IDEAS EN CIENCIAS DE LA INGENIERÍA

Cifrado de imágenes con análisis de fluctuaciones sin tendencia

Image encryption with non-trend fluctuation analysis

E. Jiménez-López[1] *
(*ejimenezl@uaemex.mx)

Recibido: 25 de febrero de 2026 Aceptado: 18 de abril de 2026

Resumen

En este trabajo, se realizó una extensión del método de Análisis de Fluctuación sin Tendencia que describe las propiedades de escala de imágenes con diferentes contrastes que presentan cualidades no lineales. En este documento, se establecieron las propiedades de escala en imágenes cifradas utilizando un método de análisis sin fluctuaciones sin tendencia bidimensional. Se realizó el cifrado de la imagen usando un sistema criptográfico que utiliza como principal insumo los autómatas celulares con la regla 182, contrastando los resultados con su versión original y el sistema estándar de cifrado avanzado. La conducta de las imágenes cifradas fue constante, similar al ruido 1/f, según indican los resultados numéricos.

Palabras clave: *Cifrado, Imagen, Análisis de Fluctuaciones sin Tendencia*

Abstract

In this work, an extension of the Detrended Fluctuation Analysis method is performed, which describes the scaling properties of images with different contrasts exhibiting non-linear qualities. In this paper, we establish the scaling properties in encrypted images using a two-dimensional detrended fluctuation analysis method. We perform image encryption using a cryptographic system that uses cellular automata with rule 182 as its main input. We contrast the results with their original version and the standard Advanced Encryption Standard system. The behavior of the encrypted images is constant, similar to 1/f noise, as indicated by the numerical results.

Keywords: *Encryption, Image, Non-Trend Fluctuation Analysis*

[1] Universidad Autónoma del Estado de México (UAEMEX), Centro de Investigación y Estudios Avanzados de la Población (CIEAP).

INTRODUCCIÓN

Hoy en día, existe una amplia variedad de métodos para analizar o identificar el comportamiento fractal o singular que puede aparecer en distintas formas de información [1]. El análisis de fluctuación sin tendencia ($AFsT$), tiene el objetivo de extraer características significativas de señales de alta dimensión, como las imágenes [2]. El cifrado de imágenes digitales es un tema importante, ya que existen muchas aplicaciones que requieren proteger diferentes tipos de información [3].

Existen numerosos métodos de cifrado de imágenes, es crucial que se pueda determinar algún tipo de calidad del contenido de la imagen encriptada. Este trabajo, tiene como objetivo final proponer y validar el exponente de escala (α) derivado del Análisis de Fluctuación sin Tendencia ($AFsT$) bidimensional como una métrica objetiva y complementaria para evaluar la calidad y la confidencialidad de los sistemas de cifrado de imágenes. Si bien el $AFsT$ bidimensional es una técnica establecida para el análisis de texturas y propiedades fractales en imágenes, su aplicación sistemática y la interpretación de sus resultados como indicador de la efectividad del cifrado constituyen la principal novedad de esta investigación.

Específicamente, se adaptó y aplicó el $AFsT$ bidimensional para caracterizar las propiedades de escalado en imágenes cifradas, demostrando cómo este exponente puede revelar la conducta única de las imágenes tras el proceso de cifrado. Se contrastó esta metodología con algoritmos de cifrado existentes, como el sistema basado en autómatas celulares (regla 182) y el Estándar de Cifrado Avanzado, para evaluar su robustez y calidad.

Estos métodos, para detectar correlaciones de largo alcance y propiedades multifractales, son herramientas muy útiles en el campo del análisis de imágenes, ya que se han aplicado para investigar características en algunas imágenes médicas [4, 5], para extraer características de textura [6, 7], para identificar regiones donde se observen afectaciones en los cultivos [8, 9]. El rendimiento de los métodos basados en técnicas fractales o multifractales es superior a otros métodos, debido a las características isotrópicas que presentan una gran cantidad de imágenes naturales y artificiales [10].

El cifrado de imágenes digitales es un tema importante, ya que existen muchas aplicaciones que requieren proteger diferentes tipos de información, como los sistemas de comunicación militares, imágenes médicas, de vigilancia, entre otros [11]. Existen numerosos métodos de cifrado de imágenes, es crucial que se pueda determinar algún tipo de calidad del contenido de la imagen cifrada. En este sentido, se consideró aplicar a las imágenes cifradas un algoritmo basado en $AFsT$ bidimensional, después del cifrado los píxeles de la imagen tienden a tener características isotrópicas o un comportamiento aleatorio. El exponente de Hurst fue considerado como un indicador efectivo para los sistemas de cifrado, se detectó la presencia de un mensaje en un portador caótico con una señal incrustada [12]. Para lograr la seguridad multimedia, algunos autores sugieren utilizar el cifrado selectivo [13]. Empleando

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

diferentes herramientas, se aporta que el cifrado de cuatro bit-planos es suficiente para proporcionar una alta confidencialidad [14].

La organización de este trabajo es la siguiente. El sistema de cifrado que se basa en un enfoque matricial se expone en la Sección 2. La Sección 3 expone el método de análisis de fluctuaciones sin tendencia bidimensionales. La Sección 4 muestra los resultados que se lograron al utilizar este mismo método sobre las imágenes cifradas. Además, se analizaron las imágenes cuando se considera solo un cifrado parcial. Por último, las conclusiones se presentan en la Sección 5.

Modelo del Sistema de Cifrado

Se utilizó un criptosistema que comprende los conjuntos M, C y X son términos binarios de longitud N, Z_2^N, en el que $Z_2 = \{0, 1\}$ y dos familias indexadas fijas de permutaciones, $\Psi = \{\psi_x : x \in X\}$ y $\Phi = \{\phi_x : x \in X\}$. Las palabras M y C se denominan textos planos y textos cifrados, mientras que los términos en el conjunto de índices X son claves de cifrado. Además, las funciones $\psi_x : M \to C$ y $\phi_x : C \to M$ se denominan funciones de cifrado y descifrado. El criptosistema convierte una serie de texto plano m en una secuencia de texto cifrado c, para cada $x \in X$ uno tiene $c = \psi_x(m)$, para revelar la secuencia de bloques cifrados, se utiliza funciones de descifrado ϕ_x, es decir, $m = \phi_x(\psi_x(m))$.

El flujo de cifrado completo es confidencial y la misma clave se emplea para cifrar y descifrar. El criptosistema se basa en el esquema de sincronización de Autómatas Celulares (AC), donde se desenvuelve con la regla 182, ha sido utilizada para crear los dos modelos de permutaciones y el generador de números pseudoaleatorios asintóticamente adecuado [15]. El fenómeno de sincronización en el acoplamiento de sistemas de AC se describe en detalle en las siguientes referencias [16, 17]. Se descubrió que dos AC acoplados se sincronizan si hay un bloque de $(2n - 1)$ sitios desacoplados entre cada par de coordenadas sucesivas, donde n es un entero positivo mayor que 1. Este método de cifrado, el cual se fundamenta en la sincronización de AC, recibe el nombre en español de $ESAC$.

Con el fin de tener una forma inteligible del texto plano m se divide en bloques, $m = \{m_1, m_2, \ldots\}$. Cada uno de estos bloques m_k, tiene una longitud de N bits. El subíndice k simplemente indexa estos bloques secuencialmente, aplicamos la Ec. (1).

$$\begin{pmatrix} \widehat{m}_k \\ y_{k+1} \end{pmatrix} = U \begin{pmatrix} m_k \\ y_k \end{pmatrix} \text{ mód } 2, \quad \text{con} \quad U = \begin{pmatrix} J_N \\ b \end{pmatrix}, \quad k = 1, 2, \ldots \tag{1}$$

En muchos sistemas de criptografía o procesamiento de señales, existe un “estado” interno que se actualiza en cada paso. Aquí, y_k parece ser un vector que representa el estado del sistema en el momento en que se procesa el bloque m_k. El bloque de texto plano m_k se utiliza para calcular el siguiente estado y_{k+1} y el bloque cifrado $\widehat{m}_k$. J_N representa una matriz $N \times (2N + 1)$; el subíndice N en J_N se refiere

a la dimensión principal de esta matriz, que está relacionada con la longitud de los bloques de texto plano (N bits). Inicialmente a partir de dos vectores de $(2N+1)$ elementos, $f = [f_1, 0, \ldots, f_{N+2}, \ldots, 0]$ y $g = [0, g_2, 0, \ldots, g_{N+1}, 0, g_{N+3}, \ldots, 0]$, donde los componentes $f_1, f_{N+2}, g_2, g_{N+1}$ y g_{N+3} tienen un valor de 1. Estas son las dos primeras filas de la matriz J_N, las otras $(N-2)$ filas se generan aplicando una operación de adición módulo 2 de las dos filas precedentes, con condiciones de contorno fijas de cero al lado izquierdo seguido por los componentes de la fila anterior movidos hacia la derecha una posición.

La matriz U se define como una concatenación de J_N y b. El texto indica que U es una matriz $N \times (2N+1)$. Dada la estructura de la ecuación principal, donde U opera sobre un vector de la forma $\begin{pmatrix} m_k \\ y_k \end{pmatrix}$, es probable que b sea un vector o una matriz que, junto con J_N, complete las dimensiones necesarias para la multiplicación matricial. El vector fila b tiene $(2N+1)$ elementos con un valor de 1 en su primera entrada y 0 en caso contrario, $b = [1, 0, \ldots, 0]$. Lo principal para calcular la secuencia $\widehat{m}_1$ de N bits, requerimos el producto de la matriz cuadrada U con un vector columna que concatena la secuencia de texto plano $m_1 = \{m_1, m_2, m_3, \ldots, m_N\}$ y una secuencia binaria aleatoria $y_1 = \{y_1, y_2, y_3, \ldots, y_{N+1}\}$ de $(N+1)$ bits. Si U opera sobre $\begin{pmatrix} m_k \\ y_k \end{pmatrix}$, tiene una dimensión de $(N + \dim(y_k))$, entonces la dimensión de la columna de U debe coincidir.

Para calcular $\widehat{m}_2$ por medio de la Ec. (1), se requiere nuevamente dos secuencias, una secuencia de texto sin formato que puede ser alterada m_2, una secuencia binaria aleatoria y_2. La última secuencia comprende la secuencia m_1, que se convierte en los bits iniciales de la nueva y_2 y el primer bit de la y_1 anterior, que se convierte en el último bit de esta secuencia. Para las siguientes secuencias, el mismo procedimiento se itera repetidamente. Nótese que la matriz superior J_N hace inexplícito el texto plano, mientras que la matriz inferior $[J_N\ ;\ b]$ ayuda a calcular una nueva secuencia pseudoaleatoria binaria y_k, para $k \geq 2$.

Para continuar con el proceso de cifrado, se requieren dos matrices, P_N y Q_N, como se muestra en la Ec. (2) tales que

$$c_k = \Psi_k(m_k) = \left[(\widehat{P} \times x) + (\widehat{Q} \times \widehat{m}_k)\right] mod 2, \quad k \geq 1, \tag{2}$$

Similar a m_k, el subíndice k indica que c_k es el resultado del cifrado aplicado al bloque m_k (o a alguna transformación de este) en la iteración k. El uso de Ψ_k sugiere que la operación de cifrado podría ser dinámica o parametrizada por k, lo que implica que las matrices o parámetros utilizados en la función podrían cambiar en cada paso. Este es el bloque de entrada original que se está cifrando en la iteración k, ya se definió en la explicación anterior como parte de la secuencia $m = \{m_1, m_2, \ldots\}$. La suma dentro

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

del módulo 2 es el resultado del cifrado de la iteración anterior, o una versión transformada del bloque de texto plano original. Indica que el proceso de cifrado descrito por esta ecuación comienza en la primera iteración $(k = 1)$ y continúa para todas las iteraciones subsiguientes.

La dimensión L de los vectores c_k y $\widehat{m}_k$ está determinada por 2^l. El subíndice l toma valores enteros positivos, lo que significa que L puede tomar valores como $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, etc. Esto implica que la longitud de los bloques cifrados y de entrada puede variar según el valor de l. La dimensión N de los vectores c_k y $\widehat{m}_k$ (y también de la matriz $\widehat{P}$) se define como $2n - 1$. El subíndice n toma valores enteros positivos, lo que significa que N puede tomar valores como $2^1 - 1 = 1$, $2^2 - 1 = 3$, $2^3 - 1 = 7$, etc. Es importante notar la condición $n > l$, lo que significa que la dimensión N está relacionada, pero es mayor que la dimensión L. La matriz $\widehat{P}$ se construye a partir de un vector $p = [p_1, p_1, \ldots, p_N]$. Este vector p tiene elementos que son 1 en posiciones específicas j y 0 en otros casos. La fórmula $j = (2^n + 1) - 2^{i+1}$ define estas posiciones 1 para $i = 0, 1, 2, \ldots, (n - 1)$. El subíndice j aquí denota la posición dentro del vector p. El rango de i (de 0 a $n - 1$) indica cuántos elementos 1 se colocarán en el vector p, y la fórmula para j determina sus ubicaciones exactas.

Las $(L - 1)$ filas se crean mediante el desplazamiento de una posición de la fila anterior hacia la derecha, comenzando con un cero. Q es una matriz triangular inferior de orden L, que puede generarse en primer lugar, desde el vector $a = [a_1,\ 0,\ \ldots,\ 0]$, donde el componente a_1 tiene un valor de 1. La primera fila de la matriz está constituida por el vector más reciente Q, las $(L - 1)$ filas se generan aplicando la regla de AC 182 de la fila anterior con condiciones de borde fijas de cero en la parte izquierda y a la derecha. Dado que el proceso de descifrado es similar al procedimiento de cifrado se puede observar el diagrama de bloques en la Figura 1.

La Figura 1 muestra el Diagrama de Flujo del Proceso del modelo de cifrado; la imagen proporciona la entrada. El mensaje original m se procesa junto con la llave z a través de la función $H_{N_t}(z,\ m)$, generando una salida intermedia. Paralelamente, se generan claves o estados U_K y U_{k+1} utilizando las funciones $H_{N_t}(x)/H_{N_b}(y)$, que dependen de las variables intermedias x e y.

En el Cifrado (E): las señales intermedias x (proveniente de la generación de claves) y $\widehat{m}$ (que es una versión inicial o modificada del mensaje original) se combinan mediante operaciones matriciales: $(\widehat{P} \times x) + (\widehat{Q} \times \widehat{m})$. La salida de esta operación es el mensaje cifrado $\widehat{c}$. Al transmitir el mensaje cifrado se envía a través del "Canal de Comunicación". Este canal puede alterar los datos.

Para el descifrado (D): el bloque recibe el mensaje cifrado $\widehat{c}$ (posiblemente alterado por el canal de comunicación) y la señal x (generada de manera similar al cifrado). Se aplican operaciones inversas a las de cifrado: $(\widehat{R} \times x) + (\widehat{T} \times \widehat{c})$. La salida de este bloque es el mensaje recuperado $\widehat{m}$.

La Salida Final que es el mensaje recuperado $\widehat{m}$ se procesa junto con la nueva llave z a través de la

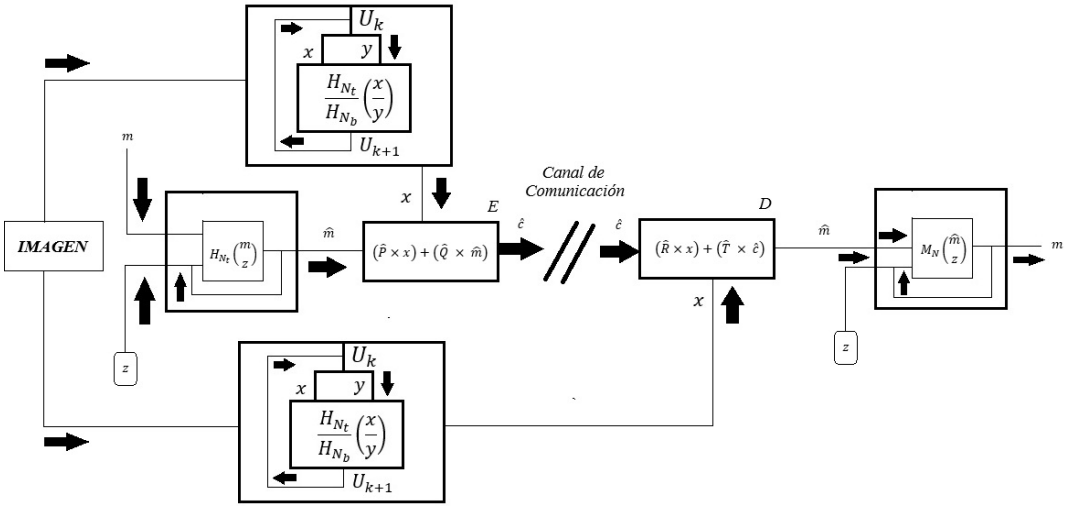

FIGURA 1. *Diagrama de Flujo del modelo de cifrado con sus componentes principales: las familias de permutaciones Ψ que están indexadas y el generador pseudoaleatorio de claves Φ. Fuente: Elaboración propia.*

función $M_N(\widehat{m},\ z)$. La salida final de este proceso es el mensaje original m. Para cada valor de píxel se convierte a su valor correspondiente de 8 bits, $[b_8 \cdots b_1]$, donde el bit más significativo es b_8 y el menos significativo es b_1.

Para finalizar esta explicación, el diagrama de flujo describe un esquema de cifrado y descifrado que utiliza funciones de hash, permutaciones y generación de llaves para asegurar la comunicación. El proceso de cifrado transforma el mensaje original usando llaves y operaciones matemáticas, el descifrado realiza las operaciones inversas para recuperar el mensaje original, asumiendo que las llaves correctas y las funciones de transformación son conocidas.

MÉTODO

Se utilizaron nueve imágenes en escala de grises. Tres de ellas tienen dimensiones de 1024 x 1024 píxeles y las demás de 512 x 512 píxeles. La Figura 2 presenta estas imágenes. Se eligieron porque son muy utilizadas como imágenes de referencia estándar en el campo del tratamiento de imágenes. Este estudio empleó Matlab (MathWorks, Natick, MA) como plataforma computacional para el análisis y modelado de datos. Todas las simulaciones y cálculos numéricos fueron implementados en este entorno, aprovechando sus capacidades para el procesamiento de señales y la resolución de ecuaciones complejas. La elección de Matlab se fundamentó en su amplia disponibilidad de herramientas especializadas y su validada precisión en la ejecución de algoritmos matemáticos. Los resultados obtenidos se basan íntegramente en las rutinas y funciones proporcionadas por este software. La reproducibilidad de los hallazgos está garantizada mediante la documentación detallada del código utilizado.

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

FIGURA 2. *Matriz de imágenes que se utilizan en este trabajo. Fuente: Elaboración propia.*

Análisis de fluctuación sin tendencia unidimensional

El $AFsT$ es un método para analizar la autosimilitud de una señal. Se utiliza para examinar datos, como intervalos de latidos en el corazón, tendencias del mercado bursátil o actividad sísmica, ofreciendo una visión profunda de la dinámica intrínseca del sistema. El $AFsT$ se utiliza en el análisis de series temporales, especialmente en aquellas que parecen no estacionarias, permitiendo detectar correlaciones de largo alcance al eliminar tendencias que no están relacionadas con las propiedades de correlación de la señal.

El $AFsT$ funciona de la siguiente manera:

1. Sea $\{X_t\}$ la serie temporal de longitud N. El primer paso es determinar la serie integrada Y, donde $Y(i)$ se define como la suma acumulada de las desviaciones de cada punto de la serie temporal respecto a su valor medio $\langle X\rangle$. La Ec. (3) para la serie integrada $Y(i)$ es:

$$Y(i) = \sum_{t=1}^{i} (X_t - \langle X\rangle), \tag{3}$$

   donde $\langle X\rangle$ es el valor medio de la serie temporal $\{X_t\}$.

2. La serie integrada Y se divide en M_s segmentos no superpuestos de igual longitud s, donde $M_s = \lfloor N/s \rfloor$. Dado que N no siempre es un múltiplo entero de s, una práctica común es repetir el mismo procedimiento en la serie temporal invertida, lo que resulta en $2M_s$ segmentos.

3. Para cada segmento ν ($\nu = 1, 2, \ldots, 2M_s$), se calcula la tendencia local $\widehat{Y}_v$ mediante un ajuste de mínimos cuadrados. Esto implica encontrar un polinomio P_v de orden n que mejor se ajuste a los datos de la Ec. (4).

$$\widehat{Y}_v(i) \equiv P_v(i). \tag{4}$$

   Se utilizó un ajuste de mínimos cuadrados de orden lineal ($n = 1$) para eliminar la tendencia local en cada segmento.

4. La varianza $F^2(\nu, s)$ para cada segmento ν se estima como la media de los cuadrados de las diferencias entre la serie integrada Y y la tendencia local $\widehat{Y}_v$. La fórmula para esta estimación se presenta en la Ec. (5):

$$F^2(\nu, s) = \frac{1}{s} \sum_{i=1}^{s} \left\{ Y[(\nu - 1)s + i] - \widehat{Y}_v(i) \right\}^2. \tag{5}$$

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

La Ec. (5) calcula la varianza promediando las diferencias al cuadrado entre los valores de la serie integrada y la tendencia estimada, dentro de un segmento específico. Para los segmentos invertidos, los índices se ajustan en consecuencia para mantener la coherencia del cálculo.

5. La función de fluctuación promedio $F(s)$ se logra al determinar la raíz cuadrada de la media de las varianzas en cada uno de los segmentos $2M_s$, como se muestra en la Ec. (6).

$$F(s) = \left\{ \frac{1}{2M_s} \sum_{v=1}^{2M_s} F^2(\nu, s) \right\}^{1/2} \tag{6}$$

6. Finalmente mostramos el escalamiento; se examina la relación entre $F(s)$ y el tamaño del segmento s. Se espera que $F(s)$ siga una ley de potencia como la mostrada en la Ec. (7).

$$F(s) \sim s^{\alpha}. \tag{7}$$

El exponente de escalamiento α indica el tipo de correlaciones presentes en la serie temporal:

a. $\alpha = 0{,}5$: Indica una serie temporal no correlacionada, como el ruido blanco.

b. $\alpha > 0{,}5$: Indica correlaciones de largo alcance. Cuanto mayor sea α, más fuerte será la correlación.

c. $\alpha < 0{,}5$: Indica correlaciones anti-persistentes.

d. Si al ruido $1/f$ le corresponde $\alpha = 1$ y al movimiento browniano le corresponde $\alpha = 1{,}5$.

El exponente de escalamiento α se estima mediante un ajuste de regresión lineal por mínimos cuadrados sobre la relación logarítmica entre la función de fluctuación $F(s)$ y el tamaño del segmento s (es decir, graficando $\log(F(s))$ vs $\log(s)$). La pendiente de la línea de ajuste óptimo corresponde al valor de α.

Análisis de fluctuación de eliminación de tendencia bidimensional

La imagen I con dimensiones $U \times V$ será tratada como una superficie y será descrita mediante una matriz $X(i,\ j)$, en el que se indica el número de filas y columnas con $i = 1, 2, \ldots, U$ y $j = 1, 2, \ldots, V$. Con el propósito de distinguir la tendencia de las oscilaciones en las imágenes, se utilizó un algoritmo bidimensional que se construyó con los siguientes pasos [17].

1. Divide la superficie $X(i,\ j)$ en ventanas cuadradas que no se superponen $U_s \times V_s$ en tamaño $s \times s$, donde $U_s = \lfloor U/s \rfloor$ y $V_s = \lfloor V/s \rfloor$. Cada ventana puede ser representada por $X_{u,v}$, tal que $X_{u,v}(i,j) = X(i + l_1,\ j + l_2)$ para $1 \leq i, j \leq s$, donde $l_1 = (u-1)s$ y $l_2 = (v-1)s$.

2. Calcula la suma acumulada para cada ventana $X_{u,v}$, situada por u y v, como se muestra en la Ec. (8). Donde $(X_{u,v},\ (k_1, k_2))$ es la media de la subimagen $X_{u,v}$, con $1 \leq i, j \leq s$.

$$P_{u,v}(i,\ j) = \sum_{k_1=1}^{i} \sum_{k_2=1}^{j} \left(X_{u,v}(k_1, k_2) - \langle X_{u,v}(k_1, k_2) \rangle\right) \tag{8}$$

3. Establezca la tendencia de la subimagen adquirida al ajustar el conjunto de datos a un plano $\widehat{P}_{u,v}(i,j) = ai + bj + c$, donde a, b y c son parámetros que se determinan con el método de mínimos cuadrados. Posteriormente, las varianzas locales relacionadas con cada subimagen se calculan $X_{u,v}$, como se muestra en la Ec. (9).

$$F^2(u,\ v,\ s) = \frac{1}{s^2} \sum_{i=1}^{s} \sum_{j=1}^{s} \left[P_{u,v}(i,\ j) - \widehat{P}_{u,v}(i,\ j)\right]^2. \tag{9}$$

4. Promediando sobre todas las subimágenes se obtiene la fluctuación general eliminada de la tendencia como se muestra en la Ec. (10).

$$F^2(s) = \left(\frac{1}{U_s V_s} \sum_{u=1}^{U_s} \sum_{v=1}^{V_s} F^2(u, v, s)^{1/2} \right). \tag{10}$$

Este algoritmo opera sobre una serie de longitudes de segmento, denotadas por s. La elección del rango para s es crucial para capturar las propiedades de escala deseadas. El rango especificado es $6 < s < \text{mín}(U,\ V)/4$, donde U y V son las dimensiones de la superficie pixelada. Al variar s, se investiga cómo las propiedades de la superficie cambian con la escala. El límite inferior de $s > 6$ se establece para evitar artefactos de baja escala y ruido local que podrían distorsionar el análisis de propiedades fractales. El límite superior, $s < \text{mín}(U, V)/4$, asegura que los segmentos analizados sean una fracción representativa de la imagen sin abarcar una porción excesivamente grande que viole las suposiciones de homogeneidad estadística en la escala considerada. Esta elección permite capturar las características de escala relevantes de la imagen.

La función de fluctuación $F_2(s)$ se emplea para cuantificar una propiedad de escala fractal en superficies bidimensionales (pixeladas). Una superficie exhibe escala fractal si sus propiedades estadísticas son invariantes ante cambios de escala. Esto significa que la apariencia o textura de la

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

superficie es similar independientemente de la escala a la que se observe. En superficies fractales, la dependencia de una medida estadística con la escala espacial suele seguir una ley de potencia. En la Ec. (7) el exponente de fluctuación de escala (α) es fundamental para caracterizar la rugosidad o irregularidad de la superficie a diferentes escalas. Un valor más alto de α generalmente indica una superficie más rugosa o irregular, con fluctuaciones más pronunciadas a medida que aumenta la escala.

El exponente de fluctuación de escala α se presenta como una extensión del exponente de Hurst (H), que es comúnmente utilizado para caracterizar la persistencia o memoria de procesos estocásticos (como señales o series temporales). El exponente de Hurst clásico satisface $0 < H < 1$. La relación entre α y H depende de si la señal (o superficie, en este contexto bidimensional) es estacionaria o no estacionaria.

Para señales bidimensionales (superficies pixeladas): si la superficie analizada es estacionaria (sus propiedades estadísticas no cambian con la posición), entonces el exponente de fluctuación de escala es directamente igual al exponente de Hurst. En este caso, la rugosidad de la superficie a diferentes escalas se comporta de manera similar a la persistencia de una señal unidimensional estacionaria. Si la superficie analizada es no estacionaria, la relación cambia ($\alpha = H + 2$). La adición de 2 al exponente de Hurst en el caso no estacionario se relaciona con las dimensiones adicionales (la dimensión espacial $2D$) que influyen en la fluctuación. En esencia, la no estacionariedad introduce una dependencia de escala adicional que se refleja en el valor de α.

El valor de α (por lo tanto de H, bajo ciertas condiciones) proporciona información sobre la naturaleza de la irregularidad de la superficie. Por ejemplo, un α cercano a 0 podría indicar una superficie relativamente lisa, mientras que un α mayor podría sugerir una superficie más rugosa o compleja. La distinción entre estacionario y no estacionario es crucial para interpretar correctamente el significado físico de α. En el contexto del análisis de imágenes, la estacionariedad de una imagen se refiere a si sus propiedades estadísticas (como la distribución de intensidades o la estructura de texturas) son uniformes en toda la imagen. Muchas imágenes del mundo real no son estrictamente estacionarias.

La aplicabilidad de estas relaciones depende de que la superficie o señal analizada realmente exhiba un comportamiento fractal y que las condiciones de estacionariedad (o no estacionariedad) se cumplan. El modelo propuesto utiliza la función de fluctuación $F_2(s)$ para cuantificar la escala fractal de superficies pixeladas mediante el exponente α. Este exponente se relaciona con el exponente de Hurst H de una manera que depende críticamente de la estacionariedad de la superficie, ofreciendo así una métrica para caracterizar su rugosidad y complejidad a través de diferentes escalas [18].

Resultados

Se presentan los resultados obtenidos utilizando el $AFsT$ bidimensional descrito anteriormente. En el análisis, se consideraron todas las nueve imágenes estándar en escala de grises de diferentes formas y

tres procedimientos de cifrado diferentes. Los esquemas del Cifrado por Sincronización de Autómatas Celulares ($CSAC$) es un algoritmo de cifrado simétrico diseñado para dispositivos con restricciones de energía. Se agrega el Estándar de Cifrado Avanzado (ECA), utilizando el modo de operación $CSAC_{v_1}$, $CSAC_{v_2}$ y ECA, respectivamente. Los resultados del desempeño del $AFsT$ bidimensional se observan en la Figura 3, donde se muestra una imagen simple del jugador de futbol en tonos de gris y sus variantes cifradas. Se nota que la función de fluctuación $F_2(s)$ para los tres procedimientos de cifrado en conjunto, muestra un comportamiento y un valor parecidos. Los exponentes de escala de fluctuación α para los conjuntos de datos de imágenes considerados en este artículo se dan en la Tabla 1. Se puede deducir que las imágenes cifradas tienen un comportamiento persistente, que se encuentra cerca del ruido $1/f$, ya que la mayor parte de los exponentes α en las versiones cifradas están próximos a la unidad. Dado que se ve la dimensión fractal como una medida objetiva para calcular la calidad del contenido de la imagen cifrada [19], se puede tomar este último resultado como otra métrica objetiva.

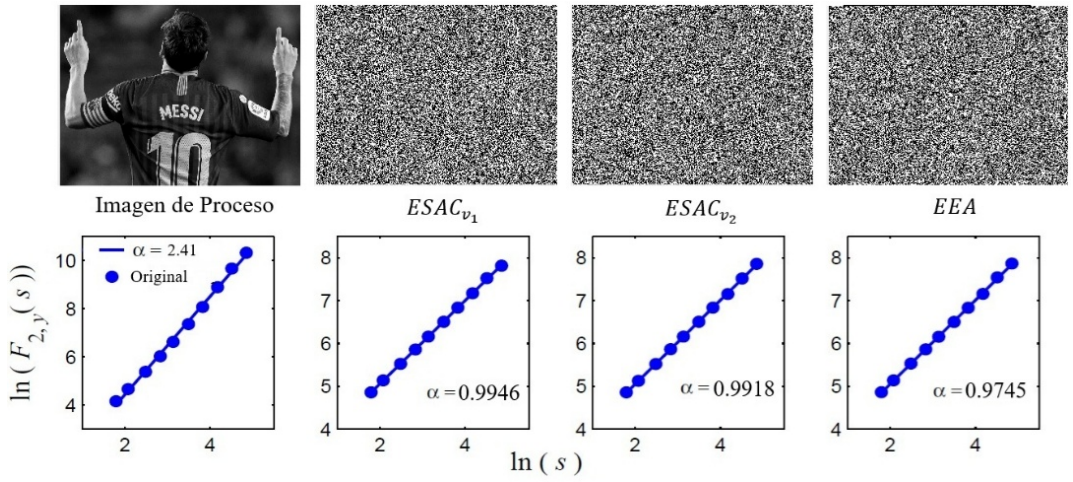

FIGURA 3. *En primera columna están las imágenes de prueba y las versiones de cifrado. En la Segunda columna están los respectivos exponentes de escala-fluctuación proporcionados por la función de fluctuación F_2. Fuente: Elaboración propia.*

Siguiendo las ideas de la referencia [20] para profundizar en la sensibilidad a los píxeles cifrados, se realizó un cifrado parcial de las imágenes, con cuatro bits por cada píxel, y se aplicó el $AFsT$ bidimensional en la imagen cifrada obtenida. En el análisis de cifrado parcial, se consideraron los 4 bits menos significativos (b_1 a b_4) de cada píxel. Se aplicó el cifrado a estos bits y se evaluó la influencia de modificar progresivamente estos bloques de bits en la estimación del exponente α. Los resultados de esta técnica de escalado para las imágenes simples de un jugador de futbol cifradas se presentan en las Figuras 4 a la 6, el resto de los exponentes de escalado de fluctuación α para los conjuntos de datos de imágenes considerados se dan en la Figura 7 que tiene la forma de tablas.

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

Tabla 1. *Índices de los exponentes de escala α, que se lograron al emplear el algoritmo en dos dimensiones de $AFsT$ en las 9 imágenes de prueba y en sus respectivas versiones cifradas. Fuente: Elaboración propia.*

Imagen	$CSAC_{v_1}$	$CSAC_{v_2}$	ECA
Futbolista	0.9946	0.9918	0.9745
Lena	0.9725	0.9705	0.9785
Fotógrafo	0.9954	0.9783	0.9808
Mandril	0.9841	0.9623	0.9787
Circuito	0.9555	0.9701	0.9884
Arroz	0.9772	0.9486	0.9798
Monedas	1.0005	0.9599	0.9723
Medica	0.9953	0.9760	0.9714
Flor	0.9884	0.9830	0.9610

Se realiza un ejemplo claro y aterrizado del modelo propuesto usando $n = 3$ y $n = 4$, enfocándonos en la parte clave: cómo se construye la matriz y cómo se cifra un bloque.

Para $n = 3$, supongamos que tenemos un bloque plano Ec. (11).

$$x = (1, 0, 1) \tag{11}$$

Se construye una matriz tipo triangular con desplazamientos a la derecha y se introducen 0, mostrada en la Ec. (12).

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{12}$$

Es un caso muy simple, pero ayuda a entender el modelo. Ahora se tiene el vector de la forma mostrada en la Ec. (13).

$$r = (0, 1, 1) \tag{13}$$

Se concatenaron los vectores x y r, como lo muestra la Ec. (14).

$$(x, r) = (1, 0, 1, 0, 1, 1) \tag{14}$$

Se aplicó el siguiente procedimiento, Ec. (15), Ec. (16) y Ec. (17):

$$y = A \bullet x \otimes r \tag{15}$$

$$A \bullet x = (1, 0, 1) \tag{16}$$

$$y = (1, 0, 1) \otimes (0, 1, 1) = (1, 1, 0) \tag{17}$$

La Ec. (17) muestra el resultado del cifrado.

Ahora, para $n = 4$ el texto plano se muestra en la Ec. (18).

$$x = (1, 0, 1, 1) \tag{18}$$

La construcción de la matriz para este ejemplo se muestra en la Ec. (19).

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{19}$$

La secuencia aleatoria que se genera en el vector es de la forma como en la Ec. (20).

$$r = (1, 1, 0, 1) \tag{20}$$

Para realizar el cifrado se realizaron las operaciones de las ecuaciones Ec. (21), Ec. (22) y Ec. (23).

$$A \bullet x = (1, 0, 1, 1) \tag{21}$$

$$y = (1, 1, 0, 1) \otimes (1, 1, 0, 1) \tag{22}$$

$$y = (0, 1, 1, 0) \tag{23}$$

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

Donde y es la secuencia cifrada que depende de la estructura matricial y de la secuencia pseudoaleatoria. La operación XOR introduce aleatoriedad. Se debe aclarar que en el modelo la matriz NO es identidad, se genera con autómatas celulares (regla 182) y dinámica iterativa.

Para los sistemas de cifrado $CSAC_{v_1}$ y ECA, los exponentes de escalado de la imagen cifrada se aproximan a los valores de los exponentes de escalado de las imágenes simples a medida que se obtienen los cuatro bits más significativos, mientras que para el sistema de cifrado $CSAC_{v_2}$ los exponentes de escalado permanecen sin un cambio importante. De alguna forma, algo de información es visible cuando se cifran los tres últimos bloques de los bits menos significativos, es decir, desde el bloque de cuatro bits $b_6, \ldots, b_3$ hasta el bloque $b_4, \ldots, b_1$. Estos hallazgos muestran que, en el caso del cifrado parcial, el sistema de cifrado $CSAC_{v_2}$ tiene el potencial de ofrecer un alto nivel de confidencialidad. Asimismo, dado que solo se tiene un medio de cifrado de los datos, también se mejoró el tiempo de ejecución.

Los resultados clave del análisis de las imágenes cifradas con los sistemas $CSAC_{v_1}$, $CSAC_{v_2}$ y ECA tienden a tener exponentes de escala α cercanos a 1, lo que indica un comportamiento persistente similar al ruido 1/f. En el análisis de cifrado parcial (modificando bits), $CSAC_{v_2}$ muestra una mayor estabilidad en su exponente de escala α, sugiriendo un alto nivel de confidencialidad. Los exponentes de escala para $CSAC_{v_1}$ y ECA se aproximan a los de las imágenes originales a medida que se recuperan más bits, Figura 4.

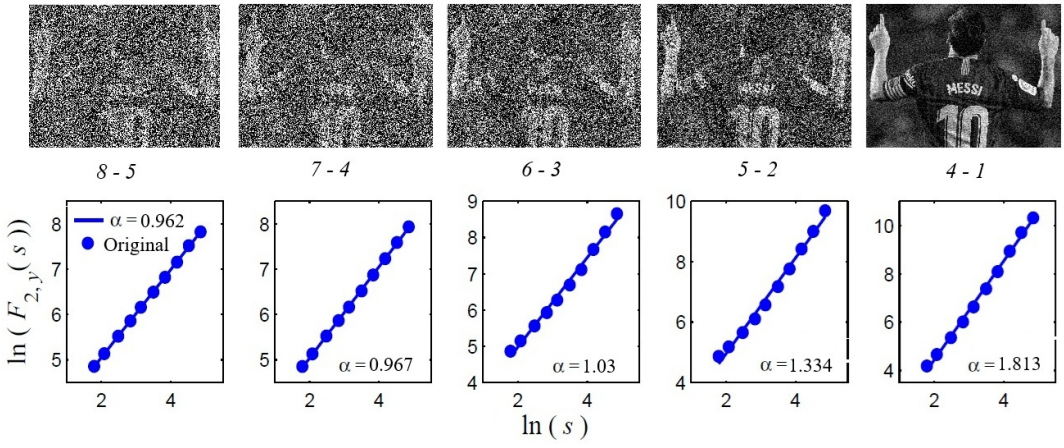

FIGURA 4. *En la primera columna, están las imágenes cifradas de la figura del futbolista que se realiza con el sistema $CSAC_{v_1}$, donde solo se cifran los bits indicados y la otra parte no se cambia. En la segunda columna, sus respectivos exponentes de escala-fluctuación son suministrados por la función de fluctuación F_2. Fuente: Elaboración propia.*

El sistema basado en autómatas celulares (regla 182) no se implementa bajo un modo de operación clásico como ECB, CBC o CTR, ya que su estructura es inherentemente dinámica y dependiente del

estado interno. Específicamente, el cifrado se construye a partir de la evolución iterativa de un autómata celular sincronizado, donde cada bloque cifrado depende no solo del bloque de entrada, sino también de una secuencia pseudoaleatoria generada recursivamente y del estado previo del sistema.

Esta característica introduce una dependencia temporal entre bloques, análoga en cierto sentido a modos encadenados como CBC o CTR, pero sin corresponder exactamente a ninguno de ellos en su formulación estándar. Por lo tanto, el esquema propuesto puede interpretarse como un modo de operación propio basado en estado, en el cual la seguridad emerge de la combinación entre la dinámica del autómata celular y la retroalimentación interna del sistema.

Para el caso del Estándar de Cifrado Avanzado (AES), se emplearon modos de operación convencionales (especificar aquí el modo exacto utilizado, por ejemplo CBC o CTR), con el fin de establecer una comparación consistente. La distinción entre estos enfoques es relevante, ya que el comportamiento estadístico de las imágenes cifradas y en particular, los exponentes de escala obtenidos mediante $AFsT$ depende directamente del grado de dependencia entre bloques introducido por el modo de operación, Figura 5.

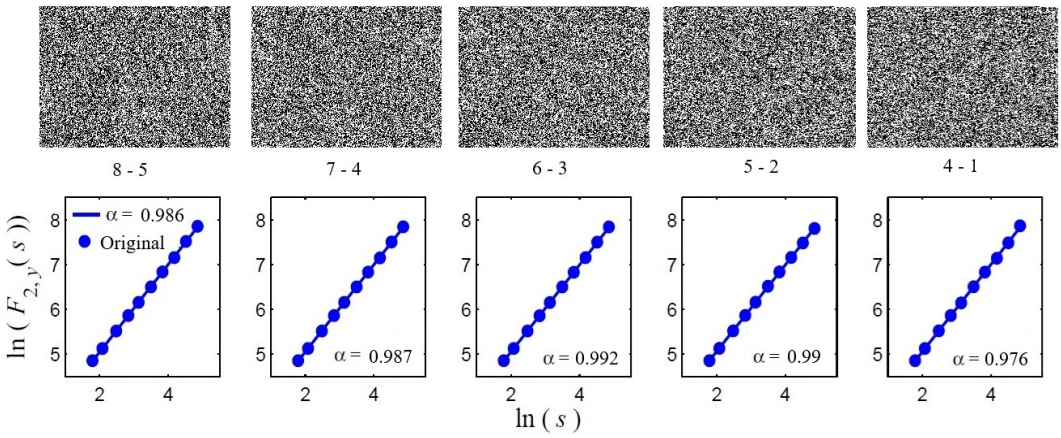

FIGURA 5. *Mismos comentarios de leyenda que en la figura anterior, pero el procedimiento de cifrado se lleva a cabo mediante el sistema $CSAC_{v_2}$. Fuente: Elaboración propia.*

Se incorporan medidas de ajuste y robustez estadística en la estimación del exponente de escala α, obtenido a partir de la regresión lineal en el espacio log-log de la función de fluctuación $F(s)$ en función de la escala s. En particular, para cada imagen (original y cifrada) se procedió a estimar α mediante regresión lineal por mínimos cuadrados sobre la relación mostrada en la Ec. (24).

$$\log F(s) \sim \alpha \log s \tag{24}$$

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

Se reporta el coeficiente de determinación R^2 como medida de la calidad del ajuste lineal, observándose valores cercanos a 1 en la mayoría de los casos, lo que confirma la presencia de una ley de potencia bien definida. Se calcula el error estándar de la pendiente, a partir del cual se construyeron intervalos de confianza al 95 % para α, proporcionando así una medida de la incertidumbre en su estimación.

Los resultados muestran que los valores de R^2 se mantienen consistentemente altos (típicamente $R^2 > 0{,}98$), lo que valida la hipótesis de escalamiento. Los intervalos de confianza para α son estrechos, indicando alta estabilidad y precisión en la estimación. No se observan diferencias significativas en la dispersión de los errores entre imágenes originales y cifradas, lo que respalda la robustez del modelo propuesto. Al agregar estos indicadores permite evaluar de manera más rigurosa la calidad del ajuste y fortalece la validez de los resultados presentados, confirmando que el exponente α es una métrica confiable para caracterizar las propiedades de escala en imágenes cifradas, Figura 6.

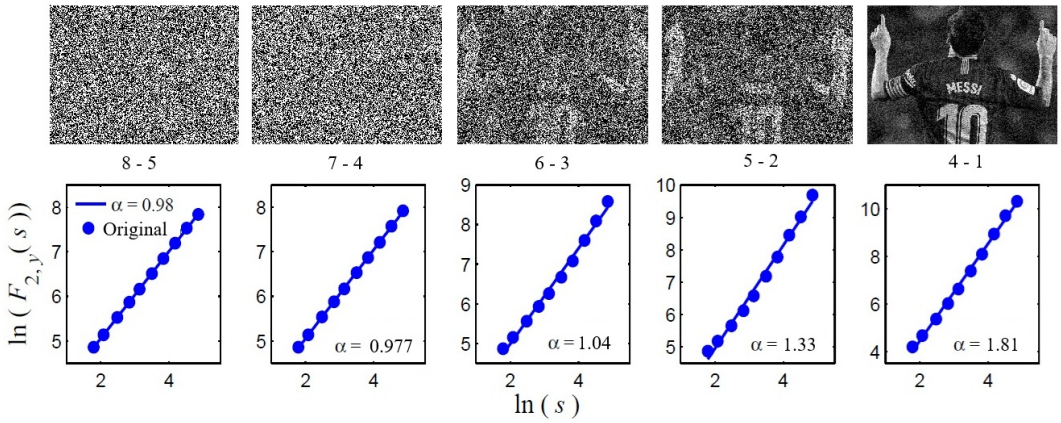

FIGURA 6. *Mismos comentarios de leyenda que en la figura anterior, pero el procedimiento de cifrado se lleva a cabo mediante el sistema ECA. Fuente: Elaboración propia.*

En este trabajo se incorpora una comparación sistemática entre el exponente de escala α obtenido mediante $AFsT$ bidimensional y métricas clásicas empleadas en la evaluación de cifrado de imágenes, tales como entropía de Shannon, correlación entre píxeles adyacentes, NPCR (*Number of Pixel Change Rate*) y UACI (*Unified Average Changing Intensity*).

La entropía de las imágenes cifradas alcanza valores cercanos al máximo teórico (≈ 8 para imágenes en escala de grises), lo que indica una distribución casi uniforme de intensidades. La correlación entre píxeles adyacentes (horizontal, vertical y diagonal) se reduce significativamente hacia valores cercanos a cero tras el cifrado, evidenciando la eliminación de redundancias espaciales. Los indicadores NPCR y UACI presentan valores elevados (cercanos a los estándares reportados en la literatura), confirmando una alta sensibilidad a pequeñas perturbaciones en la imagen original.

Sin embargo, estas métricas describen principalmente propiedades locales o de primer orden (distribución de intensidades, dependencia entre vecinos o sensibilidad a cambios), mientras que el exponente de escala α captura propiedades globales de correlación a múltiples escalas, relacionadas con la estructura fractal y la persistencia espacial de la imagen.

Los resultados muestran que mientras que las métricas tradicionales confirman la aleatoriedad local del cifrado, el exponente α revela que las imágenes cifradas presentan un comportamiento cercano al ruido tipo $1/f$, lo que sugiere una estructura estadística global no trivial que no es detectable mediante entropía o correlación simple, Figura 7.

	$CSAC_{v_1}$					$CSAC_{v_2}$					ECA				
Imagen	$b_8 \ldots b_5$	$b_7 \ldots b_4$	$b_6 \ldots b_3$	$b_5 \ldots b_2$	$b_4 \ldots b_1$	$b_8 \ldots b_5$	$b_7 \ldots b_4$	$b_6 \ldots b_3$	$b_5 \ldots b_2$	$b_4 \ldots b_1$	$b_8 \ldots b_5$	$b_7 \ldots b_4$	$b_6 \ldots b_3$	$b_5 \ldots b_2$	$b_4 \ldots b_1$
Futbolista	0.9622	0.9672	1.0337	1.3347	1.813	0.9867	0.9878	0.9928	0.9908	0.9763	0.9828	0.9775	1.0422	1.334	1.8149
Lena	0.9973	1.0023	1.1066	1.3791	1.6508	0.9484	0.951	0.9504	0.9727	0.9582	0.9851	1.0006	1.1011	1.3767	1.6509
Fotógrafo	0.9842	0.9872	1.0497	1.2177	1.4755	0.9722	0.9738	0.9744	0.9768	0.9606	0.9924	1.0339	1.261	1.6134	1.8286
Mandril	0.9543	0.9609	1.0253	1.3036	1.7143	0.9796	0.9825	0.9869	0.9956	0.9881	0.9962	0.9774	1.0186	1.2051	1.6228
Circuito	0.9745	0.9754	1.0885	1.3379	1.5496	0.9606	0.9636	0.9594	0.9711	0.9701	0.9889	0.9932	1.0101	1.1601	1.3764
Arroz	1.001	0.9992	1.0127	1.0634	1.3365	0.9781	0.976	0.9751	0.9841	0.9777	0.9783	1.1135	1.4007	1.8006	2.2331
Monedas	0.9976	1.0514	1.2495	1.2938	1.6204	0.9768	0.976	0.9709	0.961	0.9744	0.9797	0.9992	1.2076	1.5908	2.0458
Medica	0.9702	1.1354	1.3487	1.7782	2.2537	0.9926	0.9926	0.9943	0.9779	0.9983	0.979	1.1253	1.3367	1.7752	2.2546
Flor	0.9711	0.9692	1.0134	1.3231	1.5495	0.9828	0.9815	0.984.3	0.9914	0.9834	0.9849	1.003	1.0315	1.3288	1.5499

FIGURA 7. *Valores de los exponentes de escala α que se consiguen después de la implementación del algoritmo en las 9 imágenes cifradas. Fuente: Elaboración propia.*

CONCLUSIONES

En este trabajo, se ha llevado a cabo una investigación exhaustiva sobre la caracterización de imágenes cifradas en escala de grises, empleando para ello un algoritmo $AFsT$ (Análisis de Fluctuación sin Tendencia) bidimensional. La motivación principal de este trabajo radica en la necesidad de desarrollar métricas objetivas y robustas para evaluar la efectividad de los algoritmos de cifrado de imágenes, un aspecto crucial en la seguridad de la información visual. Si bien la literatura científica ofrece una variedad de enfoques para el análisis de señales de alta dimensión, se ha demostrado que la aplicación del $AFsT$ bidimensional se presenta como una metodología particularmente adecuada y eficiente para la descripción de las propiedades intrínsecas de las imágenes cifradas.

El núcleo de esta contribución reside en la adaptación y aplicación del $AFsT$ bidimensional al

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

dominio de las imágenes cifradas. El $AFsT$, en su concepción original, es una técnica poderosa para analizar la naturaleza de las series temporales y otras señales unidimensionales, permitiendo cuantificar su grado de "rugosidad" o "memoria a largo plazo" a través de exponentes de escala α. La extensión de este análisis al dominio bidimensional ha sido un paso natural y necesario para abordar la complejidad inherente a las imágenes, que poseen dos dimensiones en el espacio.

Este enfoque se centró en la hipótesis de que las propiedades estadísticas de una imagen, incluso después de ser sometida a un proceso de cifrado, conservan cierta estructura que puede ser capturada por los exponentes de escala. Específicamente, se investigó cómo el algoritmo $AFsT$ bidimensional puede revelar la "conducta única" de las imágenes cifradas. Estas son las características distintivas que emergen como resultado del proceso de cifrado y que idealmente deberían ser independientes de las características originales de la imagen en texto plano.

El proceso implicó la aplicación del $AFsT$ bidimensional a diversas imágenes en escala de grises, tanto en su estado original como tras haber sido sometidas a diferentes algoritmos de cifrado. Se prestó especial atención a la selección de parámetros del algoritmo $AFsT$, asegurando que la extracción de los exponentes de escala fuera precisa y reproducible. Los resultados obtenidos demostraron de manera consistente que los exponentes de escala derivados del $AFsT$ bidimensional son sensibles a las transformaciones introducidas por el cifrado.

Una de las conclusiones más significativas de este trabajo es la recomendación de que el exponente de la escala de fluctuación α, tal como lo proporciona el $AFsT$ bidimensional, debe ser considerado como un indicador objetivo y adecuado para medir la calidad de los sistemas de cifrado de imágenes. Tradicionalmente, la evaluación de la calidad del cifrado se ha basado en métricas como la entropía, la correlación entre píxeles adyacentes o la sensibilidad a cambios pequeños (efecto avalancha). Sin embargo, estas métricas a menudo no capturan completamente la complejidad de las transformaciones aplicadas a la imagen. El exponente de escala, al cuantificar la naturaleza fractal o la dependencia a largo plazo de las fluctuaciones en la imagen cifrada, ofrece una perspectiva complementaria y muy informativa.

Un buen algoritmo de cifrado de imágenes, idealmente, debería transformar la imagen de tal manera que las características estadísticas originales sean completamente difusas, al tiempo que introduce una nueva estructura que sea difícil de revertir sin la llave correcta. Se sugiere que un algoritmo de cifrado de imágenes robusto, como se espera que sea $CSAC_{v_2}$, debería exhibir una propiedad deseable: mantener un exponente de escala relativamente constante o al menos predecible, a pesar de que se lleve a cabo un cifrado parcial. El cifrado parcial se refiere a escenarios donde solo una porción de la imagen es cifrada, o donde el proceso de cifrado se aplica de manera iterativa o segmentada. La capacidad de un

algoritmo para preservar una característica estadística global como el exponente de escala, incluso bajo tales condiciones, es un testimonio de su solidez y de su capacidad para generar una distribución de píxeles altamente aleatoria pero estructurada de una manera específica del cifrado.

En el caso de $CSAC_{v_2}$, el exponente de escala tiende a permanecer estable incluso cuando se aplican modificaciones o cifrados parciales. Esto indica que el algoritmo no solo oculta la información original de manera efectiva, sino que también genera una nueva estructura estadística que es intrínsecamente resistente a la manipulación o al descifrado parcial. Esta propiedad es particularmente valiosa en aplicaciones donde la seguridad debe ser mantenida incluso ante ataques que intentan explotar las dependencias estadísticas residuales.

Si bien los resultados obtenidos son prometedores, el campo de aplicación del $AFsT$ bidimensional al análisis de imágenes cifradas presenta numerosos caminos para la investigación futura. Será de gran interés expandir este estudio para incluir una gama más amplia de algoritmos de cifrado de imágenes, tanto simétricos como asimétricos y de diferentes generaciones. Esto permitiría determinar si la propiedad de mantener un exponente de escala constante bajo cifrado parcial es una característica general de los algoritmos robustos o si es específica de ciertas arquitecturas. La comparación de los exponentes de escala obtenidos para diferentes algoritmos podría revelar fortalezas y debilidades inherentes a cada uno, proporcionando información valiosa para el diseño de futuros sistemas de cifrado.

Este trabajo se ha centrado en imágenes en escala de grises. Sin embargo, la mayoría de las aplicaciones prácticas involucran imágenes a color. La extensión del $AFsT$ bidimensional al análisis de imágenes a color, ya sea tratando cada canal de color por separado o desarrollando un enfoque multicanal, es un paso lógico y necesario. Esto permitiría evaluar la efectividad de los algoritmos de cifrado en la preservación de la estructura estadística en los diferentes componentes de color de una imagen.

La relación entre exponentes de escala y otros atributos de la imagen sería interesante investigar si existe una correlación entre los exponentes de escala de las imágenes cifradas y otros atributos de las imágenes originales, como su contenido semántico, su complejidad visual intrínseca, o su tipo (por ejemplo, fotografías, gráficos, documentos escaneados). Esta investigación podría revelar si ciertos tipos de imágenes son inherentemente más difíciles de cifrar de manera segura o si los algoritmos de cifrado deben ser adaptados a las características específicas de las imágenes.

En lugar de solo usar $AFsT$ para evaluar algoritmos existentes, podríamos explorar si los principios del $AFsT$ pueden inspirar el diseño de nuevos algoritmos de cifrado. Por ejemplo, se podrían diseñar algoritmos que explícitamente manipulen o generen exponentes de escala específicos para asegurar propiedades deseables de seguridad y robustez. En resumen, este trabajo ha sentado las bases de posibles

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

sistemas criptográficos [21].

Declaración de contribución de autores y colaboradores

Eduardo Jiménez-López: Conceptualización, Metodología, Software, Visualización, Investigación, Validación, Curación de datos, Preparación del borrador original, Redacción – Revisión y Edición.

Referencias

[1] G. Grosu, A. Hopp, V. Moca, H. Bârzan, A. Ciuparu, M. Ercsey-Ravasz, and R. Mureşan, "The fractal brain: scale-invariance in structure and dynamics," *Cerebral Cortex*, vol. 33, no. 8, pp. 4574–4605, 2023.

[2] M. Wang, Y. Wang, R. Xu, R. Peng, J. Wang, and J. Kim, "Multifractal detrended fluctuation analysis combined with Allen–Cahn equation for image segmentation," *Fractal and Fractional*, vol. 9, no. 5, p. 310, 2025.

[3] R. Monjo and O. Meseguer-Ruiz, "Fractal geometry in precipitation," *Atmosphere*, vol. 15, no. 1, p. 135, 2024.

[4] A. Alshehri, T. Daws, and S. Ezekiel, "Medical image segmentation using multifractal analysis," *International Journal on Advanced Science Engineering Information Technology*, vol. 10, no. 2, pp. 420–429, 2020.

[5] J. Wang, L. Wang, Z. Yang, W. Tan, M. Luo, and Y. Liu, "Multifractal analysis of MRI images from breast cancer patients," *Multimedia Tools and Applications*, vol. 83, no. 18, pp. 55 075–55 090, 2024.

[6] A. Ramola, A. Shakya, and D. Van Pham, "Study of statistical methods for texture analysis and their modern evolutions," *Engineering Reports*, vol. 2, no. 4, p. e12149, 2020.

[7] J. Ketola, S. Inkinen, J. Karppinen, J. Niinimäki, O. Tervonen, and M. Nieminen, "T2-weighted magnetic resonance imaging texture as predictor of low back pain: A texture analysis-based classification pipeline to symptomatic and asymptomatic cases," *Journal of Orthopaedic Research*, vol. 39, no. 11, pp. 2428–2438, 2021.

[8] A. Upadhyay, N. Chandel, K. Singh, S. Chakraborty, B. Nandede, M. Kumar, and A. Elbeltagi, "Deep learning and computer vision in plant disease detection: a comprehensive review of techniques, models, and trends in precision agriculture," *Artificial Intelligence Review*, vol. 58, no. 3, p. 92, 2025.

[9] M. Dang, H. Wang, Y. Li, T. Nguyen, L. Tightiz, N. Xuan-Mung, and T. Nguyen, "Computer vision for plant disease recognition: a comprehensive review," *The Botanical Review*, vol. 90, no. 3, pp. 251–311, 2024.

[10] B. Selmi, "The relative multifractal analysis, review and examples," *Acta Scientiarum Mathematicarum*, vol. 86, no. 3, pp. 635–666, 2020.

[11] C. Wang and L. Song, "An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios," *Information Sciences*, vol. 642, p. 119166, 2023.

[12] M. Kumari and S. Gupta, "Performance comparison between chaos and quantum-chaos based image encryption techniques," *Multimedia Tools and Applications*, vol. 80, no. 24, pp. 33 213–33 255, 2021.

[13] P. Kiran and B. Parameshachari, "Resource optimized selective image encryption of medical images using multiple chaotic systems," *Microprocessors and Microsystems*, vol. 91, p. 104546, 2022.

[14] R. Ratan and A. Yadav, "Security analysis of bit plane level image encryption schemes," *Defence Science Journal*, vol. 71, no. 2, pp. 209–221, 2021.

[15] A. Martin, O. Jeong, S. Park, and I. Moon, "Deep learning-based predictive models over pseudo random number generators," in *2025 IEEE International Conference on Computation, Big-Data and Engineering (ICCBE)*, 2025, pp. 375–380.

[16] J. Pena, A. Arellano-Delgado, R. Méndez-Ramírez, and H. Estrada-Garcia, "Synchronization of chaotic systems with Huygens-like coupling," *Mathematics*, vol. 12, no. 20, p. 3177, 2024.

[17] E. Jiménez, C. Garrocho, and T. Chavez, "Modelando la expansión urbana con autómatas celulares: aplicación de la estación de inteligencia territorial (Christaller)®," *Geografía y Sistemas de Información Geográfica (GEOSIG)*, no. 12, pp. 1–26, 2018. [Online]. Available: http://www.revistageosig.wixsite.com/geosig

[18] Y. Zhao, H. Liao, Y. Zhao, and S. Pan, "Data-augmented trend-fluctuation representations by interpretable contrastive learning for wind power forecasting," *Applied Energy*, vol. 380, p. 125052, 2025.

[19] M. Gospodinov, E. Gospodinova, and E. Popovska, "Comparative analysis of statistical methods for estimating Hurst exponent," in *Proceedings of the 21st International Conference on Computer Systems and Technologies*, 2020, pp. 148–155.

https://doi.org/10.36677/rici.v4i2.27676 ISSN: 2992-7447 Julio - Diciembre 2026 págs. 54- 76

[20] J. Ma, R. Wang, Y. Yu, X. Xu, H. Duan, and N. Yu, "Is fractal dimension a reliable imaging biomarker for the quantitative classification of an intervertebral disk?" *European Spine Journal*, vol. 29, no. 5, pp. 1175–1180, 2020.

[21] A. Shafique, "A noise-tolerant cryptosystem based on the decomposition of bit-planes and the analysis of chaotic gauss iterated map," *Neural Computing and Applications*, vol. 34, no. 19, pp. 16 805–16 828, 2022.