales como: condiciones iniciales, parámetros del sistema, tiempo de muestreo, ganancias, etcétera. El algoritmo de encriptamiento se describe a continuación.

Paso 1. Crear las condiciones iniciales para el oscilador caótico.

$$xo_1 = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} P(i,j,1)}{255mn} \tag{3}$$

Entonces $xo_1 \in (0,1)$ y puede ser usado como la condición inicial para el estado x_1. Este procedimiento debe ser repetido para los otros dos estados usando las matrices restantes.

Paso 2. Generar con la primera sección de la llave los parámetros del oscilador caótico. El oscilador de Colpitts tiene tres parámetros, el primero puede ser formado por $K_1 = ABCD$, el parámetro a es obtenido como:

$$a = \frac{ABCD}{FFFF}$$

donde $a \in (0,1)$, este paso debe ser repetido para los parámetros restantes del oscilador (b y d).

Paso 3. Usar el oscilador caótico para generar una secuencia de datos. Una vez que los parámetros del oscilador y la condición inicial han sido obtenidos, se debe generar suficientes datos para proveer números pseudo aleatorios necesarios para realizar las operaciones de difusión y mezcla.

Paso 4. Con la segunda sección de la llave K_2 obtener números desde las trayectorias de los estados del oscilador. Para esto se crea la matriz k_s basado en el estado x_n del oscilador y un tiempo de muestreo t especificado en la segunda sección de la llave, el cual tiene la siguiente forma:

$$t = \left(\frac{ABCD}{FFFF}\right) 10^{1-E} \tag{4}$$

y la matriz es dada por:

$$k_s = \begin{bmatrix} x_1(t) & x_2(t) & \cdots & x_n(t) \\ x_1(2t) & x_2(2t) & \cdots & x_n(2t) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(nt) & x_2(nt) & \cdots & x_n(nt) \end{bmatrix} \tag{5}$$

Entonces la matriz k_s será modificada por una transformación no invertible tal que la relación entre la etapa de difusión y la etapa de mezclado sea disminuida, esta transformación será dada a través del conjunto de Julia Z. Yong-Ping (2008):

$$Z_{n+1} = Z_n^2 + b, \quad n \in [1,\alpha], \quad b \in \mathbb{C} \tag{6}$$

$$\begin{aligned} b &= c + di \\ c &= \frac{ABCDE}{2FFFFF} \\ d &= \frac{ABCDE}{2FFFFF} \\ i &= \sqrt{-1} \end{aligned} \tag{7}$$

La llave proveerá del valor de b y el número de iteraciones para el conjunto de Julia, esto es, $\alpha = ABCDE$, seleccionando $b = c + di$ garantiza que los valores proporcionados por el fractal están dentro del atractor. El conjunto de Julia que requiere números complejos hará posible modificar aún más las cifras dadas por el sistema de Liouville y haciendo muy difícil averiguar qué números produjo el orden de la mezcla y los valores de la difusión, la condición inicial será hecha por el valor de $x_n(t_n)$ y otro elemento de la llave:

$$Z_0 = \left[0{,}5 - \frac{x_n(t_n)}{ABCDE}\right] + \left[\frac{x_n(t_n)}{ABCDE}\right] i$$

Finalmente, la transformación será la norma del valor complejo dado por el conjunto de Julia:

$$T(x_n) = |Z_n|$$

Entonces la matriz k_s es transformada en la matriz k_{st} aplicando la transformación a cada elemento:

$$k_{st} = T(k_s) = \begin{bmatrix} Z_{1,t_1} & Z_{2,t_1} & \cdots & Z_{n,t_1} \\ Z_{1,t_2} & Z_{2,t_2} & \cdots & Z_{n,t_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_{1,t_n} & Z_{2,t_n} & \cdots & Z_{n,t_n} \end{bmatrix} \quad (8)$$

El valor t_n denota el muestreo tomado desde los estados x_n en el tiempo $n \cdot t$.

Paso 5. Crear la mezcla y difusión de valores de los números previamente generados, el vector de difusión D_v es construido desde k_{st}:

$$\begin{aligned} D_{v1} &= [Z_{1,t_1} \;\; Z_{2,t_1} \;\; \cdots \;\; Z_{n,t_1}] \\ D_{v2} &= [Z_{1,t_2} \;\; Z_{2,t_2} \;\; \cdots \;\; Z_{n,t_2}] \\ D_{v3} &= [Z_{1,t_n} \;\; Z_{2,t_n} \;\; \cdots \;\; Z_{n,t_n}] \end{aligned} \quad (9)$$

y se combina con la imagen por medio de la operación binaria $\oplus$ (XOR) para producir la imagen parcialmente encriptada P_{c1}:

$$\begin{aligned} P_{cr1} &= P_r \oplus D_{v1} \\ P_{cg1} &= P_g \oplus D_{v2} \\ P_{cb1} &= P_b \oplus D_{v3} \end{aligned} \quad (10)$$

$$P_{c1} = P \oplus D_v \quad (11)$$

Con el vector transformado k_{st} se crea el vector de mezcla con tantos elementos como lo requiera el mensaje:

$$\begin{aligned} S_{v1} &= [\, Z_{1,t_1} \;\; Z_{1,t_2} \;\; \cdots \;\; Z_{1,t_{mn}} \,] \\ S_{v2} &= [\, Z_{2,t_1} \;\; Z_{2,t_2} \;\; \cdots \;\; Z_{2,t_{mn}} \,] \\ S_{v3} &= [\, Z_{3,t_1} \;\; Z_{3,t_2} \;\; \cdots \;\; Z_{3,t_{mn}} \,] \end{aligned} \quad (12)$$

$$S_v = sort(S_{v1}, S_{v2}, S_{v3}), \quad S_v \in \mathbb{R}^{mn} \quad (13)$$

Se ordenan los elementos del vector de mezcla S_v y reordenar los elementos de la imagen parcialmente encriptada P_{c1} de acuerdo con el orden de los elementos del vector de mezcla para formar P_{c2}.

$$P_{c2} = sort(P_{c1}, S_v) \quad (14)$$

La imagen encriptada será P_{c2}.

3. RECUPERACIÓN DEL MENSAJE

Para recuperar el mensaje encriptado será necesario reconstruir las trayectorias del oscilador de Liouville, entonces mediante el uso de la llave es posible construir el vector de difusión D_v y el vector de la mezcla S_v, los estados del oscilador serán reconstruidos de dos maneras: uno mediante un observador de estados y el otro por medio de las propiedades de Liouville del sistema, y finalmente se recupera la imagen encriptada. La imagen cifrada P_{c2} es reordenada en función de S_v para producir P_{c1} y después la operación XOR es aplicada con D_v, proporcionando la imagen o texto original.

3.1 Receptor polinomial exponencial

La función del observador polinomial exponencial es estimar los estados de un sistema no lineal, este tiene una estructura similar al observador de Luenberger generalizado con la ventaja de que tiene más vectores de ganancias y además hará del error de sincronización decrecer exponencialmente. La dinámica del observador es dada por:

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + \psi(\hat{x}) + \sum_{i=1}^{m} K_i (y - C\hat{x})^{2i-1} \\ \hat{y} &= C\hat{x} \end{aligned}$$

donde $\hat{x} \in \mathbb{R}^n$ son los estados del observador, y es la salida del transmisor, $\psi(\hat{x})$ es la parte no lineal del transmisor el cual satisface la condición de Lipschitz y $K_i \in \mathbb{R}^n$, $1 \leq i \leq m$ son los vectores de ganancias del observador. Las siguiente suposiciones serán necesarias durante los resultados teóricos:

A.1. Para un $\varepsilon > 0$ y $A \in \mathbb{R}^{n \times n}$ existe una matriz $P = P^T > 0$, $P \in \mathbb{R}^n$ que es la solución de la ecuación algebraica:

$$A^T P + PA + L^2 P^2 + (1 + \varepsilon) I = 0$$

A.2. La parte no lineal del transmisor $\psi(\hat{x})$ satisface la condición:

$$2\hat{x}^T P \psi(\hat{x}) \leq L^2 \hat{x}^T P^2 \hat{x} + \hat{x}^T \hat{x}$$

3.2 Estabilidad

Demostración 1. La dinámica del error de sincronización es dada por $\dot{e} = \dot{x} - \dot{\hat{x}}$:

$$\begin{aligned} \dot{e} = \; & Ax + \psi(x) - ... \\ & \cdots - \left(A\hat{x} + \psi(\hat{x}) + \sum_{i=1}^{m} K_i (y - C\hat{x})^{2i-1} \right) \end{aligned}$$

y teniendo en cuenta que una simple variable de estado será usado como salida, entonces es posible hacer:

$$\dot{e} = A(e) + \phi(e) - \sum_{i=1}^{m} K_i C e^{2i-1}$$

donde:

$$\phi(e) = \psi(x) - \psi(\hat{x})$$

Debido a A.2 la parte no lineal del error $\phi(e)$ satisface la condición:

$$2e^T P \phi(e) \leq L^2 e^T P^2 e + e^T e$$

La siguiente función candidata de Lyapunov es propuesta:

$$V = e^T P e$$

y entonces, al calcular la derivada:

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e}$$
$$\dot{V} = \left[A(e) + \phi(e) - \sum_{i=1}^{m} K_i C e^{2i-1} \right]^T Pe + e^T P \left[A(e) + \phi(e) - \sum_{i=1}^{m} K_i C e^{2i-1} \right]$$
$$\dot{V} \leq e^T \left(A^T P + PA + L^2 P^2 + I \right) e - 2e^T P \sum_{i=1}^{m} K_i C e^{2i-1}$$

Teniendo en cuenta que nuestro interés se centra en los observadores de orden dos o más ($m \geq 2$):

$$2e^T P \sum_{i=1}^{m} K_i C e^{2i-1} = 2e^T P K_1 C e + (Ce)^2 2e^T P K_2 C e + \cdots + (Ce)^{2m-2} 2e^T P K_m C e$$

Definase $M_1 = PK_1C$, $M_2 = PK_2C, \cdots$, $M_m = PK_mC \geq 0$ y ya que $e^T M_m e$ son números escalares $e^T M_m e = \left[e^T M_m e\right]^T$, por tanto:

$$\begin{aligned} & (Ce)^0 e^T M_1 e + (Ce)^1 \left(e^T M_1 e\right)^T \\ & \cdots + (Ce)^2 e^T M_2 e + (Ce)^2 \left(e^T M_1 e\right)^T \\ & \cdots (Ce)^{2m-2} e^T M_m e + (Ce)^{2m-2} \left(e^T M_m e\right)^T \\ = & \sum_{i=1}^{m} (Ce)^{2i-2} e^T \left(M_i + M_i^T\right) e \end{aligned}$$

La última ecuación muestra que $2e^T P \sum_{i=1}^{m} K_i C e^{2i-1}$ es definida positiva, el único término que queda por hacer definida negativa es:

$$\dot{V} \leq e^T \left(A^T P + PA + L^2 P^2 + I \right) e$$

De acuerdo a la suposición A.1: $A^T P + PA + L^2 P^2 + I \leq -\varepsilon I$ y en consecuencia $\dot{V} \leq -\varepsilon \|e\|^2$. Considere que $V = \|e\|^2$ entonces $\alpha \|e\|_P^2 \leq V \leq \gamma \|e\|_P^2$, $\alpha = \lambda_{min}(P)$, $\gamma = \lambda_{max}(P)$, por tanto:

$$\frac{d}{dt} \|e\| \leq -\frac{\varepsilon}{2\gamma} \|e\|$$
$$\|e(t)\| \leq \sqrt{\frac{\gamma}{\alpha}} \|e(0)\| exp\left(-\frac{\varepsilon}{2\gamma} t\right)$$

Haciendo $\xi = \sqrt{\frac{\gamma}{\alpha}} \|e(0)\|$ y $\lambda = \frac{\varepsilon}{2\gamma} t$:

$$\|e(t)\| \leq \xi exp(-\lambda t)$$

■

Este resultado muestra que los estados del oscilador pueden ser reconstruidos y el error de reconstrucción decrecerá tanto como el tiempo se incrementa.

3.3 Receptor basado en las propiedades de Liouville del sistema

El diseño del receptor está basado en las propiedades de Liouville del sistema (ver definición 2), esta propiedad permite reconstruir los estados de un sistema sin la necesidad de un observador de estado, entonces es posible crear receptores que no serán afectados por las limitaciones de un observador, y sin embargo, conservarán la mayoría de sus características de seguridad. La dinámica receptor viene dada por:

$$\begin{aligned} \dot{\hat{x}}_1 &= y - f\left[\int (y-d)dt\right] \\ \hat{x}_2 &= y \\ \hat{x}_3 &= \int (y-d)dt \end{aligned} \tag{15}$$

con este receptor, el error en la sincronización es cero:

$$\mathbf{e} = \begin{bmatrix} x_1 - \hat{x}_1 \\ x_2 - \hat{x}_2 \\ x_3 - \hat{x}_3 \end{bmatrix} = 0 \tag{16}$$

$$= \begin{bmatrix} \int \left(y - f\left[\int (y-d)dt\right]\right) dt - \int \left(y - f\left[\int (y-d)dt\right]\right) dt \\ y - y \\ \int (y-d)dt - \int (y-d)dt \end{bmatrix}$$

Esta reconstrucción requiere que las condiciones iniciales del estado de salida x_2 sean conocidas, esto hace que el algoritmo de encriptamiento sea ligeramente diferente, la condición inicial de la salida es formada por la primera sección de la llave:

$$x_2(0) = \left(\frac{ABCD}{FFFF}\right) E$$

El resto de las condiciones iniciales x_1 y x_3 estarán formadas por la imagen normal de la misma manera que se hizo en el caso del observador, con esta modificación las trayectorias del oscilador caótico dependerán de la imagen y la llave, en consecuencia, si el mensaje cambia también lo hará el orden de los valores de mezcla y de difusión. Una ventaja importante de estas propiedades del sistema sobre el observador de estado es que no hay ningún error en la reconstrucción de los estados ni hay un tiempo de espera de los estados del observador para llegar a los estados del oscilador caótico.

El proceso para recuperar la información consiste en reconstruir los estados del oscilador y con la llave siguiendo los pasos del algoritmo se vuelven a construir los vectores de difusión y mezcla, con estas reconstrucciones la imagen encriptada es reordenada y la difusión se elimina por medio de bitwise XOR para obtener la imagen original.

4. RESULTADOS NUMÉRICOS

Para probar la eficacia del algoritmo de encriptamiento se usará una imagen a color, el encriptamiento de la imagen estará basado en las trayectorias generadas por el oscilador de Colpitts a partir de las cuales se generan los vectores para la difusión y la mezcla de la imagen a encriptar. Los parámetros del receptor se ajustan de acuerdo a la llave, lo que permite una sincronización exitosa con la que se reconstruyen los datos necesarios para recuperar la imagen

encriptada, las ganancias del observador se calculan con la desigualdad $PK_iC > 0$, obteniendo $k_1 = [0{,}16, 16, 0{,}8]^T$ y $k_2 = [0{,}91, 2{,}15, 0]^T$. A continuación se muestra la imagen que se usará para probar el algoritmo.

Figura 1. Imagen a encriptar

Los resultados obtenidos se muestran en las siguientes imágenes, la primera es producida por el observador y la segunda por la reconstrucción:

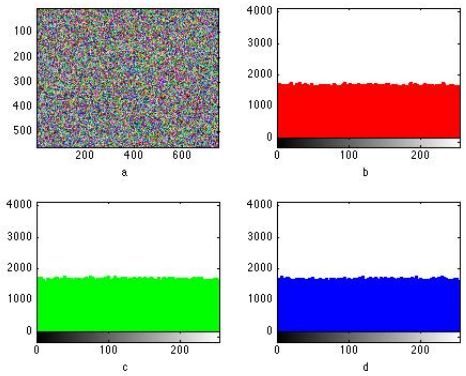

Figura 2. Imagen encriptada por el observador (a) y sus histogramas rojo (b), verde (c) y azul (d)

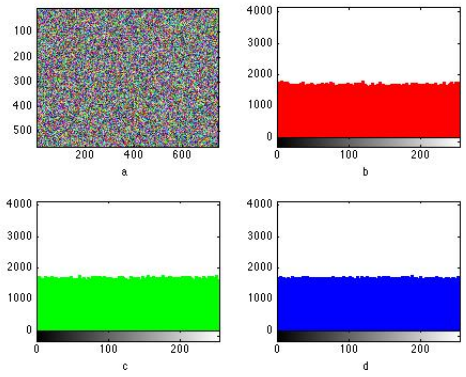

Figura 3. Imagen encriptada por la reconstrucción (a) y sus histogramas rojo (b), verde (c) y azul (d)

El error presente en el observador de estados hace que deba usarse menor precisión al calcular los vectores de difusión y mezcla reduciendo la habilidad del algoritmo de resistir ataques por fuerza bruta, en el caso de la reconstrucción esto no es necesario ya que no existe error en la reconstrucción de los estados. Las imágenes recuperadas por ambos receptores se muestran enseguida:

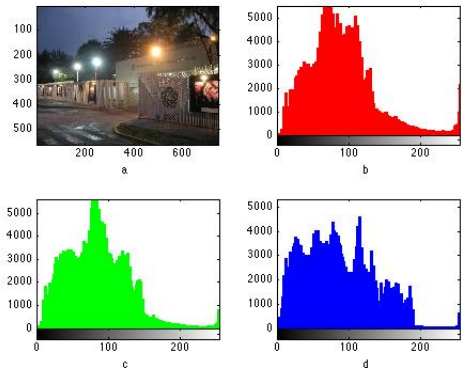

Figura 4. Imagen recuperada por el observador (a) y sus histogramas rojo (b), verde (c) y azul (d)

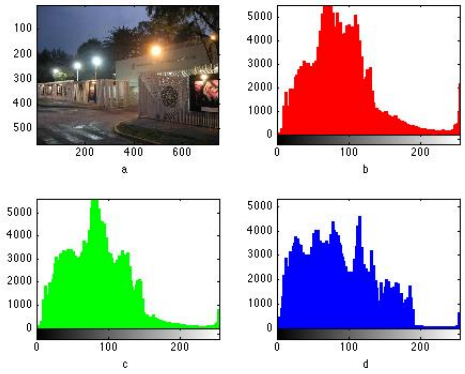

Figura 5. Imagen recuperada por la reconstrucción (a) y sus histogramas rojo (b), verde (c) y azul (d)

Ambos receptores son capaces de reconstruir con gran precisión la imagen encriptada, sin embargo, la reconstrucción hace que sea posible usar llaves mas largas por su falta de error.

5. VULNERABILIDAD AL CRIPTOANÁLISIS

Por lo regular los algoritmos de encriptamiento por bloques son susceptibles a ataques de mensaje conocido y mensaje escogido, estos algoritmos encriptan información mediante operaciones de difusión a través de la función binaria XOR y un proceso de mezcla de datos. En el caso de ataques de mensaje escogido, un atacante puede escoger el mensaje a enviar y tener acceso al mensaje encriptado, con el fin de que al escoger estos mensajes adecuadamente se puedan recuperar tanto el vector de difusión como el orden de la mezcla de los datos, de modo que si no se cambia la llave en cada mensaje se logra un algoritmo ineficaz ante este tipo de irrupciones. El algoritmo presentado evita esta fragilidad al hacer que los vectores de difusión y el orden de la mezcla dependan tanto de la llave como de los datos encriptados, por lo tanto cada mensaje diferente tendrá vectores de difusión y mezcla diferentes haciendo que sea inútil este tipo de ataques pues, aunque se descubra el vector de difusión y orden de la mezcla para un mensaje seleccionado por el atacante, estos

vectores serán inútiles al momento de intentar obtener otro mensaje distinto encriptado aun con la misma llave. Para probar esto implementamos un ataque de mensaje escogido básico, primero enviamos una imagen negra para recuperar el vector de difusión y después otra imagen conteniendo valores en orden ascendente para recuperar el orden de la mezcla, una vez teniendo estos valores se intentara recuperar la imagen previamente encriptada con estos datos, la imagen usada para el ataque es la siguiente:

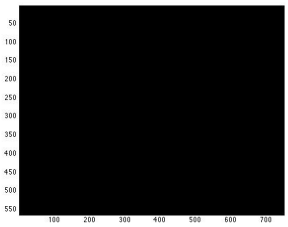

Figura 6. Imagen negra para ataque

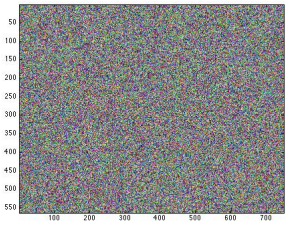

Figura 7. Vector de difusión recuperado

Al intentar recuperar la figura 1 a partir de la figura 3 usando la información recabada por medio del ataque se tiene el siguiente resultado:

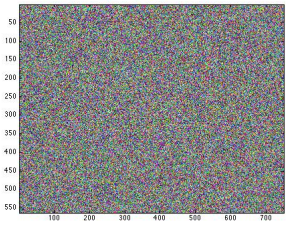

Figura 8. Vector de difusión recuperado

Como puede apreciarse en la imagen anterior el ataque es completamente ineficaz, incluso el vector de difusión recuperado no corresponde al orden de la mezcla recuperada pues se utilizaron mensajes distintos para obtener cada uno, por lo cual, cada mensaje tendrá parejas de vectores distintas, por lo tanto el algoritmo puede soportar este tipo de ataques.

6. CONCLUSIONES

Al usar la naturaleza caótica del oscilador fue posible obtener vectores de difusión y mezcla con grandes variaciones, además, el algoritmo permite que la generación de estos vectores dependan enteramente del mensaje original, esto permite obtener considerables beneficios como evitar la vulnerabilidad a ataques de mensaje conocido y mensaje escogido. Uno de los ataques más recurrentes para quebrar algoritmos de cifrado está enfocado en recuperar la llave de manera similar a la mostrada en los ataques previos, sin embargo, éstos resultarán ineficaces al utilizar los conjuntos de Julia. Este conjunto se emplea para modificar los valores aleatorios dados por el oscilador al recurrir a la norma de los números complejos generados por dicho conjunto, estableciéndose de esta manera una infinidad de posibles combinaciones que darán el mismo resultado, es decir, que para un valor de la norma le corresponde una infinidad de números complejos, haciendo que no sea posible rescatar los valores exactos de las trayectorias del oscilador sin recurrir a la llave, y en consecuencia, los parámetros del oscilador se mantienen separados del mensaje encriptado evitando que puedan recuperarse por medio de las técnicas más comunes de criptoanálisis. El algoritmo posee los beneficios del encriptamiento por bloques como son la rapidez para encriptar y desencriptar, el uso de la misma llave para todos los mensajes, pero además se puede procesar mensajes de tamaño variable e incluso muy grandes como una imagen a color, esto a diferencia de los algoritmos por bloques más comunes que requieren mensajes de tamaño fijo. Cabe mencionar que al usar las propiedades de los sistemas de Liouville se mejora considerablemente las características de seguridad del algoritmo, pues permite usar llaves considerablemente más largas, aumentando la cantidad de llaves totales que pueden existir y dando un margen más amplio para la creación de vectores de difusión y mezcla.

REFERENCIAS

L. O. Chua, L. Kocarev, K. Eckert and M. Itoh, Experimental Chaos Synchronization in Chua's Circuit, International Journal of Bifurcation and Chaos, 2(3), 705-708, 1992.

Ö. Morgül, and E. Solak, Observer Based Synchronization of Chaotic Systems, Physical Review E, 54(5), 4803, 1996.

G. Alvarez and S. Li, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, International Journal of Bifurcation and Chaos, 16(8), 2129-2151, 2006.

Z. Yong-Ping and L. Shu-Tang, Gradient Control and Synchronization of Julia Sets, Chinese Physics B 17, 543-549, 2008.

M. F. Hassan, Observer Design for Constrained Nonlinear Systems with Application to Secure Communication, Journal of the Franklin Institute, 351(2), 1001-1026, 2014.

J. Castro-Ramírez, R. Martínez-Guerra and J. C. Cruz-Victoria, A New Reduced-Order Observer for the Synchronization of Nonlinear Chaotic Systems: an Application to Secure Communications, Chaos: An Interdisciplinary Journal of Nonlinear Science, 25(10), 103128, 2015.

R. Martínez-Guerra, G. C. Gómez-Cortés and C. A. Pérez-Pinacho, Synchronization of Integral and Fractional Order Chaotic Systems a Differential Algebraic and Differential Geometric Approach with Selected Applications in Real-Time, Springer, 2015.