Revista Científica Nexo
Vol. 37, No. 02, pp. 38-60/Diciembre 2024

ISSN-E 1995-9516
Universidad Nacional de Ingeniería (UNI)
https://www.camjol.info/index.php/NEXO
http://dx.doi.org/10.5377/nsj.v37i2.19796

Algoritmo simétrico para el cifrado de imágenes formulado en el caos, curva elíptica, cajas dinámicas y permutaciones variables.

Symmetric algorithm for image encryption formulated in chaos, elliptic curve, dynamic boxes and variable permutations.

J.L. López-Maldonado[1,*], V.M. Silva-García[2], R. Flores-Carapia[2], M.D. González-Ramírez [2,*]

[1] Instituto Politécnico Nacional. ESIME-Zacatenco, Ciudad de México, México.
[2] Instituto Politécnico Nacional. CIDETEC. Ciudad de México, México.

(recibido/received: 13-06-2024; aceptado/accepted: 09-09-2024)

RESUMEN

Esta investigación propone un algoritmo de cifrado simétrico para imágenes sin pérdida ni compresión de datos del tipo BMP y TIF, a color y en escala de grises, llamado Cifrado de Imágenes con Caos y Curva Elíptica (CICCE). Está basado en el Caos y la Curva Elíptica, así como cajas de sustitución (S-Boxes) dinámicas; es decir, una S-box diferente para cada ronda. Además, se utilizó una función biyectiva para construir S-boxes dinámicas y permutaciones. CICCE es simétrico y consta de 15 rondas, considerando que en cada ronda se integra una caja de sustitución diferente (S-box 8×8), y estas cambian en cada proceso de cifrado. El caos se genera con las ecuaciones de E. Lorenz. Las imágenes de prueba experimentadas tienen dimensión de 512×512 píxeles. Se utilizaron diez instrumentos para evaluar la calidad del cifrado: entropía, correlación, transformada discreta de Fourier, NPCR, UACI, criterio de avalancha, contraste, energía, homogeneidad y una prueba de bondad de ajuste utilizando la distribución χ^2. A las imágenes cifradas también se les aplicaron cuatro tipos de ruido, con la intención de mostrar la resistencia del CICCE a este ataque. El ataque algebraico no se puede realizar porque las cajas son dinámicas; en comparación con AES, el ataque de fuerza bruta no es factible debido a la cantidad de claves (21024).

Palabras clave: Cifrado de imágenes, curva elíptica, caos, S-box dinámica, permutación variable.

ABSTRACT

This research proposes a symmetric encryption algorithm for images without loss or data compression of the BMP and TIF type in color and gray scale called Cifrado de Imágenes con Caos y Curva Elíptica (CICCE). It is based on Chaos and the Elliptic Curve, as well as dynamic substitution boxes (S-Boxes), that is, a different S-box for each round. Added a bijective function to construct dynamic S-boxes and permutations. CICCE is 15-round symmetric, considering that in each round a different substitution box (8×8 S-box) is integrated and these change in each encryption process. Chaos is generated with the equations of E. Lorenz. The examined test images are 512×512 pixels. Ten instruments were used to evaluate the quality of the encryption: entropy, correlation, discrete Fourier transform, NPCR, UACI, avalanche criterion, contrast, energy, homogeneity, and a goodness-of-fit test using the χ^2 distribution. Four

* Autor de correspondencia.
Correo: dgonzalezr@ipn.mx

types of noise were also applied to the encrypted images, with the intention of denouncing the CICCE's resistance to this attack. Algebraic attack cannot be performed because the boxes are dynamic; compared to AES, brute force attack is not feasible due to the number of keys (21024).
Keywords: Image encryption, elliptic curve, chaos, variable S-box, variable permutation.

1. INTRODUCCIÓN

El cifrado simétrico es una técnica utilizada para proteger imágenes que contienen información sensible y de alta jerarquía, tal como se muestra en las investigaciones de Ge et al. (2023), Ibrahim (2023) y Mfungo & Fu (2023). En el caso específico del Cifrado de Imágenes con Caos y Curva Elíptica (CICCE), las imágenes no se comprimen por dos razones principales. La primera es que, en todas las imágenes cifradas, se evalúa la calidad del cifrado utilizando al menos dos parámetros esenciales: la entropía y el coeficiente de correlación. En estudios donde se aplica compresión, como en el formato JPEG, estos parámetros no siempre se consideran (Song et al., 2022; Ali et al., 2023; Ran et al., 2022). En aquellos que sí lo hicieron, se observa que el valor de entropía se reduce, situándose aproximadamente en 7.8 (Li & Peng, 2023; Singh & Singh, 2022). La segunda razón para no comprimir las imágenes cifradas está relacionada con la importancia de la información almacenada, como en los ámbitos médico, financiero, militar, entre otros. En países como México, este tipo de imágenes está sujeto a regulaciones. El Archivo General de la Nación (AGN) requiere una compresión sin pérdida de información (AGN, 2022) y sustenta las características mencionadas.

De CICCE se destacan tres aspectos principales. El primer punto está relacionado con la resistencia del criptosistema propuesto frente a diversos ataques, los cuales se dividen en tres categorías:

A) Ataques relacionados con la curva elíptica. Dado que la curva elíptica es parte integral de la construcción de este criptosistema, algunos ataques pueden centrarse en la curva, lo que lleva al problema del logaritmo discreto (Filippone, 2023; Abdullah & Mahalanobis, 2023). Este ataque en la curva elíptica es comparable con la factorización de números enteros en el criptosistema Rivest-Shamir-Adleman (RSA). Resolver el problema del logaritmo discreto cuando el número de puntos de la curva tiene un factor primo de 2^{256} es equivalente a factorizar en RSA un número $n \approx 2^{3072}$ (Khan et al., 2023). Sin embargo, se pueden construir curvas elípticas cuyo número de soluciones tiene un factor primo mayor a 2^{512} (Shah, 2023), lo que haría que resolver el logaritmo discreto es equivalente a factorizar $n \approx 2^{15000}$ en RSA (Shatnawi et al., 2023), superando ampliamente lo que está disponible en el mercado actual (Azouaoui et al., 2022). Además, los ataques de fuerza bruta resultan más difíciles cuando el número de claves es mayor a 2^{512}, lo que hace que este ataque sea más complejo que contra el AES-256 (Goel et al., 2024).
B) Ataques al criptosistema simétrico propuesto. Debido a que las S-boxes son desconocidas en cada proceso de cifrado, no es posible realizar el ataque lineal, al menos no en la forma que se conoce actualmente (Jahangir et al., 2023; Liu et al., 2022). Las S-boxes dinámicas (8 × 8) impiden también los ataques algebraicos (Zhou et al., 2023). Además, el cronograma de llaves se construye usando caos y puntos de la curva elíptica, junto con un algoritmo para generar permutaciones que define una función uno a uno, es decir, una función biyectiva (Silva et al., 2023). Este último trabajo se basa en el procesamiento imágenes más grandes y requiere mayor capacidad computacional. Las imágenes cifradas con este criptosistema son resistentes al ataque diferencial (Zhang et al., 2023; Ma & Wang, 2023), ya que los parámetros Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) y Avalanche Criteria (AC) muestran valores aceptables (Sakthi & Revathi, 2024; Abdallah & Farhan, 2022; Mohamed, 2022).
C) Ataques a imágenes cifradas. Las imágenes cifradas están expuestas a cuatro tipos de ruido: oclusión, aditivo, multiplicativo y gaussiano (Wang, Peng, & Du, 2022). Para evaluar el daño al

descifrar una imagen cifrada con ruido, se propone un parámetro denominado parámetro de similitud (SP_c, donde el subíndice c indica el color).

El segundo aspecto clave es que el CICCE se basa en la Red de Sustitución-Permutación (Substitution-Permutation Network - SPN) (Arif et al., 2022), con una permutación aleatoria del tamaño de la imagen al inicio del cifrado, lo que aumenta la complejidad de los ataques al criptosistema (Abdallah & Farhan, 2022). Uno de los propósitos de este trabajo, es fundamentado por medio de la complejidad, la incertidumbre y la aleatoriedad., por ello CICCE cuenta con herramientas como el caos, la curva elíptica, permutaciones, SPN, operaciones x-or y S-Boxes dinámicas.

2. CONSIDERACIONES GENERALES

2.1. Ecuaciones de E. Lorenz para la construcción de CICCE.
E. Lorenz formuló un conjunto de ecuaciones diferenciales que son base para generar el caos, determinado en las Ecs. (1,2,3) (Moon et al., 2021).

$$\frac{dx}{dt} = \sigma(-x + y) \tag{1}$$

$$\frac{dy}{dt} = rx - y - xy \tag{2}$$

$$\frac{dz}{dt} = -bx + xy \tag{3}$$

Los parámetros $\sigma, r\ y\ b$ son positivos reales; además, los puntos críticos de las ecuaciones de Lorenz se obtienen poniendo a cero la Ec. (1), Ec. (2) y la Ec. (3). A partir de aquí, los puntos críticos se presentan en la Ec. (4):

$$P_1 = (0, 0, 0)$$

$$P_2 = \left(\sqrt{b(r-1)}, \sqrt{b(r-1)}, r-1\right) \tag{4}$$

$$P_3 = \left(-\sqrt{b(r-1)}, -\sqrt{b(r-1)}, r-1\right)$$

Considerando que las ecuaciones de Lorenz describen el fenómeno de convección en la atmósfera terrestre, son razonables los valores expresados a continuación: $\sigma = 10\ y\ b = 8/3$. Además, la solución de las ecuaciones de Lorenz tiene la forma presentada en la Ec. (5):

$$\vec{X} = \vec{\xi} e^{\lambda t} \tag{5}$$

$\vec{\xi}$ representa el eigenvector y λ los eigenvalores. Para calcular las soluciones en las proximidades del punto P_2, se utiliza la ecuación Ec. (6) se utiliza.

$$X' = AX \tag{6}$$

Donde las matrices A, X y X' se muestran en las Ecs. (7, 8, 9).

$$A = \begin{pmatrix} 10 & 10 & 0 \\ r & -1 & -\sqrt{\frac{8}{3}(r-1)} \\ \sqrt{\frac{8}{3}(r-1)} & \sqrt{\frac{8}{3}(r-1)} & -\frac{8}{3} \end{pmatrix} \quad (7)$$

$$X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad (8)$$

$$X' = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \quad (9)$$

Los eigenvalores se calculan a partir del polinomio característico, que se observa en la Ec. (10).

$$|A - \lambda I| = 0 \quad (10)$$

Considerando el parámetro $r = 28$, el polinomio característico se expresa en la Ec. (11).

$$3\lambda^3 + 41\lambda^2 - 50\lambda + 2160 = 0 \quad (11)$$

De la ecuación anterior, se consigue una raíz real y dos complejas; esto se muestra en las Ecs. (12, 13, 14).

$$\lambda_1 = -22.558424 \quad (12)$$

$$\lambda_2 = 4.445878 + 3.485904i \quad (13)$$

$$\lambda_3 = 4.445878 - 3.485904i \quad (14)$$

Con relación a los eigenvectores, es necesario generar dos para obtener la solución general. Las Ecs. (15,16) se visualizan los eigenvectores $\overrightarrow{\xi_1}$ y $\overrightarrow{\xi_2}$.

$$\overrightarrow{\xi_1} = \begin{pmatrix} 9.163288 \\ -11.507650 \\ 1 \end{pmatrix} \quad (15)$$

$$\overrightarrow{\xi_2} = \begin{pmatrix} 0.359510 + 0.116796i \\ 0.478680 + 0.294040i \\ 1 + 0i \end{pmatrix} \quad (16)$$

La solución de $\overrightarrow{\xi_2} e^{(4.445878+3.485904i)t}$ tiene una parte real y una parte compleja. La parte real es $\vec{u}$ y la parte compleja $\vec{v}$; además, si se denota $\vec{w} = \overrightarrow{\xi_1} e^{-22.558424t}$, entonces, el resultado se obtiene por la Ec. (18).

$$\varphi_x(t_0) = (0.172089)C_2 e + (0.336590)C_3 e \quad (18)$$

2.2. La Curva Elíptica para CICCE.

Este algoritmo de cifrado se basa en dos puntos de la curva elíptica y el caos. En este sentido, se realiza una descripción de los elementos utilizados en el desarrollo de una curva elíptica mostrado en la Ec. (19):

$$y^2 \equiv x^3 + ax + b \quad mod\ p \tag{19}$$

En este caso se aplica una curva con: $b = 0\ y\ a = -k$. Lo anterior se expresa en la Ec. (20).

$$y^2 \equiv x^3 - kx \quad mod\ p \tag{20}$$

Las condiciones que debe cumplir la curva para evitar criptoanálisis conocidos como attack MOV o construct trace one curves (Hernández *et al.*, 2021), que son considerados una debilidad, se muestran en las Ecs. (21,22).

$$\#E(F_q) \not\equiv 1 \quad mod\ p \tag{21}$$

$$\#E(F_q) \neq p \tag{22}$$

Donde $\#E(F_q)$ es el número primo de soluciones de la curva. Para garantizar que la curva tenga tres raíces reales diferentes es necesario que sea no singular, lo anterior se expresa en la Ec. (23).

$$4((-k)^3) \not\equiv 0 \quad mod\ p \tag{23}$$

La operación suma (+) se define sobre el conjunto de puntos solución de la curva, de modo que este conjunto (E, +) es un grupo abeliano (Washington, 2008). Se aplica el *Teorema 1* para calcular el número de soluciones:

Teorema 1. Sea p un número primo impar, $k \not\equiv 0\ mod\ p$, y $\#E(F_p)$ el número de soluciones para la curva elíptica definida por la Ec. (20), Además, $p \equiv 1\ mod\ 4$ donde p puede ser escrito en la Ec. (24).

$$p = a^2 + b^2 \tag{24}$$

Tal que a, b son enteros positivos, b es un número par y $a + b \equiv 1\ mod\ 4$. El número de soluciones está dado por la Ec. (25) cuando k no es la cuarta potencia de $mod\ p$ de alguno elemento en el campo F_p , pero una potencia cuadrada de $mod\ p$.

$$\#E(F_p) = p + 1 + 2a \tag{25}$$

El número de soluciones $\#E(F_p)$ debe ser un factor primo lo suficientemente grande como para que el ataque de logaritmos discretos no pueda llevarse a cabo, al menos con la tecnología disponible actualmente (Hla & Aung, 2019). Por otro lado k, debe cumplir la condición de no ser una cuarta potencia de $mod\ p$ de algún elemento de F_p. En este sentido, dicha condición es la siguiente: $k^{\frac{p-1}{4}}\ mod\ p \not\equiv 1$. El criterio de Euler se utiliza para determinar si k es una potencia cuadrada $mod\ p$ de algún elemento en el campo F_p (Gallian, 2021). Para obtener el número primo de soluciones, si existe, se calcula según la Ec. (26). De hecho, el número de soluciones siempre es divisible entre 4 (Silva et al., 2020).

$$q = \frac{p + 1 + 2a}{4} \qquad (26)$$

Teorema 2. Sea E una curva elíptica definida en Z_p, donde p es un número primo > 3. Entonces existen dos enteros positivos n_1, n_2 tales que hay un isomorfismo de $(E, +)$ a $Z_{n_1}\, x\, Z_{n_2}$. Además, $n_2 \mid n_2 \mid (p-1)$. (Stinson, D. R., & Paterson, M. (2018)).

Para este caso $n_2 = 1$ y $n_1 = q$, que es un factor primo de $\#E(F_p)$ y, q se define en la Ec. (26). A veces q no es primo, si es el caso, hay que buscar otro número primo p que cumpla con las condiciones del *Teorema 1*, tal que el número q sea primo. Para encontrar la primera solución y la ecuación de la curva elíptica se aplica la Ec. (27); donde sólo es necesario conocer un punto inicial (x, y).

$$k \equiv (x^3 - y^2)(x^{-1}) \mod p \qquad (27)$$

Existen investigaciones donde la curva elíptica y el elemento generador α, se calculan según los conceptos mencionados (Silva et al., 2020). Para reducir tiempos en el cálculo del inverso multiplicativo $mod\ p$ en la suma de puntos, se propone el siguiente teorema para obtenerlo.

Teorema 3. Dado un número primo p y un elemento $x \in Z_p$, tal que $x \neq 0$, entonces el inverso multiplicativo $x\ mod\ p$, se obtiene como $x^{-1} = x^{p-2} \mod p$.

Prueba 1. Como p es un número primo y $x \neq 0, \in Z_p$, se deduce que $\gcd(x, p) = 1$, por lo tanto, la inversa de x existe y es única (Stinson & Paterson, 2018).

Entonces $x \times x^{p-2}\ mod\ p = x^{p-1}p$. Sin embargo $x^{p-1}\ mod\ p \equiv 1$ según Lagrange y considerando que la ϕ de Euler satisface $\phi(p) = p^{-1}$ (Gallian, 2021). Por lo tanto, x^{p-2} es el inverso multiplicativo de x. A continuación, se muestra un ejemplo: Dado $a = 4139$ y $b = 314$, se deduce que p es 17229917. Se puede verificar que $p\ mod\ 4 \equiv 1$, y $a + b \equiv 1\ mod\ 4$. Un punto de solución $\alpha = (11199810, 4614456)$ se selecciona y k se calcula de acuerdo con la Ec. (27) dando como resultado $k = 4167325$. Entonces, k se verifica usando las Ecs. (28) y (29).

$$(4167325)^{17229917-\frac{1}{4}} \mod 17229917 \not\equiv 1 \qquad (28)$$

$$(4167325)^{17229917-\frac{1}{2}} \mod 38873 \not\equiv 1 \qquad (29)$$

La curva resultante se describe en la Ec. (30):

$$y^2 \equiv x^3 - 4167325x \mod 17229917 \qquad (30)$$

Así, según el *Teorema 1* el número de soluciones es $\#E(F_{17229917}) = 17238196$, y el primo $q = \frac{17238196}{4} = 4309549$. Además, $4309549\ mod\ 17229917 \not\equiv 1, 4(-4167325)^3\ mod\ 17229917 \not\equiv 0$, y

$E(F_{4309549}) \neq 17229917$. De estas condiciones, se determina que la curva es no-singular, no supersingular y tampoco de traza uno.

El siguiente paso es verificar si $\alpha = (11199810, 4614456)$ es un elemento primitivo, entonces se debe cumplir que $(q-1)\alpha = (11199810, -4614456)$. Posteriormente, se calculan los valores: $2\alpha = (4995846, 1046698); 4\alpha = (12063429, 15977680); \ldots; 4194304\alpha = (2413044, 15455227)$.
Los puntos resultantes son:

$4259840\alpha = (15791514, 845101);\ 4292608\alpha = (16173401, 14902172); \ldots;\ 4309548\alpha = (11199810, 12615461)$. Se debe tener en cuenta que $12615461 \equiv -4614456 \bmod 17229917$, por lo que se deduce $4309548\alpha + \alpha = \infty$.

2.3. Entropía de la información.

La entropía es un parámetro que mide la calidad de una imagen cifrada, es decir, la distribución de los niveles debe ser aleatorios. Esta medición se calcula según la Ec. (31) (Shannon, 1948):

$$H(x) = -\sum_{x \in X} P(x) \log_2 P(x) \qquad (31)$$

Las imágenes pueden tener 256 niveles de gris, definidos en un byte. En cambio, si la imagen es en color, se utilizan tres bytes para los colores rojo, verde y azul. En este sentido, una imagen está bien codificada si el histograma de los distintos niveles de cada color asemeja una distribución uniforme. En este orden de ideas, si la distribución de niveles de color es exactamente una distribución uniforme, entonces la entropía es 8. Cabe aclarar que, si un histograma tiene entropía 8, la distribución de color no es necesariamente aleatoria, ya que es posible construir una distribución teórica con entropía 8 que no sea aleatoria. Sin embargo, la aleatoriedad de la distribución del color se mide con varios instrumentos para garantizar que se cumpla esta propiedad. En la práctica, se considera que una entropía cercana a 8 indica un buen grado de aleatoriedad (Yu et al., 2021).

2.4. Coeficiente de Correlación.

Este análisis se realiza de la siguiente manera: se eligen aleatoriamente n píxeles de la imagen cifrada y se calcula la correlación tomando los píxeles adyacentes de cada uno de ellos. Es decir, en las direcciones horizontal, vertical y diagonal. La medición de este parámetro se realiza en gran parte del trabajo de cifrado de imágenes (Zeng & Wang, 2021; Shafique et al., 2020). Si este análisis se realiza en dirección horizontal y para el color rojo: se elige de forma aleatoria un punto rojo de la imagen cifrada, denotado como z_r. Posteriormente se elige el punto rojo adyacente a él en dirección horizontal, y de la misma forma que antes, este punto tiene tres colores básicos, incluido el rojo denotado como w_r. Luego, es posible calcular la correlación entre las variables z_r y w_r, cuando tienen n pares de puntos. Para las demás direcciones y colores el cálculo es similar. La fórmula para calcular la correlación en la dirección horizontal y el color rojo se presenta en la Ec. (32), y las expresiones $\bar{z}_r, \bar{w}_r$se muestran en las Ecs. (33) y (34).

$$r_{h;z_r,w_r} = \frac{\frac{1}{n}\left(\sum_{i=1}^{n}\left(z_{i,r} - \bar{z}_r\right)\left(w_{i,r} - \bar{w}_r\right)\right)}{\sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}\left(z_{i,r} - \bar{z}_r\right)^2\left(\frac{1}{n}\sum_{i=1}^{n}\left(w_{i,r} - \bar{w}_r\right)^2\right)\right)}} \qquad (32)$$

$$\bar{z}_r = \frac{1}{n}\sum_{i=1}^{n} z_{i,r} \quad (33)$$

$$\bar{w}_r = \frac{1}{n}\sum_{i=1}^{n} w_{i,r} \quad (34)$$

2.5. Transformada Discreta de Fourier (DTF).

La Transformada Discreta de Fourier (DFT) es una prueba incluida en el estándar NIST 800-22, para medir el grado de aleatoriedad de una cadena binaria, es decir, que no existen patrones repetitivos de ceros y unos, uno tras otro (Bassham III *et al.*, 2010). Los parámetros involucrados en el cálculo son: N_0, una cantidad teórica esperada dada por $(0.95) \times \frac{n}{2}$, donde n es la longitud de la cuerda; y N_1, el número de valores inferiores al umbral h, calculado a partir de la Ec. (35).

$$h = \sqrt{Ln\frac{1}{0.05}(n)} \quad (35)$$

Entonces, f_j se obtiene usando la Ec. (36), con $i = \sqrt{-1}, j = 1, 2 \ldots \frac{n}{2} - 1$ y $x_k = 2\delta_k - 1$donde δ_k es el k-ésimo bit de la cadena,

$$f_j = \sum_{k=1}^{n} x_k e^{\frac{2\pi(i)(k-1)j}{n}} \quad (36)$$

Si n es impar, se elimina el último bit de la cadena; sin embargo, en este caso n siempre es par; por otro lado, f_j es un número complejo. El módulo $\|f_j\|$ se calcula y se compara con h. Si $\|f_j\| < h$, entonces se suma 1 a N_1. De lo contrario, N_1sigue siendo el mismo. Ec. (37) se evalúa para obtener d y luego se calcula la Ec. (38), donde *erfc* está determinada por la Ec. (39). La regla de decisión es: si el valor $P - value < 0.01$, entonces se rechaza la hipótesis de que la cadena es aleatoria y, en caso contrario, se acepta.

$$d = \frac{N_1 - N_0}{\sqrt{\frac{n(0.95)(0.05)}{4}}} \quad (37)$$

$$P - value = erfc\frac{|d|}{\sqrt{2}} \quad (38)$$

$$erfc\frac{|d|}{\sqrt{2}} = 2\big(1 - \Phi(|d|)\big) \quad (39)$$

2.6. Parámetros para medir la fortaleza de CICCE contra un ataque diferencial.

Los parámetros NPCR, UACI, y AC se utilizan para evaluar la resistencia del sistema propuesto contra el ataque diferencial. NPCR se define en la Ec. (40), donde el subíndice c indica el color, y la función $D(i,j)_c$ toma un valor 1 cuando los bytes en la posición (i,j) de las imágenes cifradas 1 y 2 son diferentes; de lo

contrario, es 0. Se señala que la imagen 1 y la imagen 2 son diferentes por solo un byte. Por otro lado, las variables W y H son el ancho y alto de la imagen, respectivamente. Un porcentaje adecuado de este parámetro para evitar el ataque diferencial se encuentra en el rango cercano al 99,6% (Ravichandran et al., 2021; Kamal et al., 2021).

$$\mathrm{NPCR_c} = \frac{\sum_{\mathrm{i,j}} \mathrm{D(i,j)_c}}{\mathrm{W} \times \mathrm{H}} \times 100\% \qquad (40)$$

UACI se define en la Ec. (41). El byte $C_{1,c}(i,j)$se define de la siguiente manera: tiene una posición $(\mathrm{i,j})$ y el color c en la primera imagen. De manera similar, el byte $\mathrm{C_{2,c}(i,j)}$ tiene una posición $(\mathrm{i,j})$ y un color c en la segunda imagen. Un buen porcentaje de UACI para soportar el ataque diferencial se acerca al 33,4% (Zhang et al. 2021).

$$\mathrm{UACI_c} = \frac{1}{\mathrm{W} \times \mathrm{H}} \left[\sum_{\mathrm{i,j}} \frac{\left| \mathrm{C_{1,c}} - \mathrm{C_{2,c}} \right|}{255} \right] \times 100\% \qquad (41)$$

El cálculo de AC para un color particular se realiza según la Ec. (42), donde T es el número total de bits en la imagen cifrada, y la función $b(i,j)_c$ está definida por la Ec. (43). Es decir, si un bit en la imagen 1 para el color c es igual al bit correspondiente en la imagen 2 para el mismo color, entonces $b(i,j)_c = 0$. De lo contrario, $b(i,j)_c = 1$. Un valor apropiado de AC para prevenir el ataque diferencial es cercano al 50% (Altigani et al., 2021).

$$AC_c = \frac{\sum_{i,j} b(i,j)_c}{T} \times 100\% \qquad (42)$$

$$b(i,j)_c = \begin{cases} 0 \\ 1 \end{cases} \qquad (43)$$

2.7. Parámetros de energía, contraste y homogeneidad.

La medición de la energía revela el grado de orden o desorden que tiene la información en una imagen. Es decir, cuando la energía en una imagen cifrada es cercana a cero, significa que el grado de desorden es alto, lo que demuestra que la imagen cifrada es de alta calidad. La energía se calcula según la Ec. (44), donde i,j es la posición del píxel y $g(i,j)$ es el valor en ese punto.

$$E = \sum_{i,j} g(i,j)^2 \qquad (44)$$

El contraste, mide las diferencias de intensidad entre un píxel y los píxeles vecinos. El contraste se define en la Ec. (45). Donde, $g(i,j)$ es el valor de píxel en la posición (i,j). Si una imagen está bien cifrada si los valores de contraste son altos, es decir, cuanto mayor sean los valores de contraste, mayor seguridad mostrará el algoritmo de cifrado propuesto.

$$Contrast = \sum_{i,j} |i-j|^2 g(i,j) \qquad (45)$$

En cuanto a la homogeneidad, cuantos menores sean los valores de homogeneidad, mayor será la calidad del cifrado. Esto se calcula según la Ec (46).

$$H = \sum_{i,j} \frac{g(i,j)}{1 + |i - j|} \qquad (46)$$

2.8. Prueba de ajuste de bondad.

Esta herramienta tiene como objetivo averiguar si las distribuciones de los colores primarios se ajustan a una distribución uniforme (El-Latif et al., 2021). Si es así, se dice que la distribución de los colores es aleatoria. Sin embargo, el enfoque anterior conduce a una prueba de hipótesis estadística. Esta prueba requiere dos ingredientes, a saber: una estadística de prueba y una región de rechazo. En este trabajo, se utiliza la estadística χ^2 para cada color primario. La distribución de la variable χ^2 es la Chi-cuadrado con $k - 1$ grados de libertad y se expresa en la Ec. (47), donde o_i y exp son los valores observados y esperados, respectivamente.

$$\chi^2 = \sum_{i=1}^{k} \frac{(o_i - exp)^2}{exp} \qquad (47)$$

Según el teorema del límite central, el estadístico χ^2 se aproxima a la distribución normal con media $\mu = 255$ y desviación estándar σ, como se muestra en la Ec. (48) (Zhang, 2021). Teniendo esto en cuenta, el umbral se puede calcular usando el lado derecho de la distribución normal con un nivel de significancia de $\alpha = 0.01$, que es aproximadamente 308. Por lo tanto, la regla de decisión es: si $\chi^2 > 308$ la hipótesis de que la cadena es aleatorio se rechaza y en caso contrario se acepta.

$$\sigma = (2 \times 255)^{0.5} = 22.58 \qquad (48)$$

3. MÉTODOS Y MATERIALES

3.1. Presentación de algoritmos.

Algoritmo 1: Procedimiento de cifrado.

El presente algoritmo se ilustra en la Figura 1 y se explica de la siguiente manera:

1. Inicialmente, la imagen se descompone en texto claro según los colores RGB, para consecutivamente aplicar una permutación P (ver Algoritmo 2). A continuación, se aplica la operación x-or, la cual se realiza con la imagen permutada y la primera clave de programación (ver Algoritmo 3). Posteriormente, la cadena resultante se divide en bloques de un byte, y se lleva a cabo la operación de sustitución con la primera caja (ver Algoritmo 4); cabe destacar que la sustitución se realiza de la misma forma que en AES (Lin et al., 2021).
2. De la ronda 2 a la 14, el procedimiento es el siguiente: primero, se aplica la operación x-or entre la salida de la ronda anterior y la llave del cronograma correspondiente. A continuación, se realiza la sustitución con la S-box que le corresponde.
3. En la última ronda, primero se realiza la operación x-or con la salida de la ronda 14. Luego, se aplica la operación de sustitución con la última caja. Posteriormente, a la cadena de salida de sustitución se le aplica la operación x-or con la llave del cronograma 16. El resultado es la imagen cifrada.

Algoritmo 2: Procedimiento para la generación de permutaciones.

Dado el conjunto $Z_m = \{n \in N \mid 0 \leq n \leq m! - 1\}$ cualquier elemento de Z_m puede ser expresado en una base factorial como sigue:

$$n = D_0(m-1)! + D_1(m-2)! + \cdots\ D_{m-2}(1)! + D_{m-1}(0)! \qquad (49)$$

Según el algoritmo de división euclidiana, las constantes D_i en la Ec. (49) son únicas (Eder et al., 2021), además de que la constante $D_{m-1} = 0$. Las constantes deben cumplir con la propiedad mostrada en la Ec. (50).

$$n = D_0(m-1)! + D_1(m-2)! + \cdots\ D_{m-2}(1)! + D_{m-1}(0)! \qquad (49)$$

tal como se menciona en la investigación de Silva et al. (2019). Se destaca que este algoritmo define una función uno a uno (Aragona & Civino, 2021), lo cual es una propiedad importante, ya que significa que dos enteros diferentes $n_1 \neq n_2$ generan, a su vez, dos permutaciones diferentes. En esta investigación, se utiliza el parámetro Similarity Parameter (SP) para evaluar el daño por ruido en imágenes cifradas, tal como lo define Silva García, V.M., et al. (2024). Para generar la permutación, se toma en cuenta que la imagen tiene m píxeles. Se propone utilizar la cadena que se obtuvo en el algoritmo anterior, es decir, los bits a la derecha del punto decimal del resultado de la multiplicación $(0.172082 \times e)C_2$, donde $C_2 = x_1 \,||\, y_1$. El proceso de generación de permutaciones es el siguiente:

1. Se toman los 3 primeros bytes, y el valor entero asociado con esta cadena se denomina a_0. Se propone que $D_0 = a_0\ mod.m - 0$
2. Para el cálculo de a_1 se realiza un desplazamiento a la derecha de un byte, es decir, los bytes 2, 3 y 4. Entonces, el valor de a_1 es el número entero asociado a la cadena de bytes 2, 3 y 4. Por tanto, el cálculo de $D_1 = \alpha_1\ mod.m - 1$.
3. Según este procedimiento, la constante D_i se adquiere como $D_i = \alpha_i\ mod.m - i$. Cuando se consiguen las constantes, se calcula la permutación. Con relación a la generación de las S-boxes, el procedimiento es el siguiente: Un entero positivo se elige aleatoriamente K^2, que cumple con la condición $0 < K^2 < 512$; A partir de la curva $K^2\alpha$, el punto (x_2, y_2). El punto α es el elemento generador de la curva.

Algoritmo 3: Construcción del cronograma de llaves.

Los pasos para edificar el cronograma de llaves son:

1. Se elige aleatoriamente un número entero positivo, K^1 tal que $0 < K^1 < 2^{512}$.
2. Se calcula el punto $K^1\alpha$, que se denota como: (x_1, y_1). Donde α es el elemento generador de la curva.
3. Se propone que la constante C_2 de la Ec. (18) tome el valor entero positivo de la siguiente cadena: $x_1||y_1$.
4. Con la información del paso anterior se realiza el producto $(0.172082\ \times \mathrm{e})C_2$.
5. Del resultado anterior, se toman los bits necesarios del punto decimal de la derecha, de tal forma que la longitud de la cadena sea el tamaño de la imagen. Esta cadena se llamará k_1. De hecho, se propone que esta sea la primera clave del cronograma.
6. Para obtener el valor k_2 se procede de la siguiente manera: se realiza un desplazamiento circular de un bit a la izquierda de la tecla k_1, y el resultado es k_2. Entonces, para calcular la clave k_{i-1}, con $1 < i \leq 16$, se ejecuta un desplazamiento circular de un bit a la izquierda de la clave anterior.

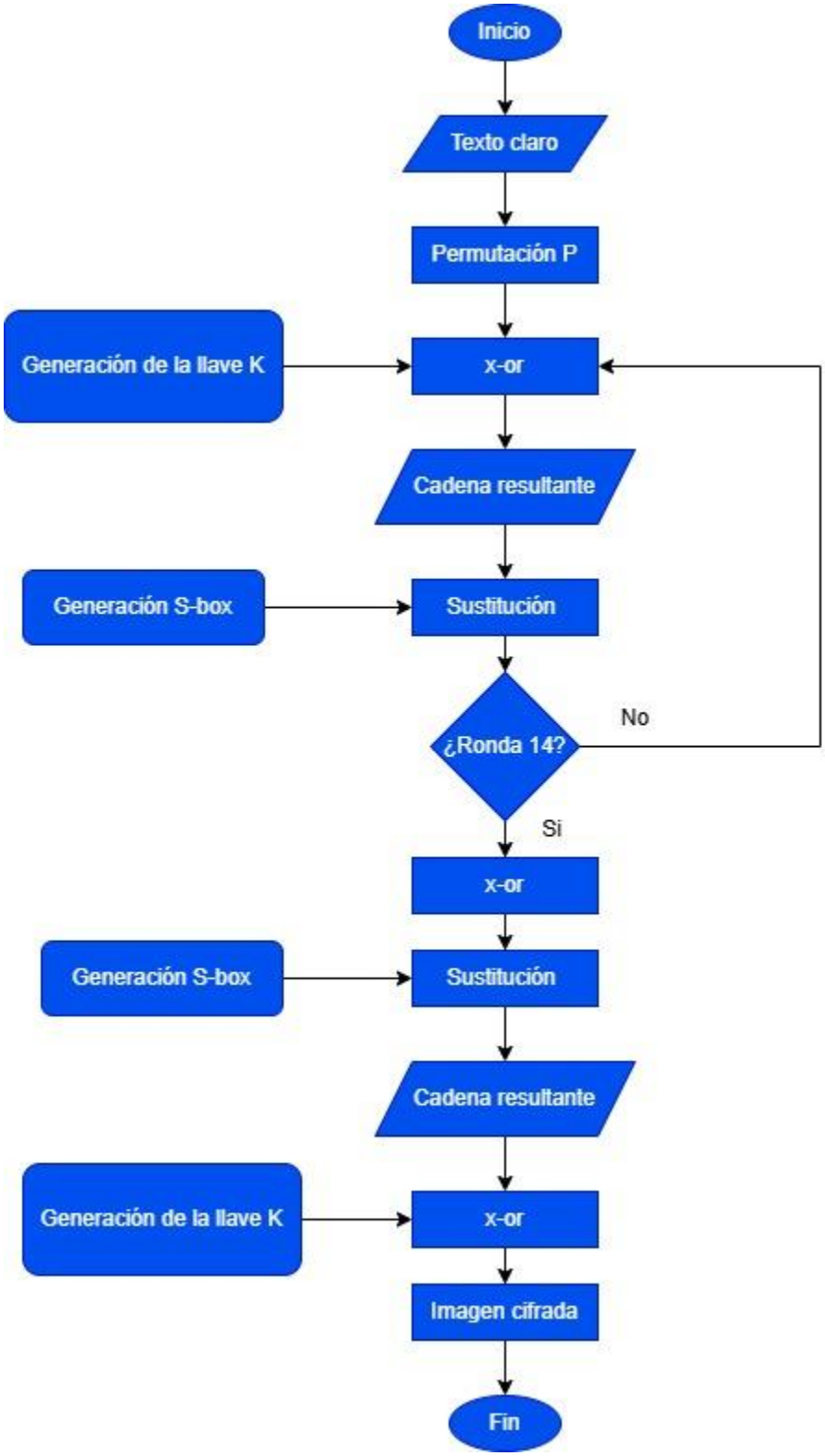


Figura 1. Proceso de Cifrado de una imagen.

Algoritmo 4. Construcción de las cajas (S-box).

1. Para la construcción de las S-boxes, la constante C_3 de la Ec. (18) se obtiene usando el entero positivo asociado con la cadena $x_2 \,||\, y_2$.
2. La multiplicación se realiza por $0.336590C_3e$ y la cadena de bits que se forma desde el punto decimal a la derecha se divide en bloques de 8 bits. Ahora, con esta información se calculan las constantes D_i para construir una permutación de 256 elementos, utilizando el algoritmo mencionado. Para obtener la primera constante D_0 se procede de la siguiente manera: se toma el primer byte de la cadena de bits después del punto decimal, y llame al número entero asociado con este byte b_0. Luego, el cálculo de la constante D_0 se realiza de la siguiente manera; $D_0 = b_0\ mod.\ 256 - 0$. Para obtener D_1, el segundo byte de la cadena se toma después del punto decimal. Este byte tiene un número entero asociado, denotémoslo como b_1. Con esta información la constante D_1, se obtiene de la siguiente manera: $D_1 = b_1\ mod.$ 256-1. Luego, siguiendo este mismo proceso se calcula la constante D_i como: $D_i = b_i\ mod. 256 - i$. Con $0 \leq i \leq 254$.
3. Una vez calculados los D_i, se utiliza la información mencionada en el inciso 3.1 para obtener la caja correspondiente. Cabe señalar que una S-box 8×8 es una permutación de 256 elementos. Finalmente, se menciona que todas las cajas se obtienen desplazando bytes a la derecha del punto decimal, y aplicando la operación modular.

3.1. Imágenes de prueba.

Las imágenes analizadas para este propósito se presentan en la Figura 2. Estas imágenes son bien conocidas en el área de procesamiento de imágenes y son de acceso libre. Tienen una resolución de 512×512 pixeles. Barbara y Cameraman son imágenes en escala de grises, y si se utiliza un sistema simétrico inadecuado para cifrarlas, existe el riesgo de que las imágenes cifradas no puedan pasar las pruebas de aleatoriedad propuestas en este trabajo.

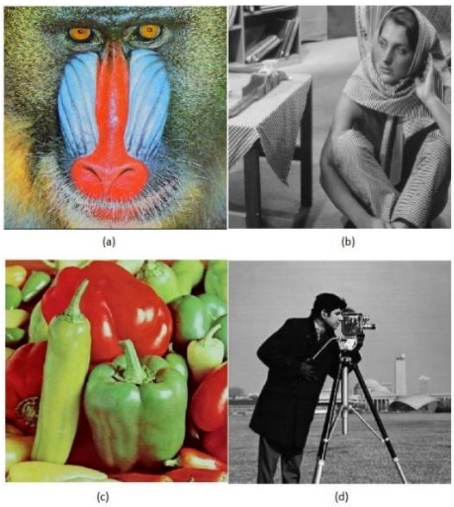
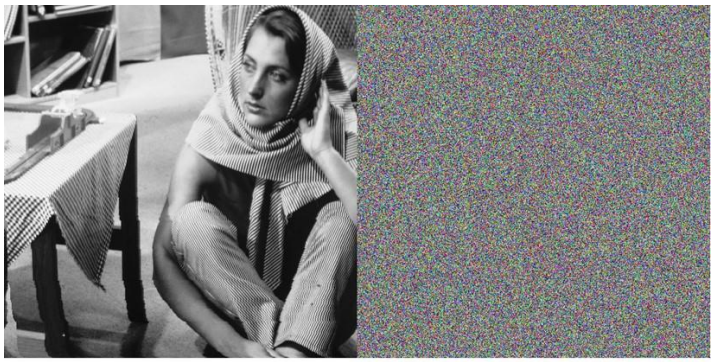


Figura 2. Imágenes utilizadas para analizar CICCE: a) Baboon b) Barbara c) Peppers d) Cameraman

4. PRUEBAS Y RESULTADOS

4.1. Pruebas realizadas.

La Figura 3, visualiza la imagen de Barbara original (a) y después en (b), el producto del cifrado con CICCE, donde a simple vista en (b) no se distingue la imagen ni se presentan rasgos de (a).



(a) (b)

Figura 3. Imagen de Barbara: (a) original y (b) cifrada con CICCE.

Para sustentar lo anterior, se muestran los resultados de imágenes cifradas sin daños. Los instrumentos para medir la aleatoriedad se dividen en dos:

1. Aquellos que presentan un resultado determinista, tales como: Entropía (Tabla 1), Correlación (Tabla 2), NPCR (Tabla 3), UACI (Tabla 4), AC (Tabla 5), Homogeneidad (Tabla 6), Energía (Tabla 7) y contraste (Tabla 8). Además, se reporta el promedio de los colores rojo, verde y azul.

Tabla 1. Entropía de las imágenes a color después del cifrado.

	Baboon	**Barbara**	**Peppers**	**Cameraman**
CICCE	7.99925	7.99926	7.99935	7.99933
Shafique & Ahmed, 2020	N/A	N/A	N/A	7.9716
Ibrahim & Alharbi, 2020	N/A	N/A	N/A	7.9023
(Zahid et al., 2021)	7.9964	N/A	N/A	N/A
(Zheng & Zeng, 2022)	7.9974	N/A	7.9970	7.9974

Tabla 2. Coeficiente de correlación de las imágenes a color después del cifrado.

	Baboon	**Barbara**	**Peppers**	**Cameraman**
CICCE	0.0039	0.0037	0.0021	0.0045
Shafique & Ahmed, 2020	0.0107	N/A	-0.0421	N/A
Ibrahim & Alharbi, 2020	N/A	N/A	N/A	0.0011
(Zahid et al., 2021)	.00568	N/A	N/A	N/A
(Zheng & Zeng, 2022)	0.0028	N/A	0.0021	0.0004

Tabla 3. Análisis NPCR de las imágenes a color después del cifrado.

NPCR	Baboon	Barbara	Peppers	Cameraman
Promedio	99.608	99.606	99.616	99.610

Tabla 4. Análisis UACI de las imágenes a color después del cifrado.

UACI	Baboon	Barbara	Peppers	Cameraman
Promedio	33.500	33.480	33.480	33.481

Table 5. Análisis AC de las imágenes a color después del cifrado.

AC	Baboon	Barbara	Peppers	Cameraman
Promedio	49.98	49.96	49.99	50.01

Table 6. Análisis de Homogeneidad de las imágenes a color después del cifrado.

Homogeneidad	Baboon	Barbara	Peppers	Cameraman
Promedio	0.389398	0.389299	0.389792	0.389606

Table 7. Análisis de la Energía de las imágenes a color después del cifrado.

Energía	Baboon	Barbara	Peppers	Cameraman
Promedio	0.015628	0.015629	0.015629	0.015630

Table 8. Análisis del Contraste de las imágenes a color después del cifrado.

Contraste	Baboon	Barbara	Peppers	Cameraman
Promedio	10.512	10.481	10.490	10.502

2. Aquellas mediciones que realizan una prueba de hipótesis: la Transformada Discreta de Fourier (Tabla 9) y la prueba de Ajuste de Bondad (Tabla 10). También en estas tablas se reporta el promedio de los colores básicos.

   Tabla 9. Aleatoriedad de las imágenes cifradas utilizando DTF (✓Aceptado, X Rechazado), cuando $\alpha = 0.01$.

	Baboon	Barbara	Peppers	Cameraman
Promedio	0.45✓	0.57✓	0.40✓	0.61✓

   Tabla 10. Prueba de Ajuste de Bondad (✓Aceptado, X Rechazado), cuando $\alpha = 0.01$

Color	Baboon	Barbara	Peppers	Cameraman
Promedio	246.9✓	247.5✓	241.1✓	268.9✓

Por otro lado, la Tabla 11, presenta los resultados NPCR, UACI y AC de dos imágenes, una completamente negra y otra completamente blanca.

A continuación, se usaron cuatro tipos de ruidos en las imágenes cifradas y el filtro de mediana 3×3 (Ibrahim et al, 2023). Se visualizan resultados de imágenes cifradas con modo AES-CBC y un porcentaje de ruido. Se analizaron dos casos de cifrado, uno con ruido aditivo y otro con oclusión. La Figura 4 (a) presenta la imagen original de Barbara. Posteriormente, esta imagen se cifra con el modo AES-CBC aplicando 40% de ruido aditivo del tamaño de la imagen aplicado a la imagen cifrada, así como se ilustra en la Figura 4 (b).

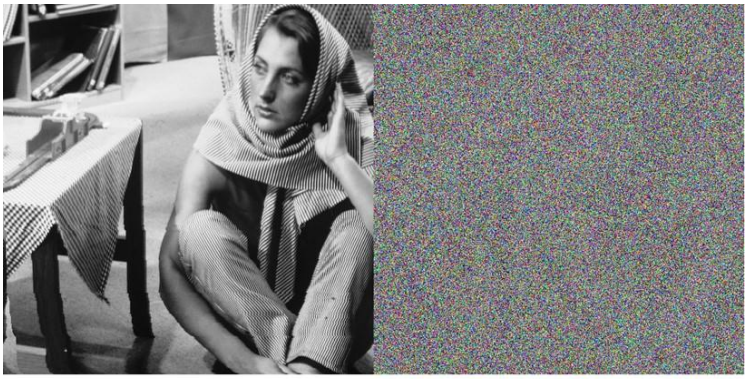


Figura 4. Imagen de Barbara: (a) original; (b) Descifrada cuando se aplicó ruido aditivo del 40% del tamaño de la imagen al cifrado AES-CBC.

La Figura 5 ilustra el segundo caso; la imagen de Cameraman es encriptada con AES-CBC, con ruido añadido de oclusión de 40% del tamaño de la imagen.

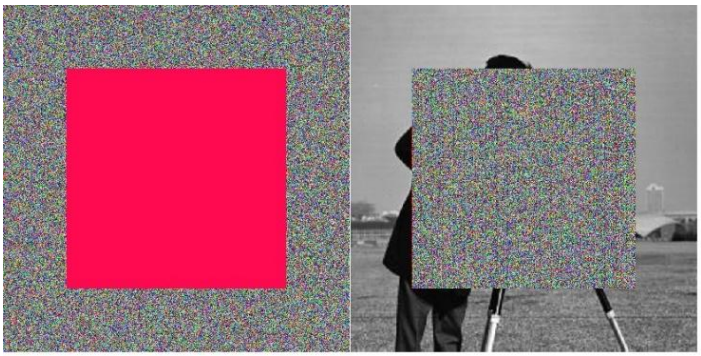


Figura 5. Imagen de Cameraman: (a) imagen cifrada con AES-CBC con un 40% de ruido de oclusión y (b) descifrada.

La Tabla 12 presenta el valor de SP con diferentes porcentajes de daño por ruido multiplicativo para las imágenes de prueba cifradas. La Tabla 13 muestra los valores de SP después de usar el filtro de mediana, cuando se aplicó un 40% de daño para los cuatro tipos de ruido. Los resultados de ambas tablas fueron generados con CICCE.

La Figura 6(a) presenta la imagen de Baboon descifrada con CICCE, después de haber insertado un ruido aditivo del 40% en la imagen cifrada. Posteriormente, se aplicó el filtro a la imagen descifrada con daños, y el resultado se muestra en la Figura 6(b).

Tabla 11. Valores NPCR, UACI y AC de una imagen completamente blanca y otra completamente negra.

Parámetro		**Imagen Negra**	**Imagen Blanca**
NPCR	Promedio	99.59	99.60
UACI	Promedio	33.45	33.46
AC	Promedio	49.98	49.99

Tabla 12. SP para diferentes tamaños de daño de las imágenes de prueba después del cifrado, utilizando ruido multiplicativo.

	% Ruido	Baboon	Barbara	Peppers	Cameraman
SP Promedio	20%	82.13	82.38	81.58	81.68
	30%	73.62	73.64	72.57	72.51
	40%	64.86	64.88	63.32	63.37

Tabla 13. SP cuando se aplicó el filtro de mediana de 3×3 a imágenes cifradas con un 40% de daño por diferentes ruidos.

Color	Tipo de ruido	Baboon	Barbara	Peppers	Cameraman
SP Promedio	*Oclusión*	80.19	85.82	91.23	91.25
	Aditivo	80.15	85.75	91.17	91.25
	Multiplicativo	80.33	86.03	91.46	91.45
	Gaussiano	80.56	85.80	91.09	91.17

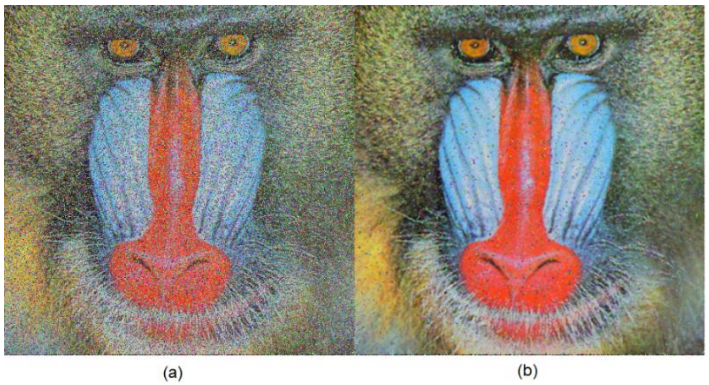


Figura 6. Imagen de Baboon: (a) descifrada con ruido y (b) descifrada y filtrada usando un filtro de mediana.

A continuación, el autor puede encontrar de forma muy puntual una serie de normas de estilo de gran utilidad para la elaboración de su manuscrito:

4.2 Análisis y discusión.

Los ataques se dividieron en tres:

1. Los que se aplican a la curva elíptica, los que se aplican al criptosistema simétrico propuesto y los que dañan las imágenes cifradas con ruido. El primero consistió en conocer la clave privada cuando se conoce la clave pública, lo que lleva al problema del logaritmo discreto. Debido a que el número primo de soluciones q utilizado en esta investigación es mayor o igual a 2^{512}. De ello se deduce que resolver el problema de logaritmo discreto en este escenario equivale a factorizar un n de tamaño 2^{15000}, de un esquema RSA, siendo mucho más grande que la versión actualmente en uso de RSA (Yarom et al., 2017). Respecto a un ataque de fuerza bruta, se hacen las siguientes reflexiones: considerando que $q \geq 2^{512}$, entonces el número de claves de CICCE a probar es mayor o igual a $(2^{512})^2$, porque se eligen dos puntos en aleatorio. Por lo tanto, realizar un ataque de fuerza bruta no es posible en este momento, porque el criptosistema AES-256 de 2^{256} llaves resiste un ataque de fuerza bruta (Bhat et al., 2021).
2. Con relación a los ataques al criptosistema propuesto se analizaron tres: ataque lineal, algebraico y diferencial. El ataque lineal y el algebraico, no se pudieron ejercer porque se desconocen S-boxes.

En cuanto al ataque diferencial, no se puede llevar a cabo porque valores de los parámetros NPCR≈99.6%, UACI≈33.4% y AC≈50% lo consideran como criptosistema robusto.

3. El tercer aspecto fue atacar las imágenes cifradas dañándolas por medio de ruido aditivo, multiplicativo, gaussiano y de oclusión. Se puede afirmar que el algoritmo de cifrado resiste daños de hasta un 40% del tamaño de la imagen de cada uno de los ruidos.

El uso de la Curve elíptica en CICCE permite distribuir las claves del sistema simétrico, porque sólo se requieren dos puntos de la curva, y estos se pueden enviar usando la misma curva. El esquema de comunicación segura sólo utiliza un único criptosistema para el cifrado de imágenes, la curva elíptica, y no dos como es el caso de la estructura PKI (Liu et al., 2021). En cuanto a la calidad del cifrado de las imágenes, se realizaron en dos direcciones: la primera se realizó según los resultados del DFT, y la prueba de bondad de ajuste propuesta. La segunda se analizó los resultados de la correlación, la entropía y los parámetros NPCR, UACI, AC, homogeneidad, contraste y energía. En ambas direcciones los resultados muestran que el cifrado de las imágenes robusto. De hecho, los resultados de homogeneidad, energía y contraste son similares a investigaciones recientes (Masood et al., 2020). Se realizó una comparación de la entropía con las investigaciones de (Shafique & Ahmed, 2020), (Zheng & Zeng, 2022), (Zahid et al., 2021) e (Ibrahim & Alharbi, 2020). Respecto a los dos primeros, la calidad de cifrado tiene una entropía de 7,99…, y la de CICCE es 7,999…; Además, con relación al número de claves, en el primero es 2^{200} y en el segundo no se menciona. Sin embargo, CICCE tiene más de 2^{512}. Respecto al tercero, el número de claves es 2^{208} y la calidad de las imágenes cifradas es 7,99… Por otro lado, el trabajo de (Silva García, V.M., et al, 2024) fue enfocado para imágenes de mayor tamaño, por lo que se requiere mayor capacidad computacional, además de la diferencia de que el mencionado es un criptosistema hibrido para imágenes con pérdida de datos. La aplicación para fundamentar los estudios de CICCE fue desarrollada en una computadora Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz 3.20GHz con 8GB de RAM, utilizando el lenguaje Java 8. En el caso de imagen de Cameraman de 512×512 pixeles en formato BMP, el tiempo de lectura, despliegue, cifrado, cifrado-despliegue correspondió a un tiempo total de 0.442 segundos. Para el resto de las imágenes, los resultados varían por ± 0.001 segundos.

5. CONCLUSIONES

En esta investigación, se desarrolló un criptosistema robusto para cifrar imágenes utilizando dos puntos de la curva elíptica. El número de soluciones de la curva es aproximadamente $q = 2^{560}$, por lo que no se puede realizar un ataque de logaritmos discretos. Además, resiste los siguientes ataques: lineal, diferencial, algebraico y fuerza bruta. Se señala que la permutación aplicada en cada proceso de cifrado es dinámica, por lo que el criptosistema CICCE es seguro.

En cuanto a la calidad de cifrado de las imágenes, se evaluó según los siguientes parámetros: entropía, correlación, Transformada Discreta de Fourier (DFT), prueba de bondad de ajuste, NPCR, UACI, AC, homogeneidad, energía y contraste. En todos los casos, los resultados fueron satisfactorios.

Finalmente, se mencionan dos aspectos adicionales: el primero es en relación con la comparación de resultados en imágenes cifradas con ruido, utilizando el criptosistema AES-CBC y CICCE, donde se observa que CICCE es superior a AES-CBC. El segundo aspecto es que el trabajo futuro pretende distribuir la semilla mediante algoritmos poscuánticos. Por último, en este trabajo no se hace ningún esfuerzo importante por construir S-boxes con alta no linealidad, ya que son dinámicas.

CONTRIBUCIÓN DE AUTORÍA CRediT

Los autores del presente artículo contribuyeron de manera equitativa en el desarrollo del trabajo en las siguientes áreas:

- Métodos matemáticos y codificación: Todos los autores participaron en la concepción y desarrollo de los métodos matemáticos subyacentes, así como en la implementación de los algoritmos de codificación que garantizan la integridad de las imágenes cifradas sin pérdida de datos.

- Pruebas y análisis de resultados: Los autores trabajaron en conjunto para diseñar y realizar las pruebas necesarias para validar la eficacia del algoritmo propuesto. Asimismo, colaboraron en el análisis de los resultados obtenidos, evaluando el rendimiento y la fiabilidad del cifrado en diversas condiciones.

- Redacción del manuscrito: Cada uno de los autores contribuyó a la escritura del artículo, asegurándose de que las secciones relativas a los aspectos matemáticos, metodológicos y experimentales del trabajo estuvieran correctamente descritas, revisadas y coherentes con los objetivos del estudio.

- Realización de experimentos: De forma colaborativa, los autores diseñaron y ejecutaron los experimentos empíricos necesarios para comprobar la funcionalidad del algoritmo, supervisando la recopilación de datos y el análisis de la calidad del cifrado en términos de precisión y eficiencia.

Esta contribución equitativa refleja el esfuerzo conjunto y colaborativo de todos los autores en el desarrollo y finalización de este trabajo de investigación.

DECLARACIÓN DE INTERESES CONTRAPUESTOS

Los autores declaran que no tienen intereses financieros en conflicto ni relaciones personales conocidas que pudieran haber influido en el trabajo presentado en este artículo.

DISPONIBILIDAD DE DATOS

Los conjuntos de datos generados y/o analizados durante el presente estudio están disponibles a solicitud razonable del autor correspondiente.

AGRADECIMIENTOS

Los autores agradecen al Instituto Politécnico Nacional de México (Secretaría Académica, COFAA, SIP y CIDETEC) y al CONAHCYT (SNI) por su apoyo para el desarrollo de este trabajo.

REFERENCIAS

Abdallah, A. A., & Farhan, A. K. (2022). A new image encryption algorithm based on multi chaotic system. Iraqi Journal of Science, 324-337. DOI: 10.24996/ijs.2022.63.1.31

Abdullah, A., & Mahalanobis, A. (2023). Minors solve the elliptic curve discrete logarithm problem. arXiv preprint arXiv:2310.04132. https://doi.org/10.48550/arXiv.2310.04132

Ali, W., Zhu, C., Latif, R., & Tariq, M. U. (2023). Image encryption scheme based on orbital shift pixels shuffling with ILM chaotic system. Entropy, 25(5), 787. https://doi.org/10.3390/e25050787

Altigani, A., Hasan, S., Barry, B., Naserelden, S., Elsadig, M. A., & Elshoush, H. T. (2021). A polymorphic advanced encryption standard–a novel approach. IEEE Access, 9, 20191-20207. https://doi.org/10.1109/ACCESS.2021.3051556

Aragona, R., & Civino, R. (2021). On invariant subspaces in the Lai–Massey scheme and a primitivity reduction. Mediterranean Journal of Mathematics, 18(4), 165. https://doi.org/10.1007/s00009-021-01781-x

Arif, J., Khan, M. A., Ghaleb, B., Ahmad, J., Munir, A., Rashid, U., & Al-Dubai, A. Y. (2022). A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution. IEEE Access, 10, 12966-12982.

Azouaoui, M., Kuzovkova, Y., Schneider, T., & van Vredendaal, C. (2022). Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks. Cryptology ePrint Archive.

Bassham III, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., ... & Vo, S. (2010). Sp 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards & Technology. https://dl.acm.org/doi/pdf/10.5555/2206233

Bhat, K., Mahto, D., Yadav, D. K., & Azad, C. (2021). Image Security Using Hyperchaos and Multidimensional Playfair Cipher. In Security and Privacy: Select Proceedings of ICSP 2020 (pp. 93-106). Springer Singapore. https://doi.org/10.1007/978-981-33-6781-4_8

de la Nación, A. G. (2022). Manual de digitalización de documentos. Boletín Del Archivo General De La Nación, 9(10), 41-117.

Eder, C., Pfister, G., & Popescu, A. (2021). Standard bases over Euclidean domains. Journal of Symbolic Computation, 102, 21-36. https://doi.org/10.1016/j.jsc.2019.10.007

El-Latif, A. A. A., Abd-El-Atty, B., Belazi, A., & Iliyasu, A. M. (2021). Efficient chaos-based substitution-box and its application to image encryption. Electronics, 10(12), 1392. https://doi.org/10.3390/electronics10121392

Filippone, G. (2023). Geometric methods in coding theory and cryptography.

Gallian, J. A. (2021). Contemporary abstract algebra. Chapman and Hall/CRC. https://doi.org/10.1201/9781003142331

Ge, B., Shen, Z., & Wang, X. (2023). Symmetric color image encryption using a novel cross–plane joint scrambling–diffusion method. *Symmetry*, *15*(8), 1499. https://doi.org/10.3390/sym15081499

Goel, A., Baliyan, H., Tyagi, S., & Bansal, N. (2024). End to end encryption of chat using advanced encryption standard-256. International Journal of Science and Research Archive, 12(1), 2018-2025. https://doi.org/10.30574/ijsra.2024.12.1.0923

Hernández-Díaz, E., Pérez-Meana, H., Silva-García, V., & Flores-Carapia, R. (2021). Jpeg images encryption scheme using elliptic curves and a new s-box generated by chaos. Electronics, 10(4), 413. https://doi.org/10.3390/electronics10040413

Hla, N. N., & Aung, T. M. (2019). Attack experiments on elliptic curves of prime and binary fields. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2018, Volume 1 (pp. 667-683). Springer Singapore. https://doi.org/10.1007/978-981-13-1951-8_60

Ibrahim, S., & Alharbi, A. (2020). Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. IEEE Access, 8, 194289-194302.

Ibrahim, A. G. A., Saleh, M., & Elmahallawy, A. A. (2023). De-Noising of Secured Stego-Images using AES for Various Noise Types. Przeglad Elektrotechniczny, 99(2).

Jahangir, S., Shah, T., & Haj Ismail, A. (2023). An algebraic and chaotic three-layered digital data encryption technique. Nonlinear Dynamics, 111(21), 20407-20423. https://doi.org/10.1007/s11071-023-08835-7

Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. IEEE Access, 9, 37855-37865. https://doi.org/10.1109/ACCESS.2021.3063237

Khan, M. R., Upreti, K., Alam, M. I., Khan, H., Siddiqui, S. T., Haque, M., & Parashar, J. (2023). Analysis of elliptic curve cryptography & RSA. Journal of ICT Standardization, 11(4), 355-378. https://doi.org/10.13052/jicts2245-800X.1142

Li, X., & Peng, H. (2023). Chaotic medical image encryption method using attention mechanism fusion ResNet model. Frontiers in Neuroscience, 17, 1226154. https://doi.org/10.3389/fnins.2023.1226154

Lin, C. H., Hu, G. H., Chan, C. Y., & Yan, J. J. (2021). Chaos-based synchronized dynamic keys and their application to image encryption with an improved aes algorithm. Applied Sciences, 11(3), 1329. https://doi.org/10.3390/app11031329

Liu, Y., Cui, Y., Harn, L., Zhang, Z., Yan, H., Cheng, Y., & Qiu, S. (2021). PUF-based mutual-authenticated key distribution for dynamic sensor networks. Security and Communication Networks, 2021, 1-13. https://doi.org/10.1155/2021/5532683

Liu, F., Sarkar, S., Wang, G., Meier, W., & Isobe, T. (2022, December). Algebraic meet-in-the-middle attack on LowMC. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 225-255). Cham: Springer Nature Switzerland.

Ma, X., & Wang, C. (2023). Hyper-chaotic image encryption system based on N+ 2 ring Joseph algorithm and reversible cellular automata. Multimedia Tools and Applications, 82(25), 38967-38992.

Masood, F., Boulila, W., Ahmad, J., Arshad, Sankar, S., Rubaiee, S., & Buchanan, W. J. (2020). A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos. Remote Sensing, 12(11), 1893. https://doi.org/10.3390/rs12111893

Mfungo, D. E., & Fu, X. (2023). Fractal-based hybrid cryptosystem: Enhancing image encryption with RSA, homomorphic encryption, and chaotic maps. Entropy, 25(11), 1478. https://doi.org/10.3390/e25111478

Mohamed, K. (2022). Chaos Based Image Encryption.

Moon, S., Baik, J. J., & Seo, J. M. (2021). Chaos synchronization in generalized Lorenz systems and an application to image encryption. Communications in Nonlinear Science and Numerical Simulation, 96, 105708. https://doi.org/10.1016/j.cnsns.2021.105708

Parida, P., Pradhan, C., Alzubi, J. A., Javadpour, A., Gheisari, M., Liu, Y., & Lee, C. C. (2023). Elliptic curve cryptographic image encryption using Henon map and Hopfield chaotic neural network. Multimedia Tools and Applications, 1-26. https://doi.org/10.1007/s11042-023-14607-7

Ran, B., Zhang, T., Wang, L., Liu, S., & Zhou, X. (2022). Image security based on three-dimensional chaotic system and random dynamic selection. Entropy, 24(7), 958. https://doi.org/10.3390/e24070958

Ravichandran, D., Banu S, A., Murthy, B. K., Balasubramanian, V., Fathima, S., & Amirtharajan, R. (2021). An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. Medical & Biological Engineering & Computing, 59, 589-605. https://doi.org/10.1007/s11517-021-02328-8

Sakthi kumar, B., & Revathi, R. (2024). A Comprehensive Review on Image Encryption Techniques using Memristor based Chaotic System for Multimedia Application. IETE Journal of Research, 1-25. https://doi.org/10.1080/03772063.2024.2373899

Shah, S. (2023). Some Families of Elliptic Curves.

Shafique, A., & Ahmed, F. (2020). Image encryption using dynamic S-box substitution in the wavelet domain. Wireless Personal Communications, 115, 2243-2268. https://doi.org/10.1007/s11277-020-07680-w

Shannon, C. E. (1948). A mathematical theory of communication. The Bell system technical journal, 27(3), 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Shatnawi, A. S., Almazari, M. M., AlShara, Z., Taqieddin, E., & Mustafa, D. (2023). RSA cryptanalysis—Fermat factorization exact bound and the role of integer sequences in factorization problem. Journal of Information Security and Applications, 78, 103614. https://doi.org/10.1016/j.jisa.2023.103614

Silva-García V.M., González-Ramírez M.D., Flores-Carapia R., Vega-Alvarado E., Rodríguez-Escobar E., A Novel Method for Image Encryption Based on Chaos and Transcendental Numbers, Vol. 7, IEEE Access, IEEE, (2019), pp: 163729–163739. https://doi.org/10.1109/ACCESS.2019.2952030

Silva-García, V. M., Flores-Carapia, R., González-Ramírez, M. D., Vega-Alvarado, E., & Villarreal-Cervantes, M. G. (2020). Cryptosystem Based on the Elliptic Curve With a High Degree of Resistance to Damage on the Encrypted Images. IEEE Access, 8, 218777-218792. https://doi.org/10.1109/ACCESS.2020.3042475

Silva-García, V. M., Flores-Carapia, R., Cardona-López, M. A., & Villarreal-Cervantes, M. G. (2023). Generation of boxes and permutations using a bijective function and the Lorenz equations: An application to color image encryption. Mathematics, 11(3), 599.

Silva-García, V. M., Flores-Carapia, R., & Cardona-López, M. A. (2024). A Hybrid Cryptosystem Incorporating a New Algorithm for Improved Entropy. Entropy, 26(2), 154.

Singh, K. N., & Singh, A. K. (2022). Towards integrating image encryption with compression: a survey. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 18(3), 1-21. https://doi.org/10.1145/3498342

Song, X., Shi, M., Zhou, Y., & Wang, E. (2022). An image compression encryption algorithm based on chaos and ZUC stream cipher. Entropy, 24(5), 742. https://doi.org/10.3390/e24050742

Stinson, D. R., & Paterson, M. (2018). Cryptography: theory and practice. CRC press. https://books.google.com.mx/books?id=nHxqDwAAQBAJ&lpg=PT12&ots=LkW4prG6CE&dq=CRYPTOGRAPHY%3A%20Theory%20and%20practice&lr&hl=es&pg=PT28#v=onepage&q=CRYPTOGRAPHY:%20Theory%20and%20practice&f=false

Wang, S., Peng, Q., & Du, B. (2022). Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Optics & Laser Technology, 148, 107753. https://doi.org/10.1016/j.optlastec.2021.107753

Washington, L. C. (2008). Elliptic curves: number theory and cryptography. CRC press. https://books.google.com.mx/books?id=nBfCEqpYKW0C&lpg=PP1&ots=sM8v2aMbsX&dq=ELLIPTIC%20CURVES%20Number%20Theory%20and%20Cryptography&lr&hl=es&pg=PA49#v=onepage&q=ELLIPTIC%20CURVES%20Number%20Theory%20and%20Cryptography&f=false

Yu, J., Li, C., Song, X., Guo, S., & Wang, E. (2021). Parallel mixed image encryption and extraction algorithm based on compressed sensing. Entropy, 23(3), 278. https://doi.org/10.3390/e23030278

Zahid, A. H., Ahmad, M., Alkhayyat, A., Hassan, M. T., Manzoor, A., & Farhan, A. K. (2021). Efficient dynamic S-box generation using linear trigonometric transformation for security applications. IEEE Access, 9, 98460-98475.

Zeng, J., & Wang, C. (2021). A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata. Security and Communication Networks, 2021, 1-15. https://doi.org/10.1155/2021/6675565

Zhang, Z., Tang, J., Ni, H., & Huang, T. (2023). Image adaptive encryption algorithm using a novel 2D chaotic system. Nonlinear Dynamics, 111(11), 10629-10652.

Zhang, M., Zhou, J., Zhang, G., Zou, M., & Chen, M. (2021). EC-BAAS: Elliptic curve-based batch anonymous authentication scheme for Internet of Vehicles. Journal of Systems Architecture, 117, 102161. https://doi.org/10.1016/j.sysarc.2021.102161

Zhang, Y. (2021). Statistical test criteria for sensitivity indexes of image cryptosystems. Information Sciences, 550, 313-328. https://doi.org/10.1016/j.ins.2020.10.026

Zhang, D., Chen, L., & Li, T. (2021). Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation. Entropy, 23(3), 361. https://doi.org/10.3390/e23030361

Zheng, J., & Zeng, Q. (2022). An image encryption algorithm using a dynamic S-box and chaotic maps. Applied Intelligence, 52(13), 15703-15717.

Zhou, S., Qiu, Y., Wang, X., & Zhang, Y. (2023). Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. Nonlinear Dynamics, 111(10), 9571-9589.