Revista Cubana de Ingeniería Vol. XII (2) e278 (2021) ISSN: 2223-1781

Artículo Original

Encriptado de Imágenes Basado en Advanced Encryption Standard y Caos

Image Encryption Based on Advanced Encryption Standard and Chaos

Ernesto Godínez-Rodríguez[1,*], Miguel Patiño Ortíz[2], Alexander Balankin[2], Rolando Flores Carapia[3], Julián Patiño Ortíz[2], Víctor Manuel Silva García[3], Miguel A. Martínez Cruz[2]

[1]Centro de Innovación y Desarrollo Tecnológico en Cómputo (CIDETEC). Instituto Politécnico Nacional. Av. "Juan de Dios Bátiz" s/n esq. Miguel Othón de Mendizábal, Col. Nueva Industrial Vallejo, Del. Gustavo A. Madero. Ciudad de México, México

[2]Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME). Instituto Politécnico Nacional. Manuel de Anda y Barredo Edificio 5, 3er piso. Unidad Profesional Adolfo López Mateos, Zacatenco 07738, Gustavo A. Madero. Ciudad de México, México

[3]Centro de Innovación y Desarrollo Tecnológico en Cómputo. Instituto Politécnico Nacional, México.

*Autor de correspondencia: egodinez@ipn.mx

Recibido: 2 marzo 2021 **Aceptado:** 27 abril 2021 **Publicado:** 30 abril 2021

Resumen

Los entornos inseguros de comunicación, como Internet, se exponen a que la información que circula a través de ellos sea utilizada sin permiso por terceros. En la actualidad, las imágenes cada día cobran más relevancia como una evidencia de la realidad y se incluyen en los sistemas de información que contienen datos biométricos, planos industriales o militares, imágenes médicas y hasta obras artísticas entre otras, las cuales transitan por la red. Este trabajo presenta un nuevo método para el cifrado de imágenes, se basa en el algoritmo simétrico Advanced Encryption Standard (AES) modificado con una serie caótica y una permutación. Las propiedades pseudoaleatorias de las series numéricas generadas con la ecuación logística, aplicándoles una permutación variable, operan con cada bloque de 128 bits de la imagen original, antes de comenzar la tercera ronda del algoritmo AES. Para evaluar los resultados se calculó la correlación y la entropía de la imagen encriptada, también se obtuvo la distribución de los 256 valores de cada color en modo RGB y se presentó el histograma de las imágenes originales y encriptadas. Además, se calculó el índice de Lyapunov de la serie de números generados por la ecuación logística para comprobar sus características caóticas. El método propuesto no tuvo un consumo de tiempo significativo en comparación con el obtenido solo con AES, el cual se probó cifrando imágenes conocidas de la literatura correspondiente e imágenes con cadenas repetitivas y poca profundidad, para mostrar el fortalecimiento de AES con el nuevo esquema.

Palabras clave: AES, caos, encriptación, criptosistema simétrico, cifrado de imágenes

Abstract

Insecure communication environments such as the Internet expose the information that circulates through this medium to be used without permission by third parties. Nowadays, images are becoming more and more relevant as evidence of reality and are included in information systems that contain

biometric data, industrial plans, medical images and even artistic works, among others, which pass through the network. This work presents a new method for image encryption. It is based on the symmetric Advanced Encryption Standard (AES) algorithm modified with a chaotic series and a permutation. The pseudo-random properties of the numerical series generated with the logistic equation, applying a variable permutation, operate with each 128-bit block of the original image, before starting the third round of the AES algorithm. To evaluate the results, the correlation and entropy of the encrypted image were calculated, the distribution of the 256 values of each color was also obtained in RGB mode, and the histogram of the original and encrypted images was presented. In addition, the Lyapunov index was calculated from the series of numbers generated by the logistic equation to check its chaotic characteristics. The proposed method did not have a significant time consumption compared to that obtained only with AES, which was tested by encrypting known images from the corresponding literature and images with repetitive chains and shallow depth, to show the strengthening of AES with the new scheme.

Keywords: AES, chaos, encryption, symmetric cryptosystem, image encryption

1. Introducción

El uso extendido de los dispositivos de comunicación a través de internet y las redes sociales, han permitido que cada vez más información se encuentre digitalizada. El número y la variedad de transacciones con esta información, cuyo aumento ya es exponencial, se realiza mediante canales abiertos compartidos y entornos inseguros, exponiéndose a que en cualquier momento un agente externo pueda interceptarla, modificarla o incluso robarla y en general, hacer un mal uso de ella, según el Informe de Investigaciones de Violación de Datos 2018, 11ª Edición. Por otro lado, las imágenes se utilizan cada vez más como evidencia de la realidad, ya que simplifican el proceso de identificación; las bases de datos incorporan cada vez más información a través de imágenes para describir o identificar cualquier tema [1]. Millones de personas aportan datos que se transmiten a toda hora por su dispositivo y tienen que ver con su identidad [2], como la autenticación biométrica [3] o el reconocimiento de huellas dactilares [4], rostros o firmas digitales. También las aplicaciones industriales y comerciales manejan imágenes sensibles, como expedientes médicos digitalizados, planos arquitectónicos, documentos financieros y económicos, planos de proyectos industriales o militares, imágenes secretas y fotografías artísticas, que se almacenan, procesan y transmiten. Por esa razón, muchas de estas imágenes deben estar encriptadas. Sin embargo, esta es una tarea que consume recursos, lo que motiva a la búsqueda de algoritmos nuevos e innovadores que permitan mayor seguridad y, una mejora en el rendimiento y consumo de recursos. Se han propuesto diversos métodos para el cifrado de imágenes, la mayoría de ellos basados en teorías matemáticas [5], por ejemplo, el teorema de restos chinos, la curva elíptica o las funciones caóticas.

En cuanto a la aplicación del caos al cifrado de imágenes se han desarrollado muchos trabajos. En [6] se propone un método simétrico por bloques que cifra imágenes para eliminar los patrones que este tipo de métodos determinísticos muestran como una debilidad en cierto tipo de imágenes; coincidente con uno de los objetivos del presente trabajo, que con el menor consumo de recursos AES no presente patrones reconocibles en la imagen cifrada. En [7] se presenta un método de cifrado de imágenes, con un nuevo generador de números aleatorios (RNG) basado en caos y se construye con ellos la tabla S-Box utilizada con AES y un sistema caótico, y por ejemplo en [8] se propone un algoritmo de cifrado de imágenes rápido basado en el mapa sinusoidal y el mapa caótico, descartando AES para el proceso de cifrado. Se implementan dos funciones caóticas para mejorar la no linealidad y la aleatoriedad, reconociendo los mapas caóticos como un núcleo del caos. Se basan en mapas caóticos de alta dimensión y los resultados presentados son satisfactorios: la correlación y la entropía encontradas son del orden de 0,0030 y 7,9976, respectivamente, por lo que sirvieron de

referencia para el presente trabajo. Se presenta un esquema basado en la permutación y difusión a través de un mapa logístico entrelazado en [9], como método inicial de encriptación de imágenes con más parámetros de control y condiciones iniciales que el clásico mapa logístico unidimensional (1D). Se menciona el problema de la alta redundancia en los métodos de cifrado tradicionales, y obtiene 7,999330 y 7,997158 de entropía para Baboon y Lena.

En [10] se aumentó el número de rondas de 10 a 16 para un tamaño de clave de 128 bits, con el fin de incrementar su complejidad. Sin embargo, el aumento en el número de rondas requiere más tiempo de cálculo. Se presentó una propuesta para un método de cifrado rápido basado en el algoritmo AES para el cifrado de imágenes HD en escala de grises, disminuyendo el número de rondas a 9 en lugar de 10. Esto redujo el tiempo de cifrado aproximadamente en 1/10. Una segunda modificación propuso una caja Sbox nueva y simple. Los resultados de correlación y entropía encontrados son -0,0215 y 7,9999, respectivamente, aunque el método no se aplicó a imágenes conocidas y es difícil comparar su calidad.

El método de cifrado de imágenes en [11] utiliza un mapa logístico caótico 3D con codificación de ADN para la confusión y difusión de píxeles de la imagen, utiliza tres claves simétricas para inicializar el mapa logístico del caos 3D, lo que fortalece el algoritmo de cifrado. Los resultados de correlación para Lena, Baboon, Peppers y Barbara respectivamente son de 0,0035; -0,0010; 0,0089; 0,0010 y de entropía de 7,9899; 7,9893; 7,9890 y 7,9894, muy adecuados, aunque el espacio de llave es de 2^{32}.

A pesar de muchas de sus ventajas, AES presenta algunas debilidades a la hora de cifrar imágenes con redundancia y poca profundidad. En este desarrollo, se proponen algunas modificaciones al algoritmo AES para su fortalecimiento. Se aplica un enfoque novedoso que utiliza una permutación y la ecuación logística para cambiar cadenas de bits repetitivas en una imagen. Fue seleccionado el modo de cifrado CBC (Cipher Block Chaining), por añadir mayor seguridad que otros modos existentes [12], sobre todo por aplicar un XOR a cada bloque de entrada. El sistema incluye las funciones de cifrado y descifrado, las funciones para el cálculo de entropía, correlación, índice de Lyapunov, gráfica de la ecuación Logística y los histogramas, así como su visualización gráfica y manejo con menús, el cual fue desarrollado en su totalidad en lenguaje C++.
El algoritmo propuesto en el presente trabajo puede ser utilizado en documentos no sólo con archivos de formato tipo imagen, sino cualquier otro formato como texto, ya que opera con cadenas de 128 bits, con lo que podemos resaltar la mayor competencia del presente trabajo.

El presente desarrollo se organiza de la siguiente manera: en la Sección 2 se presentan los métodos propuestos y su funcionamiento: el criptograma AES, la Permutación JV y la generación de números pseudoaleatorios con la ecuación Logística. Se presenta el diagrama del algoritmo propuesto, que combina AES y caos; en la Sección 3 se presentan los resultados y su análisis, considerando parámetros como el índice de Lyapunov, el coeficiente de correlación, la entropía, la redundancia, así como la variación mínima de la llave para cifrar y descifrar. Finalmente, en la Sección 4, se presentan las conclusiones.

2. Materiales y Métodos

Los esquemas visuales criptográficos son protocolos que codifican un mensaje formado por una imagen definida por píxeles en lugar de codificar un mensaje de texto definido por letras y números [3]. La imagen digital es una matriz de números de $n \times m$ píxeles, donde el nivel de gris de cada píxel (Xi, Yj) varía de 0 (negro) a 255 (blanco). En las imágenes en color hay tres matrices, uno para cada color RGB (Red, Green, Blue). Los números entre 0 y 255 para cada color son representados con 8

bits, por lo que una imagen necesita un byte por píxel con sus 256 variantes de color, esto es 3 bytes para cada pixel en imágenes de color [13].

Hay imágenes que contienen cadenas o bloques contiguos con solo ceros o unos, como letras escaneadas, imágenes en blanco y negro o símbolos con poca variación en su forma. Cuando estas imágenes están encriptadas solo con AES, existen patrones que se pueden observar a simple vista en la imagen encriptada, descubriendo información sobre el contenido de la imagen [14]. En general, al cifrar una imagen que tiene un bajo nivel de aleatoriedad en sus bits, el resultado podría ser un cifrado deficiente que muestre información sobre la imagen original. Esto se debe a que la distribución de diferentes tonalidades en colores primarios sigue un patrón determinado [15]. La Ecuación Logística y la Permutación JV han sido cuidadosamente seleccionadas para modificar el algoritmo AES, porque ofrecen un menor consumo de recursos de tiempo con mejores indicadores de entropía y correlación. En el presente trabajo se desarrolló un método para el cifrado de imágenes sin pérdidas en formato BMP, utilizando el criptograma Advanced Encryption Standard (AES) reforzado con la Permutación JV [16] y el comportamiento caótico de la ecuación logística, antes de iniciar la tercera ronda de AES.

AES

El método principal utilizado en el presente trabajo es AES (Advanced Encryption Standard), desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, también conocido como Rijndael. Es un esquema de cifrado de bloques adoptado como estándar internacional, anunciado por el Instituto Nacional de Estándares y Tecnología como NIST FIPS PUBS 197 2001 [17] y se convirtió en un estándar efectivo el 26 de mayo de 2002. Hoy en día, AES es uno de los más populares algoritmos así como el más estudiado y utilizados en criptografía simétrica. Aunque no es tan rápido como otros métodos, en general tiene un margen de seguridad mucho mayor [18]. La base AES se toma de la teoría matemática de los Grupos Finitos de Evarist Galois [17]. La unidad básica del algoritmo AES es un byte, una secuencia de 8 bits tratada como una entidad simple. Las entradas y salidas de información, así como la clave de AES son secuencias de bits contiguos que se procesan en arreglos de bytes, formando bloques de 128 bits = 16 bytes de 8 bits (en el presente trabajo *InputBlock* = 128 bits por bloque). Se hará referencia a los bytes como a_n, donde $0 \leq n < 16$. Los valores de cada byte en el algoritmo AES se presentarán como la concatenación de sus valores de bits individuales (0 o 1). Estos bytes se interpretan como elementos de campo finito (basados en la Teoría de Campos Finitos de Évariste Galois [17]) usando una representación polinomial (Ecuación 1) (NIST FIPS PUBS 197 2001) [17]:

$$\sum b_i x^i = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0 \quad (1)$$

AES es un algoritmo de cifrado simétrico, en el que se aplican 4 transformaciones a cada bloque de entrada de 128 bits organizado en una matriz de 4x4 bytes llamada Estado. SubBytes sustituye cada byte mediante la tabla de sustitución SBox, ShfitRows. En la matriz estado la segunda fila se desplaza a la derecha una vez, la tercera fila se desplaza a la derecha dos veces y la cuarta fila se desplaza a la derecha tres veces; en MixColumns cada byte se reemplaza por un valor que depende de los 4 bytes en la misma columna a través de la matriz de Estado con la multiplicación en Grupos Finitos (2^8) usando 4 términos de la Ecuación 1 y en AddRoundKey se aplica un XOR con el bloque de entrada y la clave de ronda. Estas 4 transformaciones se aplican juntas en dos etapas, una de 9 rondas y otra de una ronda final ligeramente diferente a las primeras (NIST FIPS PUBS 197 2001) [18].

De los 5 modos de operación para algoritmos simétricos estandarizados por el NIST (National Institute for Standards and Technology), en este trabajo se utilizó el modo CBC (Cipher Block

Chaining), porque cuando varios bloques de texto sin formato se cifran con la misma clave, surgen una serie de problemas de seguridad; el mecanismo de encadenamiento de CBC ofrece el modo más apropiado para cifrar imágenes [19,20].

El modo de cifrado CBC inicia con un XOR entre el bloque de entrada y un Vector de Inicialización (IV), ambos de la misma longitud. Enseguida al bloque resultante se le aplica el cifrado y posteriormente el bloque cifrado toma el lugar de Vector de Inicialización del siguiente bloque de entrada y así sucesivamente. El uso del vector de inicialización es importante, pues de no usarlo, podría ser susceptible de ataques de diccionario. También es necesario que el IV sea aleatorio y no un número secuencial o predecible [20].

La Ecuación Logística

La ecuación logística (2) tiene su base teórica en el estudio de la dinámica poblacional [21], aunque existen muchas disciplinas donde se utiliza esta ecuación fundamental por ser una de las fuentes caóticas más sencillas con los parámetros adecuados.

$$x_{n+1} = r x_n (1 - x_n) \quad (2)$$

Para el presente desarrollo se han generado los números x_{n+1} necesarios para cada imagen con los valores iniciales $x = 0{,}1$; $x = 0{,}2$ y $r \in [0; 4]$. Los valores resultantes que aparecen en la Tabla 1 y la Figura 1 muestran el límite del parámetro r hasta llegar a valores caóticos, ya que no muestran ningún período ni patrón. El exponente de Lyapunov λ [22] se define con la Ecuación 3 y es la sumatoria del logaritmo del valor absoluto de la derivada de la función. En nuestro caso λ_l será el índice correspondiente obtenido de la derivada de la ecuación logística (4).

$$\lambda = \frac{1}{n} \sum_{i=0}^{n-1} ln\,|f'(x_i)| \quad (3)$$

$$\lambda_l = \frac{1}{n} \sum_{i=0}^{n-1} ln\,|r - 2rx_i| \quad (4)$$

En la Tabla 1 aparecen algunos valores de λ_l donde se aprecian los estados de normal o caótico, de acuerdo con [22], según el valor de ***r***, en donde un exponente positivo corresponde un estado caótico, gráficamente con $r = 4$ se aprecia en las Figuras 1 y 2.

El índice de Lyapunov mide la tasa exponencial promedio de divergencia de las órbitas cercanas [22]. Cualquier sistema que contenga al menos un exponente positivo de Lyapunov se define como caótico, donde la magnitud del exponente refleja la escala de tiempo en la que la dinámica se vuelve impredecible [23]. Para determinar la divergencia entre trayectorias cercanas, se grafican con dos valores iniciales cercanos. La Figura 2 muestra estas diferencias. En ella se aprecia el comportamiento de la ecuación logística con $r = 4$ y dos valores iniciales de $X_{n.}$. La Figura 3 muestra el comportamiento a largo plazo con la gráfica de bifurcación de la ecuación logística de X_{n+1} desde $r = 1$, trazando órbitas de 100 puntos con incrementos de r de 0,0005; gráfica que ya es un ícono en los sistemas dinámicos no lineales [22] y que corresponde a los estados de la Tabla 1. En la Figura 3 se aprecia que para $r > 3{,}2$ se presentan la primera bifurcación y, en $r > 3{,}5$ inician 2 órbitas con bifurcaciones más cerradas que se pierden y se mezclan, contrastando con $r < 3{,}2$. En $r = 3{,}57$ inician 2 nubes de puntos que según [22] revela una mezcla de orden y caos cada vez más extendida conforme r aumenta. En el presente trabajo se obtuvieron los números pseudoaleatorios con $r = 4$, parámetro en el que en la Figura 3 aparece la maraña caótica [22] de bifurcaciones.

Tabla 1. Cálculo del exponente de Lyapunov λl para la ecuación logística variando r, con n = 1000, valor inicial Xn = 0,1

r	λ_l	**Estado**
2,000009	-5,019849	Normal
2,500000	-0,300148	Normal
3,000000	-0,002509	Normal
3,500000	-0,368223	Normal
3,569643	-0,000211	Normal
3,569644	-0,000128	Normal
3,569646	0,000030	Caótico
3,600000	0,083154	Caótico
3,700000	0,159633	Caótico
3,800000	0,193306	Caótico
3,900000	0,212308	Caótico
4,000000	0,300713	Caótico
4,000001	0,301375	Caótico

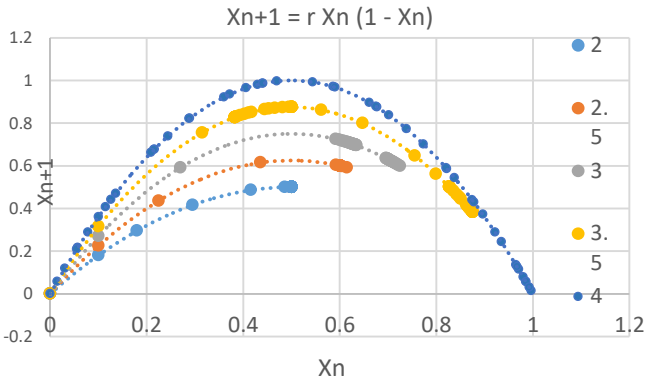


Fig.1 Valores de X_{n+1} vs X_n: calculado con Ecuación 2, variando r= 2; 2,5; 3; 3,5 hasta 4

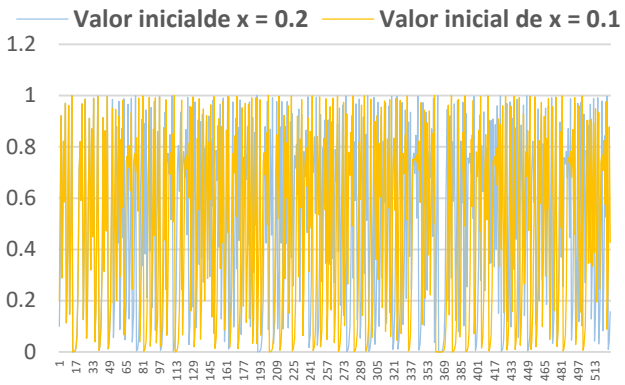


Fig.2 Diferencias de $f(x_{n+1})$ vs t, valuado con Ecuación 2, valores iniciales X_0=0,1 y X_0=0,2, con r = 4

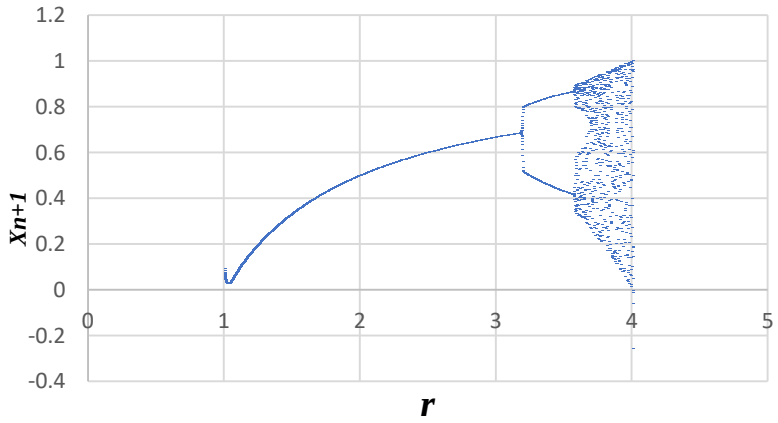


Fig.3 Gráfica de Bifurcación de la ecuación Logística con 1 < r ≤ 4 órbitas de 100 con incrementos de r del orden de 0,0005

Permutación JV

En la tercera ronda del criptograma de AES, antes de iniciar con la subrutina subBytes, se aplica el algoritmo con una cadena de 16 caracteres de entrada que es equivalente a un bloque de 128 bits de la imagen original. Estos caracteres tienen un orden inicial que será modificado. La permutación cambiará la posición de cada uno de éstos 16 caracteres de entrada de la imagen. El nuevo ordenamiento es determinado por los números pseudoaleatorios generados previamente con la ecuación logística almacenados en el vector nLo[i] y según la secuencia del algoritmo basado en la permutación JV [16] siguiente:

0.- Se toma de la imagen la cadena de entrada *cadenaIn[i]* 128 bits o 16 bytes de 8 bits.
1.- Se define un arreglo incremental como sigue:
$X[0] = 0, X[1] = 1, X[2] = 2, \ldots X[i] = i,$ donde $0 \leq i < 16$
2.- Se obtiene el orden *A1* con los números pseudoaleatorios nLo[i] de la ecuación logística:
$A1 = nLo[i] \bmod (16-i)$
3.- Se obtiene el arreglo *P[i]* con el nuevo ordenamiento.
$P[i] = X[A1]$
4.- Se obtiene el arreglo cadenaOut[i] con la nueva cadena ordenada conforme al algoritmo.
$cadenaOut[i] = cadenaIn[P[i]]$
5.- Continua el algoritmo AEScon la subrutina subBytes.
6.- Este algoritmo se repite con cada bloque de 128 bits de la imagen en la tercera ronda del criptograma AES.

Algoritmo AES-CAOS

Implementando los números pseudo aleatorios generados con la ecuación logística en su rango caótico y aplicando la permutación JV en el criptosistema AES se desarrolló el algoritmo AES-CAOS que aparece en la Figura 4. Previo al inicio del algoritmo se generan 16 valores numéricos enteros pseudoaleatorios con la ecuación 2 de acuerdo a los parámetros explicados en la sección 2.2, para cada bloque de la imagen, indicado en el bloque caoticNum de la Figura 4, se selecciona por cada imagen un Vector Inicial y una llave principal también de una longitud de 128 bits, equivalente a 16 enteros con valores entre 0 y 256 en formato decimal o entre 00 y FF en hexadecimal, por ser el valor mínimo y máximo expresable con dos bytes, ya que las operaciones en las subrutinas del criptograma se realizan a nivel de bits, se aplica la misma llave a todos los bloques de la imagen.

AES inicia con la operación XOR entre el bloque de 128 bits de la imagen y la llave principal indicada con el bloque addRoundKey en la Figura 4. La llave principal a su vez genera 10 llaves que serán utilizadas en cada ronda del criptograma, indicado con el bloque de creaLlaves. A continuación, en las siguientes dos rondas el algoritmo AES ejecuta en cada bloque de 128 bits las subrrutinas SubBytes, ShiftRows, MixColumns y con AddRounKey el bloque de salida hace XOR con la llave de ronda generada previamente en creaLlaves; en la ronda 3 se aplica la Permutación JV. Posteriormente el algoritmo AES continua con las subrutinas mencionadas hasta completar 9 rondas y finaliza con una ronda corta formada con SubBytes, ShiftRows y AddRoundKey; este proceso de transformación es aplicado a cada bloque y hasta el último de 128 bits de la imagen, obteniendo con esto la imagen cifrada en su totalidad.

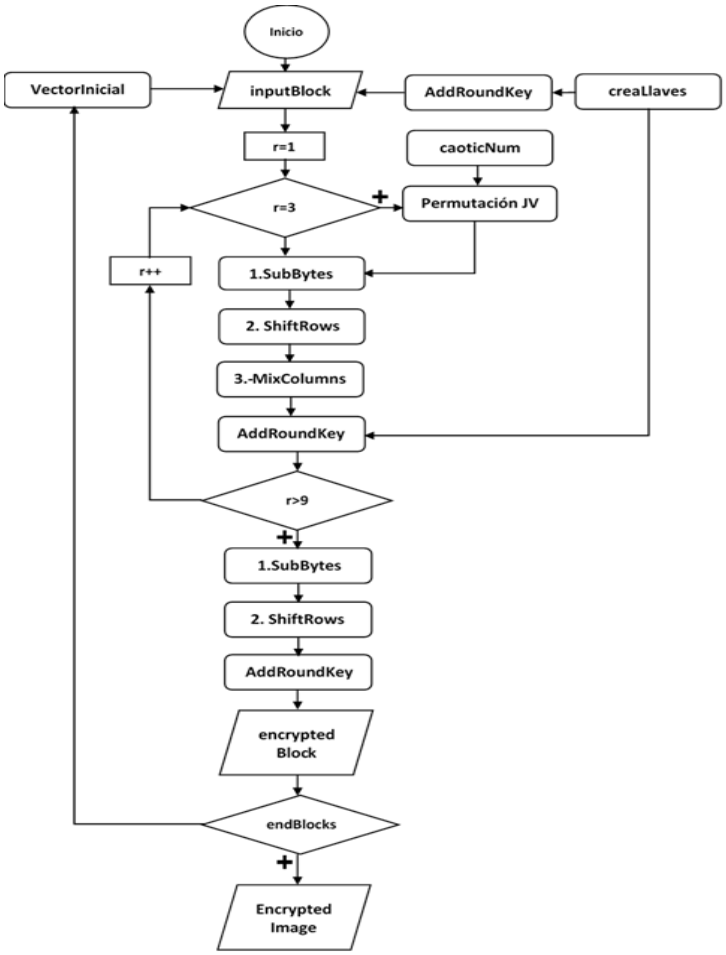


Fig.4 Implementación de la ecuación logística y el criptograma AES

3. Resultados y Discusión

La calidad de la imagen encriptada se evaluó con los criterios de Correlación y Entropía; también se obtuvieron los histogramas de cada imagen. Por otro lado, cabe mencionar que las imágenes encriptadas se generan sin pérdida de información, pues entidades como bancos, empresas o incluso gobiernos no permiten que las imágenes pasen por un proceso de compresión, con pérdida de información. El sistema de cifrado propuesto se adhiere en su implementación a la visión sistémica, ya que se conceptualiza como un problema global, donde se aplica un enfoque integral en una solución concreta.

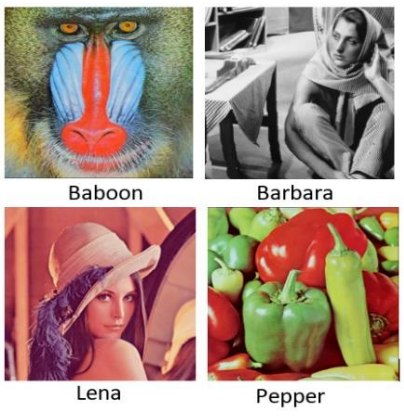


Fig.5 Imágenes de prueba

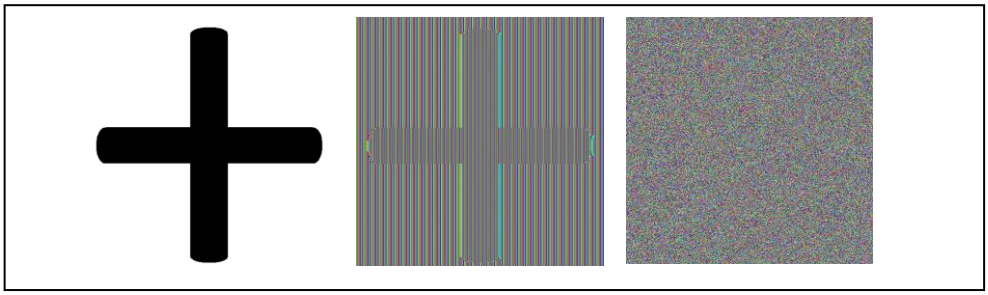


Fig.6 Cruz.bmp (izquierda), cifrado AES (centro) vs cifrado

El esquema de encriptación AES-CAOS, fue probado con el cifrado y descifrado de más de treinta imágenes. En la Figura 5 aparecen 4, muy utilizadas en la literatura del cifrado, con fines comparativos; las figuras 6 y 7 muestran ejemplos de imágenes con grupos repetitivos para ilustrar el fortalecimiento con el nuevo esquema de cifrado AES-CAOS y en la Tabla 3 aparecen 6 ejemplos de imágenes en diferentes ámbitos del quehacer humano, como en medicina, una tomografía y una radiografía; una huella humana, para biometría, usadas cada vez más como elementos de identificación en documentos electrónicos como firma y hasta para ingreso a lugares de trabajo o en dispositivos móviles, fotocopias de documentos con texto plano considerados confidenciales, tan usado en oficinas. Los resultados se comparan con algunos resultados de las mismas imágenes publicados en [9, 24-26]. Hay un repositorio con los archivos de todas estas imágenes, su cifrado y descifrado en formato BMP en https://imagesencription-egr.blogspot.com/, para más detalle.

Estas pruebas se llevaron a cabo en una computadora con un procesador Intel® Core ™ i3. El nivel de secreto está garantizado, ya que se probó con una variación mínima en la clave y los resultados de entropía muestran que es seguro. La imagen cruz.bmp de la Figura 6 muestra los valores bajos de entropía utilizando solo el algoritmo AES. La Tabla 2 muestra el comparativo de usar AES Y AES-CAOS, observando resultados satisfactorios aplicando el nuevo criptosistema.

AES vs AES-CAOS

En la Tabla 2 aparecen los valores comparativos de entropía y correlación de AES-CAOS y AES de 6 imágenes de prueba, seleccionadas por sus características de baja profundidad y grupos de bits repetitivos y como ejemplos del uso de imágenes en diferentes ramas. Para resaltar el fortalecimiento con el nuevo algoritmo AES-CAOS, se muestra en rojo, en la Tabla 2, los índices de entropía obtenidos con el cifrado AES, los cuales fueron mejorados en casi tres unidades de medida de entropía, y las imágenes ya no muestran pistas de su contenido. Las imágenes de texto plano, como pueden ser las conocidas fotocopias, mostraron una gran mejoría en los valores de entropía, en la imagen de "índice" se obtuvo una entropía de 5,47599666 cifrando con AES y 7,99941348 de entropía cifrada con AES-CAOS, asimismo, estas imágenes visualmente ya no muestran pistas del contenido de la imagen original.

Las Figuras 6 y 7 muestran más claramente 2 ejemplos comparativos de imágenes cifradas solo con AES y con AES-CAOS. Se puede apreciar que existen patrones en las imágenes encriptadas con el desempeño de AES, esta es una debilidad del algoritmo, como se puede ver muy claro en la imagen llamada "cruz". Se realizaron pruebas con imágenes comúnmente usadas en la literatura criptográfica, en las cuales se obtuvieron los indicadores de entropía, coeficiente de correlación con AES en la Tabla 3 y adicionalmente tiempo de encriptación y desencriptación AES-CAOS en la Tabla 4. Se puede ver que comparativamente los mejores resultados se encuentran con el nuevo método propuesto.

Tabla 2. Comparativo de los resultados de entropía y correlación de AES-CAOS y AES. Imágenes con grupos repetitivos y baja profundidad

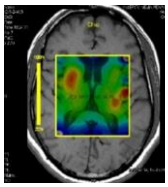
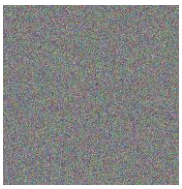
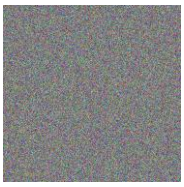
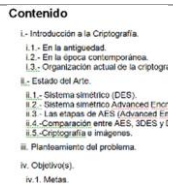
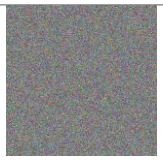
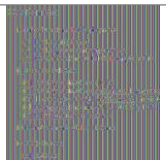
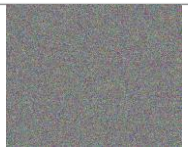
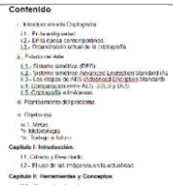
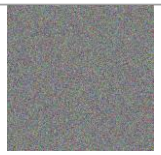
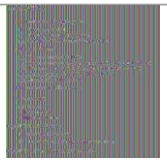
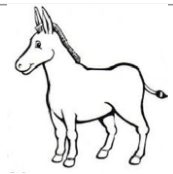
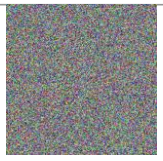
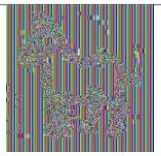
	Nombre del archivo	Imagen	Imagen Cifrada		AES-CAOS		AES	
			AES CAOS	AES	Entropía	Correlación	Entropía	Correlación
1	huella1				7,99975694	-0,004626	**7,4254866**	-0,036
2	Espectroscopia				7,99927698	-0,008768	**7,6180066**	-0,0992
3	índice				7,99941348	0,014367	**5,47599666**	-0,1342
	Tórax				7,99947322	0,015308	7,9933700	-0,021
5	indice1				7,99927138	0,024958	**5,17055333**	-0,1019
6	Burrito				7,99739740	0,0569	**5,96686**	-0,1365

Tabla 3. Resultados de la encriptación sólo con AES

Imagen	Entropía	Correlación
LENA	7,99786333	0,018065
BABOON	7,99773999	-0,01060
BARBARA	7,99781333	0,016627
PEPPERS	7,99783333	0,033944
CRUZ	4,68383	-0,1577
POEMASSORJUANA	5,8510	-0,0987

Como se mencionó anteriormente, algunas de las imágenes de prueba encriptadas reportadas en la Tabla 2 (Cruz y PoemasSorJuana) tienen índices de entropía y correlación bajos cuando se procesan con AES. Esta es una de las razones por las que se agrega una función al cifrado AES para eliminar esta debilidad, correspondiente al siguiente comentario:

"Si se supone que una imagen original tiene sus bytes ordenados, se puede contrastar con la imagen cifrada por medio del índice chi-cuadrada. En muchas imágenes con un chi-cuadrada bajo para cada color, por ejemplo, menos de medio millón, el criptosistema AES se puede aplicar directamente" [15], por lo antes expuesto, es necesario introducir un elemento en AES para eliminar esta inconsistencia.

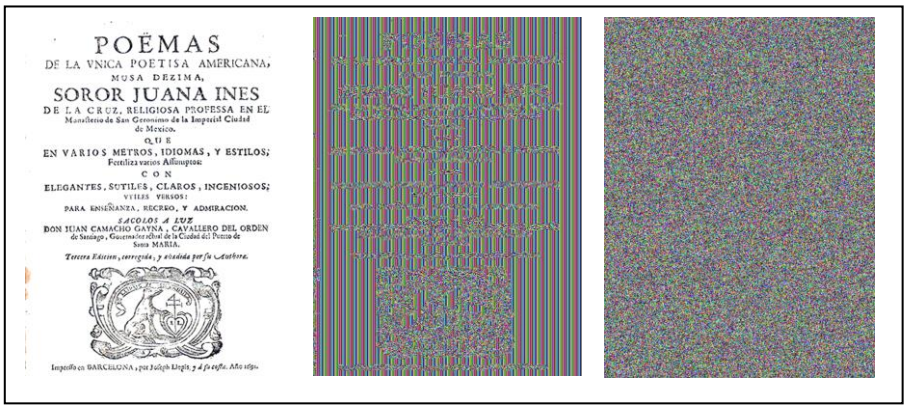


Fig.7 PoemasSorJuana. Cifrado AES (centro) VS cifrado AES-CAOS (derecha)

Tabla 4. Resultados de la encriptación con AES-CAOS

IMAGEN	Tiempo (Segundos)		Entropía	Correlación
	Encriptado	Descifrado		
LENA	2,437	2,953	7,99935844	0,0053690
BABOON	2,547	2,719	7,99930466	0,0084660
BARBARA	1,109	2,828	7,99936344	0,0042287
PEPPERS	1,031	2,641	7,99929357	0,0095525
CRUZ	0,953	1,063	7,99926338	0,0093233
POEMASSORJUANA	0,75	0,813	7,99989729	0,0097642

Seguridad y espacio de la clave

No se conocen claves débiles o semi-débiles para el algoritmo AES, ya que para que un algoritmo de cifrado de imágenes tenga alta seguridad, el espacio de claves debe ser al menos tan grande como 2^{100} [9], en AES-CAOS el espacio de llaves está dado por 2^{128}, por lo que no hay restricciones en la selección de la clave. Para la simetría del algoritmo, la única condición es que la clave de cifrado debe ser la misma. Si el algoritmo realiza el cifrado y descifrado incluso con la más mínima variación, los resultados no solo serán incorrectos, sino que se observa una mayor complejidad en el descifrado. Las pruebas se realizaron con diferentes claves en cifrado y descifrado, el análisis estadístico entre la imagen cifrada y descifrada mostró una dispersión similar a la imagen. El coeficiente de entropía para la imagen de LENA cifrada con la clave "2b7e151628aed2a6abf7158809cf4f3**c**"fue 7,99935844 y descifrada con la clave "2b7e151628aed2a6abf7158809cf4f3**d**" fue de 7,99926179, los índices de correlación fueron 0,0127 y 0,0498, por lo que se puede asegurar que su descifrado fue totalmente inadecuado aún con una mínima variación en la calve, confirmando que la llave de cifrado es un elemento fundamental en la seguridad del cifrado de imágenes.

Análisis Estadístico de Resultados

La calidad de las imágenes de prueba encriptadas, se analiza mediante tres herramientas estadísticas: histogramas, correlación de los píxeles cercanos y entropía del conjunto de píxeles que componen la imagen.

Histogramas

Los histogramas son una representación estadística que indica la proporción de píxeles para cada tonalidad en una imagen. El histograma de una imagen digital es una función discreta $h(r_k) = n_k$, donde r_k es el nivel de frecuencia del elemento k; en una imagen en escala de grises r_k es la frecuencia del k-ésimo nivel de gris. Al dividir el número total de píxeles de la imagen n, la probabilidad P de ocurrencia k se obtiene con la Ecuación 5:

$$P(r_k) = (\frac{n_k}{n}) \tag{5}$$

La suma total de los componentes en el histograma es igual a 1 [13], que es la suma de las probabilidades de todos los elementos k. En un gráfico de histograma, el eje de abscisas es el valor de $h(r_k)$ entre 0 y 255, mientras que las ordenadas corresponden al nivel de intensidad de la tonalidad n_k, dado por la Ecuación 6. El tamaño de la imagen en píxeles se calcula con la Ecuación 7.

$$h(r_k) = n_k \tag{6}$$

$$longh = k_x \text{ x } m_y \tag{7}$$

Las Ecs. (8), (9) y (10) se obtienen considerando que cada píxel tiene su componente en cada color.

$$h(r_{kR}) = n_{kR}\, Red \tag{8}$$

$$h(r_{kB}) = n_{kB}\, Blue \tag{9}$$

$$h(r_{kG}) = n_{kG}\, Green \tag{10}$$

La Figura 8 muestra las imágenes originales y encriptadas de Baboon y Lena, respectivamente. Cada figura incluye los histogramas correspondientes a cada color básico en RGB, antes y después del cifrado. Como se puede observar en el histograma de las imágenes cifradas, existe una variación mínima entre los valores n_k y de la función $h(r_k)$ para cada color básico que se confunden entre sí, indicando que la probabilidad es igual o casi igual para cada elemento de color.

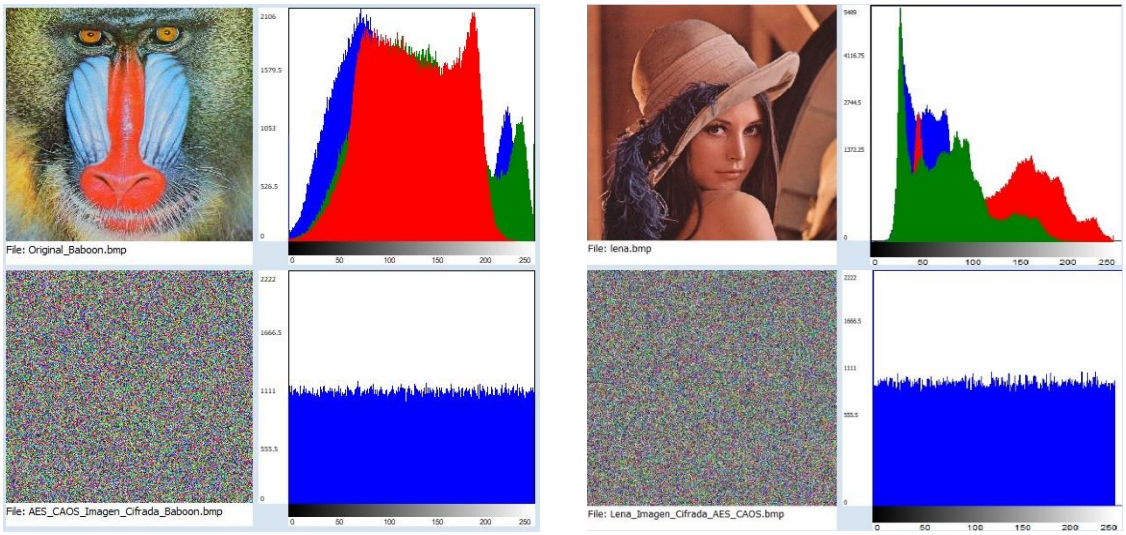


Fig.8 Histogramas de las imágenes encriptadas de Baboon y Lena

Si una imagen cifrada genera un histograma que está organizado de manera uniforme, resistirá todas las formas de ataques estadísticos ya que la frecuencia de ocurrencia de los valores de la imagen encriptada es casi la misma según la Ecuación 5.

Medición de la entropía

Con la entropía de Shannon concebida [27] se obtiene la medida matemática de la información o la incertidumbre, y se calcula en función de la distribución de probabilidad [28]. Suponga que existe una variable aleatoria discreta *x* que toma valores de un conjunto finito *X* de acuerdo con una distribución de probabilidad específica. ¿Cuál es la información obtenida por los resultados de un experimento que se realiza de acuerdo con esta distribución? De manera equivalente, si el experimento (todavía) no se llevó a cabo, ¿cuál es la incertidumbre sobre el resultado? Esa incertidumbre es la entropía de *x*, denotada por *H(x).* Sea x_i uno de los elementos que aparecen en la imagen, con un valor en el rango de 0 a 256, la probabilidad de que aparezca alguno de los elementos es 1/256 Ecs. (11), (12), pero si este elemento aparece dos veces será 2/256. En general, es:

$$\text{Probabilidad X(i)} = \frac{\text{casos probables de X (i)}}{\text{Total de casos X}} \tag{11}$$

Entonces tenemos:

$$P(Xi) = \frac{FrecX(i)}{FecTot\ X} \tag{12}$$

La frecuencia de ocurrencia de cada elemento X_i se obtiene y se divide entre el total de elementos de *X*. La suma de las probabilidades multiplicada por el logaritmo base 2 de las probabilidades de *X(i)* es el cálculo de la entropía, dada por la Ecuación (13) [27]:

$$H(X) = -\sum_{i=0}^{256-1} p(x_i) log_2\ p(x_i) \quad (13)$$

Para un algoritmo ideal, se debe tener la capacidad de hacer que la imagen cifrada sea completamente aleatoria y que la entropía de la información esté cerca del valor teórico 8 [27]. En la Tabla 5 aparecen los resultados de entropía obtenidos de algunas de las imágenes más usadas en la literatura y cifradas con el algoritmo propuesto en el presente trabajo y los obtenidos por otros desarrollos recientes.

Tabla 5. Resultados comparativos de entropía

IMAGEN	AES-CAOS	[9]*	[24]*	[25]*	[26]*
LENA	7,99935844	7,997158	7,9980	7,9974	7,99986
BABOON	7,99930466	7,999330	7,9990	n/d	7,99884
PEPPERS	7,99929357	n/d	n/d	7,9972	7,99963

* Corresponde al número de la Referencia

Coeficiente de Correlación

La correlación permite conocer el grado de relación entre las variables, para determinar qué tan bien una ecuación describe o explica la relación entre las variables [28]. La correlación depende del grado de variación conjunta de dos variables aleatorias. Este es el grado de dependencia de ambas variables llamado covarianza en estadística y viene dado por la Ecuación 14.

$$S_{xy} = \frac{\sum_{i=1}^{N} x_i y_i}{N} - \bar{x}\bar{y} \quad (14)$$

Donde *N* es el total de elementos, y las desviaciones estándar indican el grado de dispersión de los datos con respecto al valor promedio de cada variable de *x* e *y*; es decir, la variación esperada con respecto a la media aritmética, que viene dada por las ecuaciones 15 y 16:

$$\sigma_x = \sqrt{\frac{\sum_{i=0}^{N} x_i^2}{N} - \bar{x}^2} \quad (15)$$

$$\sigma_y = \sqrt{\frac{\sum_{i=0}^{N} y_i^2}{N} - \bar{y}^2} \quad (16)$$

La relación entre cada píxel adyacente de la imagen original es cercana a uno, mientras que en la imagen codificada debería tender a cero. El análisis de esta relación entre dos variables mide una propiedad denominada correlación [28], que es una función estadística aplicable en muchos campos. En este caso se utiliza para la relación entre los valores de los tres colores básicos que componen dos píxeles adyacentes. El valor del índice de correlación varía en el intervalo [-1,1]: Si r = 1, hay una correlación positiva perfecta. El índice indica una dependencia total entre las dos variables llamada relación directa: cuando una de ellas aumenta, la otra también lo hace en proporción constante. Si 0 <r <1, existe una correlación positiva [28]. Si r = 0, no existe una relación lineal, pero esto no implica necesariamente que las variables sean independientes: aún puede haber relaciones no lineales entre ellas.

Si -1 <r <0, existe una correlación negativa. Si r = -1, hay una correlación negativa perfecta. El índice indica una dependencia total entre las dos variables llamada relación inversa: cuando una de ellas aumenta, la otra disminuye en proporción constante. Para implementar el coeficiente de

correlación en las imágenes originales (IO), cifradas (IC) y descifradas (ID), se aplicó la función del lenguaje de programación C ++ srand (tiempo (0)) para generar un número aleatorio a partir de una semilla de tiempo. El rango a partir del cual se seleccionan estos números aleatorios es el ancho y el alto de la imagen, por lo que se eligen 1000 pares de píxeles adyacentes (x, y) de las imágenes IO, IC e ID en la dirección diagonal (x + 1, y + 1). El código C ++ correspondiente es el siguiente:

```
srand( time( 0 ) );
 for(i = 0; i < 1000; i++)
  {
  Xa[i] = rand() % (widthImgO-3);
  Ya[i] = rand() % (heightImgO-1); .....
```

En la Figura 9, en la parte de abajo izquierda y derecha, se observan las gráficas de los píxeles seleccionados al azar para la IO de la imagen original y descifrada. Los puntos trazados se concentran en la diagonal del espacio gráfico. En el caso de la imagen encriptada (centro abajo de la imagen encriptada), no existe relación en los pares de píxeles aleatorios y por lo tanto se observa dispersión, coincidentemente con un valor de correlación más cercano a cero. En la imagen recuperada o descifrada, la parte de abajo derecha de la imagen muestra una gráfica con la concentración de puntos en la parte diagonal del cuadrado del espacio gráfico. Entonces, se puede decir que es prácticamente idéntico al de la imagen original.

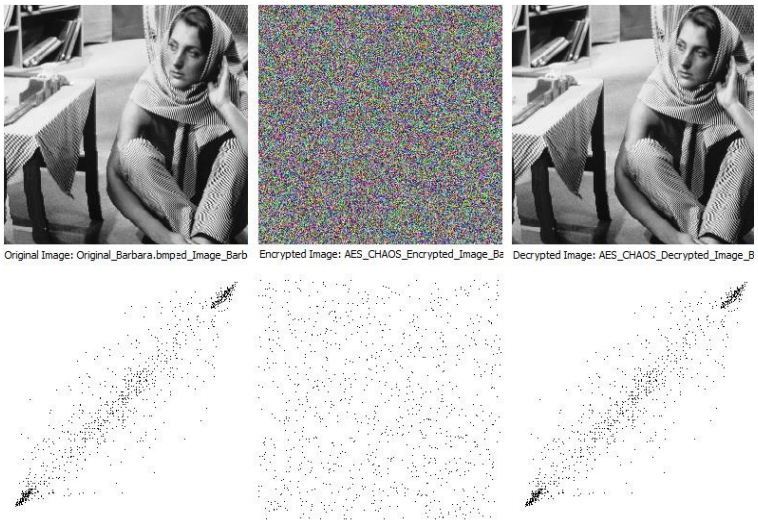


Fig.9 Arriba: Imagen original (lado izquierdo), cifrada con AES-CAOS (centro) y descifrada (lado derecho)
Abajo: gráficas de correlación correspondiente

Como se puede observar, los resultados de las gráficas de los píxeles aleatorios seleccionados corresponden a la base teórica expuesta en el punto anterior. En la Figura 9, se presenta la imagen original, cifrada y descifrada en la parte superior, con las gráficas de los puntos correspondientes de los valores del índice de correlación de cada imagen y los cálculos del Coeficiente de Correlación en la parte inferior. En la Tabla 4 aparecen los resultados obtenidos de las correlaciones de las imágenes de prueba con el presente desarrollo, en donde comparados con los obtenidos con AES de la Tabla 3 se observan mejores resultados por lo que se advierte el fortalecimiento de AES con la presente propuesta.

4. Conclusiones

Los sistemas caóticos introducen propiedades de difusión y confusión en estándares criptográficos como AES. La ecuación logística con parámetros en su órbita caótica y la permutación JV fortaleció con tres unidades de entropía el estándar internacional AES en el cifrado de imágenes. Al cifrar con AES-CAOS se eliminaron los patrones que se presentan al cifrar con AES en Imágenes con grupos repetitivos y de bajo nivel de profundidad. Un mínimo cambio en la clave AES-CAOS no solo será inapropiado, sino que producirá resultados con mayor entropía que el cifrado original. Un ataque de fuerza bruta para encontrar la clave es inviable con espacios de clave de 2^{128}. El cifrado de AES-CAOS de 128 bits, considerando los ordenadores más rápidos, es suficiente para satisfacer las necesidades de al menos 10 años.

Referencias

1. Sun X., Yang J., Sun M., Wang K., *A Benchmark for Automatic Visual Classification of Clinical Skin Disease Images*. Lecture Notes in Computer Science, 2016. **9910**: p. 206-222. DOI: https://doi.org/10.1007/978-3-319-46466-4.
2. Rahmawati E., Listyasari, M., Aziz, A.S., Sukaridhoto, S., Damastuti, F.A., Bachtiar, M.M., Sudarsono, A., *Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone*. International Electronics Symposium on Engineering Technology and Applications (IES-ETA), 2017. p. 234-238. DOI: https://doi.org/10.1109/elecsym.2017.8240409.
3. Monoth T., *Tamperproof Transmission of Fingerprints Using Visual Cryptography Schemes*. Procedia Computer Science, 2010. **2**: p. 143-148. DOI: https://dx.doi.org/10.1016/j.procs.2010.11.018.
4. Anil K., Jain, K.N., Arun, R., *50 years of biometric research: Accomplishments, challenges, and opportunities*. Pattern Recognition Letters, 2016. **79**: p. 80-105. DOI: https://doi.org/10.1016/j.patrec.2015.12.013.
5. Zia, B., Jarosław, W., Tabasam, R., Sohail, Z., Wojciech, S., *Chaotic Dynamical State Variables Selection Procedure Based Image Encryption Scheme*. Symmetry MDPI, 2017. DOI: https://doi.org/10.3390/sym9120312.
6. Artiles, J.A.P., Chaves, D.P.B., Pimentel, C., *Image encryption using block cipher and chaotic sequences*. Signal Processing: Image Communication, 2019. **79**: p. 24-31. DOI: https://doi.org/10.1016/j.image.2019.08.014.
7. Çavuşoğlu, Ü., Kaçar, S., Zengin, A., Pehlivan, I., *A novel hybrid encryption algorithm based on chaos and S-AES algorithm*. Journal Nonlinear Dynamics, 2018. DOI: https://doi.org/10.1007/s11071-018-4159-4.
8. Wenhao, L., Kehui, S., Congxu, Z., *A fast image encryption algorithm based on chaotic map*. Optics and Lasers in Engineering, 2016. **84**: p. 26-36. DOI: https://doi.org/10.1016/j.optlaseng.2016.03.019.
9. Guodong, Y., Xiaoling, H., *An efficient symmetric image encryption algorithm based on an intertwining logistic map*. Neurocomputing, 2017. **251**: 45-53. DOI: https://doi.org/10.1016/j.neucom.2017.04.016.
10. Puneet, K., Shashi, B., *Development of modified AES algorithm for data security*. Optik Elsiever Journal, 2016. **127**(4): p. 2341-2345. DOI: https://doi.org/10.1016/j.ijleo.2015.11.188.
11. Patel, S., Bharath, K.P., Rajesh, K.M., *Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique*. Multimed Tools Appl, 2020. **79**: p. 31739-31757. DOI: https://doi.org/10.1007/s11042-020-09551-9.
12. Schneier, B., *Applied Cryptography*, 1996. John Wiley & Sons. ISBN 978-1-119-09672-6.
13. Gonzalez, R.C., Woods, R.E., *Digital Image Processing*. 2nd Edition, 2002. Prentice Hall: New Jersey. ISBN: 978-0-201-18075-8.

14. Ferguson, N., Schneier, B., Kohno, T., *Cryptography Engineering: Design Principles and Practical Applications*, 2010. Wiley Publishing. ISBN: 978-0-470-47424-2. DOI: https://doi.org/10.1002/9781118722367.
15. Silva-García, V.M., Flores, C.R., *Images encryption using AES and variable permutations*, 2014, Cornell University Library. DOI: https://arxiv.org/abs/1409.5491v1.
16. Silva-García, V.M., *Algorithm for Strengthening Some Cryptographic Systems*. Applied Mathematical Sciences, 2010. **4**(20): p. 967-976.
17. Dworkin, M., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E., Dray, J., *Advanced Encryption Standard (AES)*, 2001. Federal Inf. Process. Stds. (NIST FIPS). National Institute of Standards and Technology: Gaithersburg. DOI: https://doi.org/10.6028/NIST.FIPS.197.
18. Messier, M., Viega, J., *Secure Programming Cookbook for C and C++*, 2003. O'Reilly Media, Inc. ISBN: 978-0-596-00394-4.
19. Dworkin, M., NIST Special Publication 800-38A. *Recommendation for Block Cipher Modes of Operation*, 2001. National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-38A.
20. Stallings, W., *Cryptography and Network Security: Principles and Practice*. 7th Edition, 2017. Pearson Education Limited. ISBN 978-0-13-444428-4.
21. Mellodge, P., *A Practical Approach to Dynamical Systems for Engineers*, 2015. Woodhead Publishing. ISBN: 978-0-081-00202-5. DOI: https://doi.org/10.1016/B978-0-08-100202-5.00004-8.
22. Strogatz, S.H., *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry and Engineering*, 2000. Addison-Wesley Publishing Company. ISBN: 0-201-54344-3.
23. Ibrahim, Y., Fahmi, K., Mohamed, A., *Mohamed, A.S., A New Image Encryption Scheme Based on Hybrid Chaotic Maps*. Complexity, 2020. **2020**: 9597619. DOI: https://doi.org/10.1155/2020/9597619.
24. Sneha, P.S., Sankar, S., Kumar, A.S., *A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps*. J Ambient Intell Human Comput, 2020. **11**: p. 1289-1308. DOI: https://doi.org/10.1007/s12652-019-01385-0.
25. Arab, A., Javad R., Mohammad, G.B., *An image encryption method based on chaos system and AES algorithm*. The Journal of Supercomputing, 2019. DOI: https://doi.org/10.1007/s11227-019-02878-7.
26. Laiphrakpam, D., Khumanthem, M.S., *Image Encryption using Elliptic Curve Cryptography*. Procedia Computer Science, 2015. **54**: p. 472-481.
27. Moatsum, A., Azman, S., Je, S.T., Rami, S.A., *A new hybrid digital chaotic system with applications in image encryption*. Signal Processing, 2019. **160**: p. 45-58. DOI: https://doi.org/10.1016/j.sigpro.2019.02.016.
28. Murray, R., Spiegel, L.J., *Estadística*. 4ta. Ed., 2008. Shaum. ISBN: 978-970-10-6887-8.
29. Debabrata S., Goutam S., *Classification of SAR Images Based on Entropy*, I.J. Information Technology and Computer Science, 2012. DOI: https://doi.org/10.5815/ijitcs.2012.12.09

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional, la Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME), al Centro de Innovación y Desarrollo Tecnológico en Cómputo (CIDETEC) y a la Secretaría Académica del Instituto Politécnico Nacional, por su apoyo.

Conflicto de Intereses

No hay conflictos de intereses.

Contribución de los autores

Ernesto Godínez-Rodríguez. ORCID: https://orcid.org/0000-0002-4508-3351
Desarrolla la investigación y redacta el manuscrito.

Miguel Patiño Ortiz. ORCID: https://orcid.org/0000-0002-5630-8077
Administración, supervisión, validación, redacción y edición del artículo de investigación.

Alexander Balankin. ORCID: https://orcid.org/0000-0001-7357-2948
Investigación en la teoría de sistemas dinámicos caóticos y el índice Lyapunov.

Rolando Flores Carapia. ORCID: https://orcid.org/0000-0002-8557-9941
Conceptualización del proyecto de investigación e implementación en software de las metodologías de AES, entropía, histogramas y correlación.

Julián Patiño Ortiz. ORCID: https://orcid.org/0000-0001-8106-9293
Administración y supervisión del proyecto de investigación.

Víctor Manuel Silva García. ORCID: https://orcid.org/0000-0003-1312-5294
Conceptualización general y las metodologías utilizadas de AES y Permutación JV.

Miguel A. Martínez Cruz. ORCID: https://orcid.org/0000-0002-4431-9262
Validación de los valores de los números pseudoaleatorios con parámetros caóticos de la ecuación logística.