Encryption of RGB Images by Means of a Novel Cryptosystem Using Elliptic Curves and Chaos

E. Hernández-Díaz, H. Pérez-Meana, and V. Silva-García

***Abstract*—A new symmetric cryptosystem is proposed in this paper which will be used to carry out image encryption without compression. The proposed system has been developed to encrypt images in BMP format. A significant contribution of this investigation is the use of one solution point of a zero valued constant elliptic curve in order to generate a set of 15 encryption keys. On the other hand, using a differential equation that produce chaotic numbers a permutation and its inverse permutation are generated. Every encryption key and both permutations are the same size as the image. The proposed cryptosystem is tested for the purpose of verifying its resistance against several cryptographic attacks as well as the randomness and quality of its ciphering. Results are showed and compared with some recent scientific articles published between 2017 and 2019.**

***Index Terms*—Elliptic-curve cryptography, Advanced encryption standard, Chaos, Randomness, Symmetric cryptosystem.**

I. Introducción

LAS imágenes, pueden ser copias o escaneos de documentos importantes considerados como información sensible. La criptografía usa algoritmos (principalmente matemáticos), para proteger la información, haciéndola ininteligible para atacantes capaces de interceptarla durante su proceso de transmisión.

El criptosistema propuesto cifra imágenes BMP, ya que, en el país de origen de esta investigación, México, existen regulaciones que no permiten la pérdida de información en documentos importantes que son cifrados [1]. El criptosistema diseñado es simétrico, se ejecuta en 14 rondas y es del tipo Substitution Permutation Network [2]. Sus llaves de cifrado se generan haciendo uso de una Curva Elíptica cuya constante es cero. Por otro lado, usando la ecuación diferencial de Robert May mostrada en (13), se encuentran las coordenadas x, y del elemento generador de la Curva Elíptica, y se construye una permutación y su inversa que se aplican durante el cifrado para agregar difusión. Además, en la ejecución del esquema se emplea la S-Box de AES [3], para agregar confusión. Finalmente, las llaves de cifrado se generan con puntos solución de Curvas Elípticas, por su conocida resistencia ante el ataque del logaritmo discreto [4], de este modo, las llaves de cifrado son prácticamente imposibles de inferir, y son fundamentales para construir un criptosistema robusto. Esta es la principal motivación para proponer un esquema de ese tipo

En el estado del arte existen propuestas como las siguientes. En [5] se propone un criptosistema que usa puntos solución de Curvas Elípticas y un generador de números aleatorios para obtener las llaves de cifrado. Con matrices aleatorias se permutan los pixeles de cada plano RGB de la imagen, combinando el criptosistema AES de 128 bits para cifrar.

En [6] se presenta un esquema que usa el SHA-512 de la imagen a cifrar para obtener las llaves de cifrado. El cifrado se realiza en bloques de 128 bits, y combina el uso de Curvas Elípticas-El Gamal y un algoritmo genético basado en el ADN.

El criptosistema propuesto en [7] usa un generador de números pseudo aleatorios basado en Curvas Elípticas para obtener las llaves de cifrado. El cifrado se realiza permutando los pixeles de cada plano de la imagen a cifrar con un algoritmo que requiere de n puntos solución de la Curva Elíptica dependiendo de sus dimensiones (ancho x largo) y del uso de una Caja de Sustitución (S-Box) dinámica.

Las diferencias de esta propuesta con respecto a las anteriores son: a) Se propone un algoritmo para generar Curvas Elípticas que cumplen con ciertos requisitos para considerarlas resistentes a ataques como el del Logaritmo Discreto. Se infiere que probablemente en los artículos anteriores se utilicen Curvas Elípticas existentes que se consideran seguras. b) Se propone el uso de una prueba de bondad de ajuste (χ^2), para determinar la aleatoriedad del cifrado, y, c) El cifrado se realiza en un solo bloque determinado por las dimensiones de la imagen a cifrar (ancho x largo).

Una vez explicado lo anterior, el documento se divide en la siguiente forma. En la sección II se definen las Curva Elípticas, y su uso en la Criptografía, así como la familia de Curvas Elípticas que se emplean en esta investigación. En la sección III se describe el Criptosistema propuesto. En la sección IV se realizan experimentos y el criptosistema se pone a prueba. En la sección V se hace un análisis de los resultados obtenidos. En la sección VI se presentan las conclusiones.

II. Las Curvas Elípticas y la Criptografía

V. S. Miller [8], y N. Koblitz [9] propusieron el uso de Curvas Elípticas en la criptografía. Una Curva Elíptica es una forma geométrica proyectiva, cuya expresión general es definida en la ecuación de Weierstrass mostrada en (1).

$$y^2 \equiv x^3 + kx + l \bmod p \tag{1}$$

Una Curva Elíptica E es definida en un campo F_p, y genera un conjunto de soluciones $E(F_p)$ de dos variables (x, y); formando

Erick Armando Hernández-Díaz, Instituto Politécnico Nacional, Ciudad de México, México, erick_hd@live.com.mx.

Héctor Manuel Pérez-Meana, Instituto Politécnico Nacional, Ciudad de México, México, hmperezm@ipn.mx.

Victor Manuel Silva-García, Instituto Politécnico Nacional, Ciudad de México, México, vsilvag@ipn.mx.

Corresponding author: Héctor Manuel Pérez Meana.

un grupo abeliano, sobre el cual es posible definir la operación de adición (*E*, +) con sus respectivas propiedades.

Este proceso se describe a continuación.

Sean los puntos P, Q $\in E(F_p)$, a través de los cuales cruza una recta denominada como *L*. Si se proyecta la tangente, terminará intersecando a *E* en un punto el cual se denomina R'. Si este se refleja en el eje de las *X*, se obtendrá un nuevo punto llamado R, el cual es definido en la forma, $R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2)$ [10].

Para calcular las coordenadas de R, primero se realiza el cálculo de la pendiente λ de la recta. En este sentido, se presentan 3 posibles casos, (a) $x_1 \neq x_2$; (b) $x_1 = x_2, y_1 = -y_2$; (c) $x_1 = x_2, y_1 = y_2$.

Para el caso (a), se usan las ecuaciones (2), (3) y (4).

$$\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} \bmod p \tag{2}$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p \tag{3}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p \tag{4}$$

Para el caso (b), se define el elemento nulo ∞, tal que se cumplan dos condiciones: $P + (-Q) = \infty$, y, $P + \infty = P$.

Para el caso (c), se usan (4), (5), (6), donde.

$$\lambda = (3{x_1}^2 + a)(2y)^{-1} \bmod p \tag{5}$$

$$x_3 = (\lambda^2 - 2x_1) \bmod p \tag{6}$$

En este trabajo de investigación se usan Curvas Elípticas de la forma que se muestra en (7), donde $l = 0$.

$$y^2 \equiv x^3 - kx \bmod p \tag{7}$$

Para calcular los valores *p*, *k*, y el número de soluciones de la Curva Elíptica, se hace uso del siguiente teorema.

Teorema 1 [11]. Sea $p = a^2 + b^2$, dónde *p* es un número primo, *a* un entero impar positivo, y, *b* un entero par positivo. Además, sea $\#E(F_p)$ el número de soluciones de la Curva Elíptica escrita en (7). Así mismo, se cumpla con que $p \equiv 1 \bmod 4$, y, $a + b \equiv 1 \bmod 4$. El número de soluciones *es* $\#E(F_p) = p + 1 + 2a$. Además, *k* no puede ser potencia cuarta módulo *p* de ningún elemento del campo F_p, sin embargo, *k* tiene que ser potencia al cuadrado de algún elemento del campo F_p.

El punto desde el que se construye el sistema de soluciones se denomina generador y se representa con la letra griega *α*. El generador corresponde al primer elemento del subgrupo, el siguiente elemento será 2*α*, así sucesivamente hasta llegar a $(q-1)\alpha$; el cuál es el inverso aditivo de *α*, esto es, $(q-1)\alpha = (x_0, -y_0)$. En este trabajo de investigación se encuentran las coordenadas x_0, y_0 del generador realizando combinaciones con los números después del punto decimal de una cadena obtenida con la ecuación mostrada en (16). Por otro lado, el punto $q\alpha$ es el elemento nulo, el cual también es conocido como infinito ∞. Además, el subgrupo generado al ser abeliano es cíclico, lo que significa que, $\infty + \alpha = \alpha$.

Por otra parte, el número de soluciones y el orden de la Curva Elíptica tiene un factor primo denominado q, y se calcula con (8). Para asegurar que q es primo se le aplica la prueba de primalidad de Miller Rabin por lo menos 20 veces [12]; la tasa de error de esta prueba es de $(1/4)$, de este modo se disminuye a $(1/4)\text{^}20$, y se obtiene certeza de que q realmente es primo.

$$q = \frac{p+1+2a}{4} \tag{8}$$

Por último, se utiliza la ecuación (9) para calcular a *k*, si se cumplan los requisitos que se describieron anteriormente.

$$k \equiv (x_0^3 - y_0^2)(x_0)^{-1} \bmod p \tag{9}$$

El algoritmo completo para la búsqueda de las Curvas Elípticas empleadas para cifrar se muestra en Fig. 1. Además, las Curvas Elípticas deben cumplir con cuatro características:

i. Ser No Singular [13]. Es decir, una Curva Elíptica que cumple con la condición, $4(-k)^3 \bmod p \not\equiv 0$.

ii. No ser Supersingular [13]. Es decir, el número de soluciones deberá cumplir con $q \bmod p \not\equiv 1$, ya que este tipo de Curvas Elípticas evitan ataques, como el diseñado por Menezes Okamoto y Vanstone (MOV) [14].

iii. No ser de Traza Uno [13]. Es decir, $q \neq p$, porque las Curvas Elípticas de este tipo son débiles.

iv. Tener un conjunto solución *q* de por lo menos un tamaño de 2^{160} bits [13], para que sea imposible solucionar el problema del logaritmo discreto [4], el cual al resolverse permitiría conocer el valor *m* de un punto *Q* = *mP*, cuando se sabe quiénes son *Q* y *P*. El algoritmo Pohlig-Hellman fue diseñado para solucionar ese problema [15], sin embargo, debido a que el tiempo de procesamiento de los cálculos es exponencial, usando números de gran longitud, es prácticamente imposible resolverse con el uso de una computadora.

III. Desarrollo

A. Generación de las Llaves del Cronograma

El criptosistema propuesto requiere un cronograma de 15 llaves de cifrado. El emisor del mensaje debe elegir un valor r, que hace referencia a un punto solución de una Curva Elíptica de la forma mostrada en (7), y debe cumplir con $1 < r < p - 1$. A partir de r se crea un nuevo conjunto solución $r\alpha = Q_0 = (x_0, y_0)$, y de este modo,

$$\begin{aligned} Q_1 &= Q_0 + \alpha = (x_1, y_1) \\ Q_2 &= Q_1 + 2\alpha = (x_2, y_2) \\ &\ldots \\ Q_n &= Q_{n-1} + n\alpha = (x_n, y_n) \end{aligned} \tag{10}$$

Después, se concatena cada coordenada *x*, *y*, de cada Q_i para crear un arreglo de enteros denominado como *K*, que corresponde a la llave de cifrado base del cronograma y debe tener una longitud igual o mayor al tamaño de la imagen *I* a ser cifrada. Si la extensión de la cadena supera al de la imagen, se recorta el excedente para conseguir que coincida.

$$K = x_0 || y_0 || x_1 || y_1 || x_2 || y_2 || \ldots || x_n || y_n \tag{11}$$

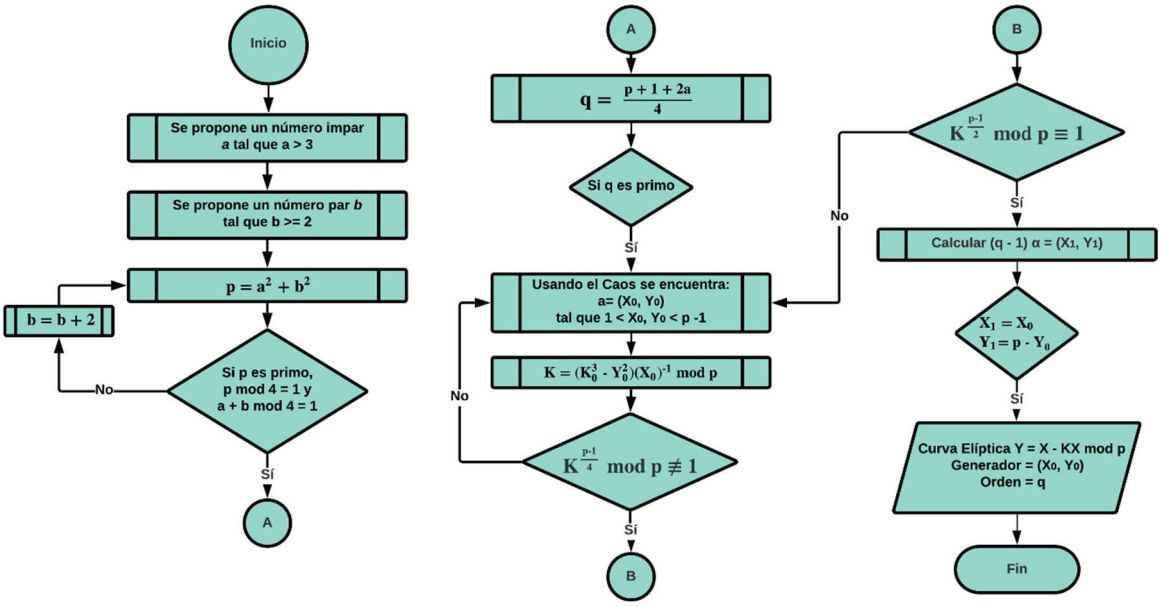

Fig. 1. Diagrama de flujo del algoritmo usado para calcular las curvas elípticas empleadas para desarrollar el algoritmo propuesto.

A partir de *K* se generan las llaves k_1 a k_{15}, y se usa una llave diferente por ronda para cifrar, a excepción de la ronda catorce en dónde se usan dos llaves de cifrado. En esta parte del proceso, es importante el uso de la caja S-Box de AES cuyo funcionamiento es descrito en el FIPS 197 [3], y ayuda a incrementar la aleatoriedad del cifrado por su alta no linealidad de 112, siendo 128 la máxima.

Se afirma que la S-Box de AES fortalece al criptosistema contra ataques lineales ya que hay investigaciones que afirman que en la actualidad solamente ha sido posible vulnerar 6 de un máximo de 14 rondas que puede tener AES tras ser sometido a ataques de criptoanálisis lineal [15-16].

Para obtener a k_1, los elementos de *K* son substituidos con la S-Box, después, la salida obtenida es desplazada en 5 bits a la derecha. Para obtener a k_2, se repite el proceso, pero empleando a k_1, así sucesivamente hasta llegar a k_{15}.

$$k_1 = \left(S_{BOX}(K)\right) \gg 5$$
$$k_2 = (S_{BOX}(k_1)) \gg 5$$
$$\dots$$
$$k_{15} = \left(S_{BOX}(k_{14})\right) \gg 5 \quad (12)$$

La motivación para generar las llaves de cifrado con este método es que se considera que las coordenadas de los puntos solución de una Curva Elíptica del orden de 2^{160} son numeros pseudoaleatorios y un atacante tendría dos problemas para encontrar el origen de éstos: saber qué Curva Elíptica ha sido usada y conocer el valor *r* que se eligió para construir a *K*.

B. Generación de las Permutaciones

Para este propósito se usa la ecuación diferencial de Robert May que destaca por su simplicidad y permite generar cadenas de números pseudoaleatorios con propiedades caóticas [17]. En (13) se muestra su expresión discreta.

$$\frac{dP}{dt} = eP - fP^2 \ (e, f > 0) \quad (13)$$

La ecuación se resuelve determinando tamaños de paso fijo $h > 0$ y tomando valores discretos en el tiempo para *P*, en la forma, $P(t_0)$, $P(t_1)$ … $P(t_n)$. Al aplicarse el algoritmo de Euler [16], se obtiene la ecuación (14)

$$P_{n+1} = P_n + (eP_n - fP_n^2) * h \quad (14)$$

La ecuación anterior se rescribe para obtenerse (15)

$$P_{n+1} = sP_n - tP_n^2 \quad (15)$$

donde $s = 1 + eh$, y, $t = fh$. Y finalmente se obtiene una ecuación iterativa que se muestra en (16).

$$x_{n+1} = sx_n(1 - x_n) \quad (16)$$

Los parámetros iniciales de esta ecuación son x_0 y s, dónde $0 < x_0 < 1$, y $0 < s < 4$. Después de 200 iteraciones se puede observar que los números de la cadena después del punto decimal empiezan a mostrar patrones de repetición, en ese caso el Caos no se produce. Si se observa que el límite de x tiende a infinito ($x_\infty = \lim_{n\to\infty} X_n$), se afirma que el Caos se ha producido. Se presentan ejemplos de ambos casos en la Tabla I.

TABLA I
EJEMPLOS DE CADENAS CALCULADAS CON EL CAOS

Iteraciones	X_0	*s*	Cadena *C*
200	0.035	2.7	0. 629629629629629…
200	0.035	3.8	0. 772084702356020…

Con la ecuación (16) se genera un arreglo de enteros denominado *C*, tomando en cuenta los valores después del punto decimal, y usando una función biyectiva para generar la permutación [18], que funciona bajo el algoritmo de la división Euclidiana [17], cuyo tamaño es determinado por la dimensión de la imagen a cifrar. Por 3 razones se utiliza esta ecuación diferencial para generar las permutaciones: 1) Cada valor x_n es determinístico, es decir, siempre se obtendrá lo mismo si se mantienen los parámetros iniciales. 2) Cualquier variante en los

valores de entrada, generarán una salida diferente. 3) Es imposible predecir cual será el arreglo *C* resultante, a menos que se conozcan los números x_0 y s.

C. Criptosistema Propuesto

El criptosistema propuesto consta de 14 rondas, usa 15 llaves de cifrado, y aplica sustituciones, permutaciones y operaciones XOR. Para describir al criptosistema se utilizan las siguientes variables: $R_{A,B}$, donde A es igual al número de ronda, y, B es igual al número de operación realizada; I_E es la imagen de entrada, I_c es la imagen cifrada e IC_N es la imagen cifrada tras la ronda *N*; *P* se refiere a la permutación, y, P^{-1} a la permutación inversa; S_{BOX} es la caja de sustitución de AES; por último, k_N hace referencia a la llave de cifrado número *N* del cronograma.

a) Ronda 1

Al inicio de la Ronda 1 se realiza una operación XOR bit a bit entre I_E, y, k_1, esto es: $R_{1,1} = I_E \oplus k_1$. Seguidamente se aplica la caja S-Box de AES a $R_{1,1}$, en la siguiente forma: $R_{1,2} = S_{Box}(R_{1,1})$ Después, $R_{1,2}$ se permuta usando *P* y se obtiene como salida de la primera ronda a $IC_1 = P(R_{1,2})$.

b) Rondas i, desde i = 2 a i = 13

Las Rondas 2 a 13 son idénticas. En cada una de ellas se llevan a cabo iterativamente las siguientes operaciones: Inicialmente se realiza una operación XOR bit a bit entre IC_{i-1} y k_i, esto es $R_{i,1} = IC_{i-1} \oplus k_i$. Seguidamente se aplica la caja S-Box de AES a $R_{i,1}$, y se obtiene como salida final tras i-ésima ronda a IC_i. Esto es, $IC_i = S_{BOX}(R_{i,1})$.

c) Ronda 14.

Finalmente, en la Ronda 14 se realiza una operación XOR bit a bit entre IC_{13} y k_{14}, esto es: $R_{14,1} = IC_{13} \oplus k_{14}$. Seguidamente se aplica la caja S-Box de AES a $R_{14,1}$, en la siguiente forma: $R_{14,2} = S_{Box}(R_{14,1})$. Después, $R_{14,2}$ se permuta usando P^{-1} y se obtiene $R_{14,3} = P^{-1}(R_{14,2})$. Para terminar, se realiza una operación XOR bit a bit entre $R_{14,3}$ y k_{15}, para obtener a I_C tras las 14 rondas, esto es, $I_C = R_{14,3} \oplus k_{15}$. Las rondas descritas se muestra en Fig. 2.

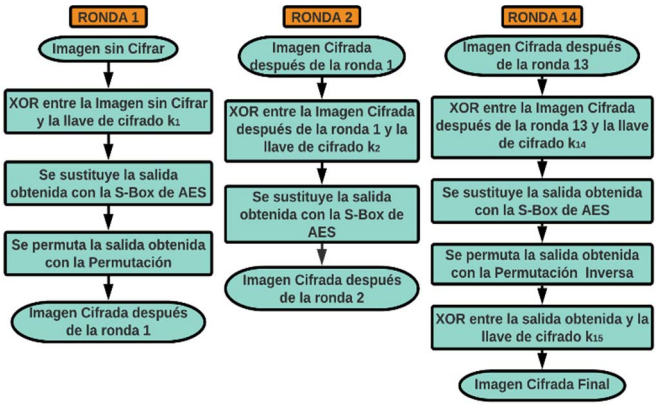

Fig. 2. Diagrama que describe las rondas 1, 2 y 14 del algoritmo de cifrado.

IV. Experimentos y Análisis de Seguridad

Para comprobar la resistencia del criptosistema ante ataques y la calidad de cifrado, es necesario realizar experimentos, los cuales deben ser pasados a través de distintas pruebas y realizar una interpretación de sus resultados.

A. Curva Elíptica para Generar la llave de Cifrado

Para llevar a cabo los experimentos, se utiliza la siguiente Curva Elíptica, en dónde:

a = 4bbb7efbc9d1baec18aac90fb
b = 56b28fc1333657fa084cde1fe
k = ee9bba45d3a0ca64ee28f639205c4b7bc50a6a8959afad226
p = 33c3dadc52e3b1f08d7ff0ea757d4946557e3dc73967afce1d
q = cf0f6b714b8ec7c235ffc3a9fbd2e4973ae1d492f1f423c05

Es muy importante considerar cuatro aspectos de esta Curva Elíptica. Primero, al realizar el cálculo de $4(-k)^3 \bmod p$, se obtiene como resultado:

1df50d44dc4b6d6676997a9040528bad6c5cd5cde2da5e4030

determinando que la Curva Elíptica cumple con $4(-k)^3 \bmod p \not\equiv 0$, y es No Singular.

Segundo, al calcular $q \bmod p$, se obtiene:

cf0f6b714b8ec7c235ffc3a9fbd2e4973ae1d492f1f423c05

determinando que la Curva Elíptica no es Supersingular, ya que, $q \bmod p \not\equiv 1$.

Tercero, es evidente que $p \neq q$, por lo cual se comprueba que no es de Traza Uno.

Finalmente, la expresión decimal del conjunto solución *q* es 812336343192204619397401200060595925747475271144695871723 57, cuyo tamaño es de 2^{196}.

Todo lo anterior comprueba que la Curva Elíptica a usar cumple con todos los requerimientos explicados en la sección II.

B. Imágenes Propuestas

Para las pruebas se usan cuatro imágenes RGB en formato BMP: Peppers y Lena de 512 x 512, Girl de 787 x 576 y Colors de 1920 x 1080. Estas imágenes y su resultado tras ser cifradas se muestran en Fig. 3, Fig. 4, Fig. 5 y Fig. 6.

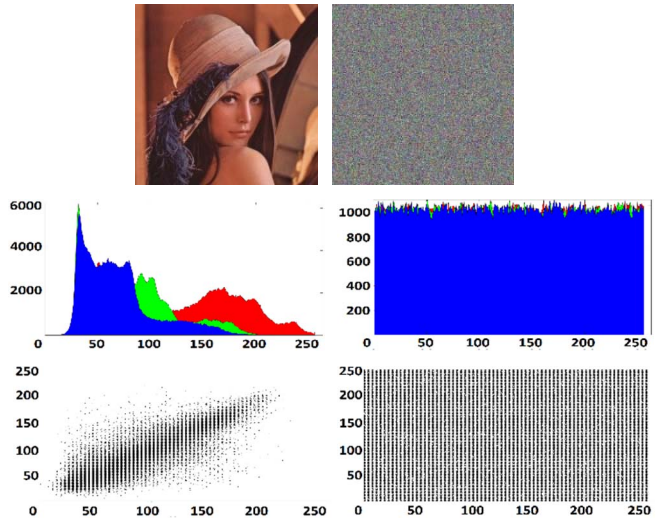

Fig. 3. Lena, histograma y diagrama de dispersión antes y después de cifrar.

C. Pruebas Estadísticas de Aleatoriedad

Este tipo de pruebas son importantes para comprobar la resistencia del criptosistema a ataques estadísticos.

(i) *Entropía.* Aportación del matemático francés Claude E. Shanon [19]. Analizando el histograma de la imagen cifrada se

determina que tan uniforme es su distribución frecuencias usando la expresión matemática que se muestra en (17).

$$H(x) = -\sum_{x \in X} P(x) log_2 P(x) \quad (17)$$

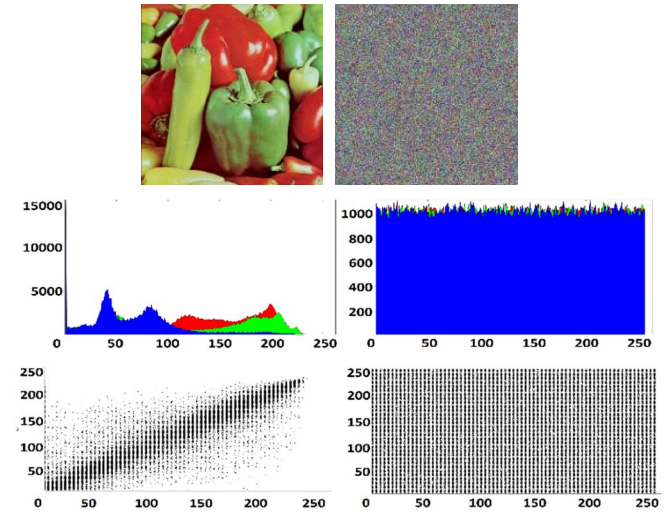

Fig. 4. Peppers, histograma y diagrama de dispersión antes y después de cifrar.

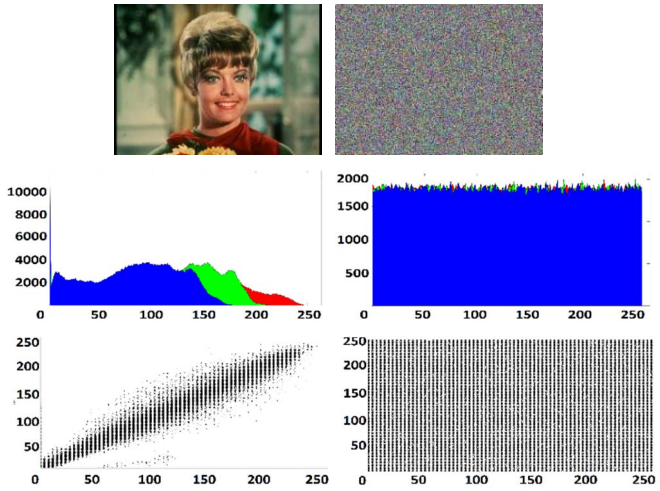

Fig. 5. Girl, histograma y diagrama de dispersión antes y después de cifrar.

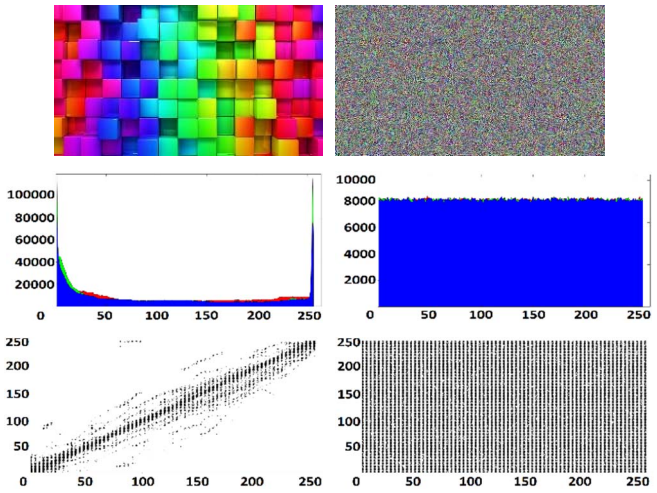

Fig. 6. Colors, histograma y diagrama de dispersión antes y después de cifrar.

La prueba se aplica en cada uno de los planos RGB de la imagen cifrada. Debido a que el valor máximo posible es 255, para poder expresarse se requiere un byte que como es sabido está formado por 8 bits, de este modo se espera que la distribución ideal sea un valor cercano a ocho [10]. Los resultados obtenidos de esta prueba se muestran en la tabla II, y, se comparan con las referencias [5, 6 y 7] en la tabla X.

TABLA II
ENTROPÍAS

Imagen	Rojo	Verde	Azul	Promedio	S-Box [28]
Lena	7.9993	7.9994	7.9993	7.99930611	7.99923238
Peppers	7.9995	7.9994	7.9994	7.99943079	7.99932173
Girl	7.9996	7.9996	7.9995	7.99959008	7.99960410
Colors	7.9999	7.9999	7.9999	7.99990655	7.99990863

(ii) *Coeficiente de Correlación* [20]. Esta prueba estadística cuantifica la relación que existe entre dos variables contiguas x, y, es decir, su objetivo es determinar si existe o no una dependencia entre una y otra, dicho de otro modo, comprobar si la cercanía posicional que comparten es aleatoria o no. Su expresión matemática se muestra en (18).

$$r = \frac{\sum[(x-\sum(x))(y-\sum(y))]}{\sqrt{\frac{i}{n}\sum_{i=1}^{n}(x_i-\sum(x))^2}\sqrt{\frac{i}{n}\sum_{i=1}^{n}(y_i-\sum(y))^2}} \quad (18)$$

donde x, y son pares de pixeles contiguos elegidos aleatoriamente. La prueba se realiza en tres direcciones. a) Horizontal, es decir, un píxel y el inmediato a la derecha. b) Vertical, es decir, un píxel y el inmediato inferior. c) Diagonal, es decir, un píxel y el inferior a la derecha. Si tras la prueba los valores obtenidos son cercanos a -1 y 1, se considera que la correlación lineal es alta. En consecuencia, un valor cercano a 0 indicará un nivel alto de aleatoriedad. Los valores absolutos obtenidos se muestran en las Tablas III, IV y V. y, se comparan con los resultados de las referencias [5, 6 y 24] en la tabla XI.

TABLA III
COEFICIENTES DE CORRELACIÓN HORIZONTALES

Imagen	Rojo	Verde	Azul	Promedio	S-Box [28]
Lena	0.0026	0.0027	0.0057	0.00372613	0.01322178
Peppers	0.0070	0.0056	0.0140	0.00889528	0.01048835
Girl	0.0033	0.0002	0.0015	0.00174115	0.01279921
Colors	0.0211	0.0078	0.0057	0.01159149	0.01495893

TABLA IV
COEFICIENTES DE CORRELACIÓN VERTICALES

Imagen	Rojo	Verde	Azul	Promedio	S-Box [28]
Lena	0.0000	0.0082	0.0110	0.00644598	0.01107951
Peppers	0.0239	0.0215	0.0160	0.02050918	0.00283142
Girl	0.0056	0.0159	0.0143	0.01201082	0.00856559
Colors	0.0050	0.0202	0.0158	0.01370130	0.01330631

(iii) *Prueba de distribución* χ^2 [21]. Plantea dos hipótesis, la nula H_0 y la alternativa H_a. La primera afirma que la imagen cifrada tiene una distribución aleatoria y la segunda lo niega. Se necesita un umbral que define una región de rechazo para definir cuál de las dos hipótesis es aceptada y se calcula con la ecuación

mostrada en (19). Dónde fo corresponde a las frecuencias de la imagen cifrada, y fe corresponde a la cantidad de frecuencias posibles, en este caso, 256.

$$\chi^2 = \sum_{i=1}^{n} \frac{(fo_i - fe)^2}{fe} \quad (19)$$

TABLA V
COEFICIENTES DE CORRELACIÓN DIAGONALES

Imagen	Rojo	Verde	Azul	Promedio	S-Box [28]
Lena	0.0036	0.0034	0.0185	0.00855536	0.00939815
Peppers	0.0279	0.0205	0.0125	0.02036789	0.00505178
Girl	0.0090	0.0049	0.0031	0.00571787	0.01919350
Colors	0.0139	0.0018	0.0197	0.01184446	0.00786417

En las pruebas basadas en hipótesis estadística se pueden cometer 2 errores: el error tipo I, es decir, rechazar a H_0 cuando es verdadera, y el error tipo II que es el caso opuesto. El error tipo I es el más importante y en este trabajo se usa con el valor $\alpha = 0.01$ [18]. En términos prácticos, un umbral menor o igual a 308 sirve para aceptar a H_0. Los resultados obtenidos de esta prueba se muestran en la Tabla VI.

TABLA VI
DISTRIBUCIONES CHI CUADRADA

Imagen	Rojo	Verde	Azul	Promedio	S-Box [28]
Lena	259.48	235.42	260.12	261.671804	279.781750
Peppers	230.36	257.71	279.98	256.017911	247.436445
Girl	250.17	255.39	267.67	257.743869	249.202422
Colors	264.97	294.22	246.88	268.691069	272.688292

D. Pruebas de la Llave de Cifrado

Para que las llaves de cifrado soporten ataques de fuerza bruta, su longitud no debe ser menor a 2^{100} [22].

(i) *Prueba de la sensibilidad de la llave.* Con esta prueba se demuestra su fortaleza ante ataques estadísticos. Si se cifra una imagen con una serie de llaves, y después, se cifra la misma imagen, pero con un pequeño cambio en cada una de éstas, ambas imágenes cifradas deben ser distintas y, debe ser imposible descifrar las imágenes con las llaves usadas en cada caso. Esta diferencia se puede medir con la ecuación mostrada en (20) [23]. Los resultados obtenidos de esta prueba se muestran en Fig. 7 y en la Tabla VII.

$$DiffImg = \frac{Pixeles\ Diferentes}{PixelesTotales}\ x\ 100 \quad (20)$$

TABLA VII
PRUEBA DE SENSIBILIDAD DE LLAVE

Imagen	Pixeles Diferentes	Diferencia Calculada (%)
Airplane	260997 de 262144	99.562454223632

E. Pruebas Diferenciales

Una prueba conocida para comprobar la resistencia de un criptosistema a este tipo de ataques es la siguiente: Primero, se cifra una imagen, después se cambia un píxel de la misma imagen y se vuelve a cifrar. Las imágenes cifradas al compararse deben ser completamente diferentes, para medir esta diferencia se hace uso de los estándares NPCR y UAC1 [24]. El primer estándar está determinado por la ecuación mostrada en (21) y el segundo por la ecuación mostrada en (22). En la práctica, en ambas pruebas se espera obtener valores promedio superiores a 99.4% para el NPCR y superiores a 33.3% para el UACI.

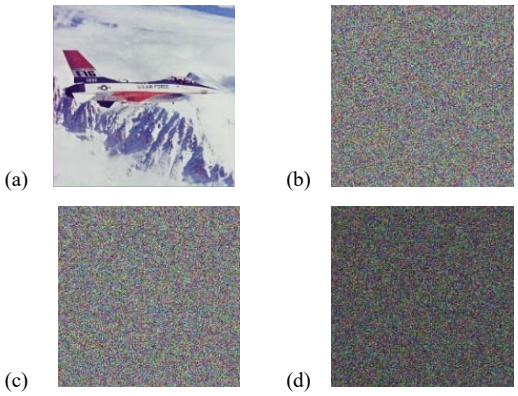

Fig. 7. (a) Airplane.bmp, (b) Imagen cifrada, (c) Imagen cifrada con una llave de cifrado modificada, (d) Diferencia entre imágenes cifradas.

$$NPCR: N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} x100\% \quad (21)$$

$$UACI: U(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{255 * T} x100\% \quad (22)$$

dónde C^1 y C^2 son las imágenes cifradas, T hace referencia al número total de pixeles y $D(i,j)$ es definido en (23).

$$D(i,j) = \begin{cases} 0, if\ C^1(i,j) = C^2(i,j) \\ 1, if\ C^1(i,j) \neq C^2(i,j) \end{cases} \quad (23)$$

Para esta prueba, el punto *r* de la Curva Elíptica que se elige para crear la *K* que generará las 15 llaves de cifrado de cada imagen corresponde a su respectivo SHA-1. Los resultados obtenidos se muestran en la Tabla VIII y se comparan con los resultados de las referencias [5, 6, 25, 26 y 27] en la tabla XII.

TABLA VIII
NPCR Y UACI

Imagen	NPCR (%)	UACI (%)
Lena	99.611253914388	33.459778330684
Peppers	99.610900878906	33.480101426068
Girl	99.607922725775	33.501321919186
Colors	99.572514789094	33.410932708988

F. Ataques de Texto Plano Conocido y Texto Plano Escogido

Si un criptosistema soporta los ataques de texto plano conocido y escogido, hará lo mismo con cualquier otro ataque del mismo tipo [5-6]. Los atacantes suelen usar imágenes blancas y negras para entender los patrones de cifrado de los criptosistemas. Por tanto, en esta prueba se cifran imágenes de ambos colores, y se miden sus entropías y coeficientes de correlación tras ser cifradas para comprobar que existe

suficiente confusión y difusión en ambas para evitar encontrar un patrón que pueda usarse para vulnerar el criptosistema con ambos ataques. Los resultados obtenidos se muestran en la Tabla IX y en Fig. 8.

TABLA IX
ATAQUES DE TEXTO PLANO CONOCIDO Y ESCOGIDO

Prueba	Imagen Blanca	Imagen Negra
Entropía Promedio	7.999335986914	7.999441145183
C. de C. Horizontal	0.011187436200	0.010201902029
C. de C. Vertical	0.011207796265	0.026154013426
C. de C. Diagonal	0.005429915826	0.022401709901

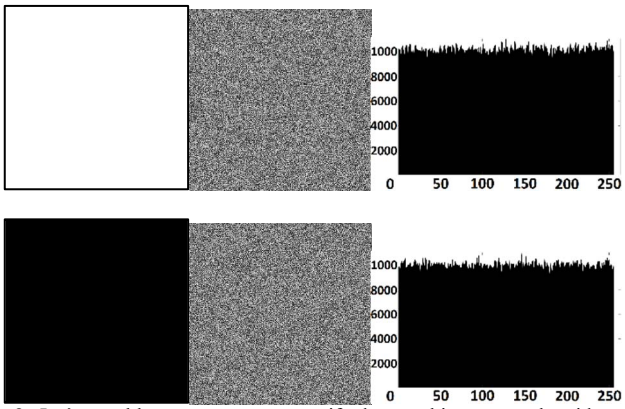

Fig. 8. Imágenes blanca y negra tras ser cifradas y su histograma obtenido.

G. Resultados Obtenidos

TABLA X
COMPARATIVA DE ENTROPÍAS CON EL ESQUEMA PROPUESTO Y OTROS SISTEMAS REPORTADOS

Imagen	C. Propuesto	Ref. [5]	Ref. [6]	Ref. [7]
Lena	7.9993	7.9998	7.9993	7.9993
Peppers	7.9994	7.9998	7.9994	7.9994

TABLA XI
COMPARATIVA DE LOS COEFICIENTES DE CORRELACIÓN CON EL ESQUEMA PROPUESTO Y OTROS SISTEMAS REPORTADOS

Esquema	Horizontal	Vertical	Diagonal
Propuesto	0.0037	0.0031	0.0056
Ref [5]	0.0045	0.0018	0.0001
Ref [6]	0.0019	0.0024	0.0011
Ref [24]	0.0031	0.0005	0.0041

TABLA XII
COMPARATIVA DE LOS PARÁMETROS NPCR Y UACI CON EL ESQUEMA PROPUESTOS Y OTROS PREVIAMENTE REPORTADOS

Esquema	NPCR (%)	UACI (%)
Propuesto	99.6112	33.4630
Ref. [5]	99.6000	33.4800
Ref. [6]	99.6113	33.4682
Ref. [25]	99.6235	33.6063
Ref. [26]	99.6100	33.4500
Ref. [27]	99.6078	33.4182

TABLA XIII
TIEMPOS DE CIFRADO DE LAS IMÁGENES USADAS EN LOS EXPERIMENTOS

Imagen	Dimensión	Tiempo de cifrado ms
Lena.bmp	512×512	0.140333
Airplane.bmp	512×512	0.146000
Girl.bmp	512×512	0.213333
Blanco.bmp	785×756	0.211333
Colors.bmp	1920×1080	0.843333

V. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Respecto a la Entropía, se explicó en el apartado IV que una distribución ideal de frecuencias es un valor igual a 8 y valores cercanos a este indican alta aleatoriedad. De acuerdo con la Tabla II, las imágenes obtuvieron entropías de al menos 7.999. Por lo cual, se considera que los resultados son buenos.

Respecto al Coeficiente de Correlación medido en tres direcciones, se explicó en el apartado IV que un valor de cero implica ausencia de correlación. De acuerdo con las Tablas III, IV y V, todos los resultados obtenidos se acercan a cero. Por lo cual, se considera que los resultados son buenos.

Respecto a la prueba de distribución Chi Cuadrada, se explicó en el apartado IV que un umbral con un valor igual o menor a 308 serviría para aceptar la H_0, la cual indica que existe un alto nivel de aleatoriedad. De acuerdo con la Tabla VI, el umbral más alto obtenido es de 294.2. Por lo cual, se considera que los resultados son buenos. Resultados similares se obtuvieron tanto en entropía, coeficiente de correlación y distribución Chi Cuadrada usando la S-Box propuesta en [28].

Respecto a la prueba de sensibilidad de la llave, se explicó en el apartado IV que al cifrar una misma imagen que una llave y otra levemente modificada, las imágenes cifradas obtenidas deben ser diferentes. De acuerdo con la Tabla VII, el porcentaje de diferencias de pixeles entre ambas fue de mayor al 99.5%. Por lo cual, se considera que los resultados son buenos.

Respecto a la prueba del NPCR y UACI, se explicó que al cifrar con una misma llave dos imágenes, modificando únicamente un píxel de una de ellas, los cifrados obtenidos deben ser diferentes. De acuerdo con la Tabla VIII, se obtuvieron resultados mínimos de 99.57 para el NPCR y de 33.41 para el UACI. Por lo cual, se considera que los resultados son buenos.

Respecto a los ataques de texto plano conocido y escogido, se explicó que, al cifrarse una imagen blanca y otra negra, y midiendo sus entropías y coeficientes de correlación, es posible validar que el criptosistema soporta ambos ataques y otros ataques similares. En este experimento se cifraron imágenes de 512 x 512, de acuerdo con la Tabla IX, las entropías obtenidas fueron cercanas a 8 y los coeficientes de correlación fueron cercanos a cero. Por lo cual, se considera que los resultados son acordes a los reportados en la literatura.

Por otro lado, en la tabla X, XI y XII, se comparan las entropías, coeficientes de correlación y valores NPCR y UACI obtenidos con los reportados en otros artículos científicos. Se observa que los resultados de las pruebas son muy similares con los de los otros artículos, de este modo se demuestra que esta propuesta equipara al actual estado del arte.

Como información adicional, en la Tabla XIII se muestran los tiempos de cifrado registrados en cada una de las imágenes de distintos tamaños usadas para los experimentos.

Finalmente, las pruebas a las que fue sometido comprueban que es robusto y resistente a ataques estadísticos y diferenciales, además de otros como el del logaritmo discreto y el MOV.

VI. Conclusiones

En este artículo se propuso un criptosistema simétrico cuyas llaves de cifrado son generadas usando Curvas Elípticas de constante cero. Además, se ha utilizado una ecuación caótica para generar una permutación y su inversa para aumentarla difusión y la calidad de cifrado. El uso de la S-Box de AES aporta confusión y aumenta la resistencia del criptosistema propuesto contra ataques lineales, debido a su alta no linealidad. Una diferencia de este esquema con respecto a otros es la aplicación del cifrado en un solo bloque, ya que, como es sabido, la mayoría de los criptosistemas simétricos dividen la información en bloques de longitud determinada. De acuerdo con los resultados obtenidos tras las pruebas diferenciales y estadísticas aplicadas a las imágenes cifradas, se afirma que la propuesta es robusta. En futuros trabajos, se espera generar cajas de sustitución dinámicas para probar su eficacia con esta propuesta y fortalecerlo contra posibles ataques algebraicos; así como la aplicación de otras pruebas como ataques de oclusión y de ruido. Finalmente, será deseable medir su eficacia en el cifrado de otros medios informáticos como audio o vídeo.

Agradecimientos

Los autores quieren agradecer al Instituto Politécnico Nacional (ESIME Culhuacan y CIDETEC) y al CONACyT por su apoyo económico para el desarrollo de este trabajo de investigación.

Referencias

[1] Nom-151, Norma Oficial Mexicana NOM-151-SCFI – Prácticas comerciales, Requisitos que deben observarse para la conservación de mensajes de datos, Diario Oficial de la Federación, México, 2002.

[2] H. Feistel, W. A. Notz, and J. L. Smith. “Some cryptographic techniques for machine-to-machine data communications,”. Proceedings of the IEEE, 63(11), 1975, pp. 1545–1554.

[3] FIPS PUB 197. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication. United States of America, 2001.

[4] R. Schoof, “The Discrete Logarithm Problem,” Open Problems In Mathematics, Springer, 2016, pp. 403-416.

[5] S. Toughi, M.H. Fathi, Y.A. Sekhavat. “An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System,” IEEE Access, China, 2018, pp. 1-17.

[6] Y. Luo, X. Ouyang, J. Liu. L. Cao “An image encryption method based on elliptic curve ElGamal encryption and chaotic systems,” Signal Processing, No. 141, 2017, pp. 217-227.

[7] U. Hayat, N.A. Azam. “A novel image encryption scheme based on an elliptic curve,” Signal Processing, No. 155, 2019, pp. 391-402.

[8] V.S. Miller. “Use of Elliptic Curves in Cryptography,” Advances in Cryptology - CRYPTO '85, LNCS 218, 1986, pp. 417-426.

[9] N. Koblitz. “Elliptic Curve Cryptosystems.” Math. Comput., 48, no. 177, 1987, pp. 203-209.

[10] Douglas R. Stinson, “Cryptography Theory and Practice,” 3rd ed, Chapman&Hall/CRC, 2006, pp. 54-56, 254-267.

[11] Kenneth H. Rosen, “Elliptic Curves. Number Theory and Cryptography,” 2nd ed, Chapman&Hall/CRC, 2008, pp. 47-58.

[12] H. C. A. van Tilborg, S. Jajodia“Encyclopedia of Cryptography and Security,”, 2nd Edition, Springer, 2011, p.p. 784.

[13] A. J. Menezes, T. Okamoto & S.A. Vanstone. “Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field,” IEEE Transactions on Information Theory, 39, no. 5, 1993, pp. 1639-1646.

[14] S.C. Pohlig, M.E. Hellman. “An Improved Algorithm for Computing Logarithms over GF(p)GF(p) and Its Cryptographic Significance,” IEEE Transactions on Information Theory, IT-24, no. 1, 1978, pp. 106-110.

[15] J. Liu, S. Chen, l. Zhao. “Lagrange Interpolation Attack against 6 Rounds of Rijndael-128,”. 5th International Conference on Intelligent Networking and Collaborative Systems, IEEE, 2013, p.p. 652-655.

[16] T. Tiessen, L.R. Knudsen, S. Kölbl, M. M. Lauridsen. “Security of the AES with a Secret S-Box,”. Fast Software Encryption, 22nd International Workshop, FSE 2015, p.p. 175-189.

[17] C. Henry Edwards, David E. Penney, ”Differential equations and and Boundary value problems,” 4ta ed., Pearson Prestice Hall, 2009, pp.112-116, 429–431.

[18] V.M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna Benoso, M. Aldape-Pérez, “Substitution Box Generation Using Chaos: An Image Encryption Application,” Applied Mathematics and Computation, Vol. 332, Elsevier, 2018, pp.123–135.

[19] E. Shannon, “A mathematical theory of communication,” Bell Syst, Tech J. 27, 1948, pp.379–423, 623-656.

[20] Ronald E. Walpole, Raymond H. Myers, Sharon L. Myers, Keying Ye, “Probability and statistics for Engineering and Sciences” 9th ed, Pearson Education, 2012, pp. 430–435.

[21] Robert G.D. Steel, James H. Torrie, “Biostatistical, Principles and Procedures”, 1st ed, Mc. Graw Hill, 1985, pp-56-57.

[22] G. Alvarez, S. Li. “Some basic cryptographic requirements for chaos-based cryptosystems,”. International Journal of Bifurcarion Chaos, Vol. 16, No. 8, 2006, p.p. 2129-2151.

[23] L. Li, A. A. Abd-El Latif, X. Niu. “Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images,”. Signal Processing, No. 92, 2012, pp. 1069-1078.

[24] Y. Wu, J. P. Noonan, S. Agaian. “NPCR and UACI Randomness Tests for Image Encryption,”. Journal of Selected Areas in Telecommunications, 2011, p.p. 1-8.

[25] A Patro, B Acharya, “An efficient color image encryption based on 1-D chaotic maps,” Journal of Information Security and Applications, Vol. 36, pp. 23-41, 2019.

[26] X. Wang, Q. Wang, “A novel image encryption algorithm based on dynamic S- Box constructed by chaos,” Nonlinear Dynamics, Vol. 75, No.3, pp. 567-576, 2014.

[27] M. García-Martinez, L. J. Ontañon-García, E. Campos-Canton , Celikovsky, “Hyperchaotic encryption based on multi-scroll piecewise linear systems,” Applied Mathematics and Computation, Vol. 270, pp. 413-424, 2015.

[28] J. Aboytes-González, J. Murguía, M. Mejia-Carlos, H. González-Aguilar, M. Ramírez-Torres, “Design of a strong S-box based on a matrix approach,” Non-linear Dynamics, Vol. 14, pp. 2003- 2012, 2018.

Erick Armando Hernández-Díaz. Nació en la Ciudad de México. Obtuvo el título de Ingeniero en Computación por la Universidad Nacional Autónoma de México (UNAM) en 2015, y el grado de Maestro en Ciencias de la Tecnología de Cómputo por el Instituto Politécnico Nacional (IPN) en 2016. Actualmente es alumno del doctorado en Comunicaciones y Electrónica en la Sección de Posgrado e Investigación del Instituto Politécnico Nacional. Sus áreas de investigación son criptografía aplicada y esteganografía.

Héctor Manuel Pérez-Meana. recibió el grado de M.S, por The University of electro-Communications, Tokio, Japón, y el grado de Doctor en Ingeniería Eléctrica por The Tokyo Institute of Techonology, Tokio, Tokio, Japón, en 1989. Es investigador miembro del Sistema Nacional de Investigadores, con el Nivel SNI III, también es miembro senior del IEEE, de la IEICE y de la Academia mexicana de ciencia. Actualmente es jefe de la Sección de Estudios de Posgrado e

Investigación de la Escuela de Ingeniería Mecánica y Eléctrica, Campus Culhuacan, del Instituto Politécnico Nacional (IPN) en México. Ha publicado más de 150 artículos en revistas indexadas y dos libros. También ha dirigido más de 20 tesis doctorales., miembro, The Mexican Researcher System y The Mexican Academy of Science. Sus principales áreas de investigación son sistemas adaptativos, procesamiento de imágenes, reconocimiento de patrones, marcas de agua y campos relacionados.

Víctor Manuel Silva-García. recibió el grado de Maestro en Estadística por la Universidad Autónoma de Chapingo en 1981, y el grado de Doctor en Ciencias de la Computación por el Instituto Politécnico Nacional (IPN), en 2007 con Mención Honorífica. Es investigador miembro del Sistema Nacional de Investigadores, con el Nivel SNI I. Actualmente es profesor en el Centro de Innovación y Desarrollo Tecnológico en Cómputo (CIDETEC) y en la Escuela Superior de Cómputo (ESCOM), ambas del Instituto Politécnico Nacional. (IPN) en México. Ha publicado más de 20 artículos en revistas indexadas y dos libros. También ha dirigido más de 20 tesis de maestría y 5 doctorales. Sus principales áreas de investigación son seguridad informática, criptografía aplicada y matemáticas aplicadas a la computación.