DESDE 2013
https://repository.uaeh.edu.mx/revistas/index.php/icbi/issue/archive
Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI
ISSN: 2007-6363

Publicación semestral, Vol. 13, No. Especial (2025) 70–77

Simetría en histogramas de imágenes cifradas con la transformación negativa-positiva
Symmetry in histograms of images encrypted with negative-positive transformation

M. A. Cardona-López [a], J. C. Chimal-Eguía [a], V. M. Silva-García [b], R. Flores-Carapia [b,*]

[a] *Centro de Investigación en Computación, Instituto Politécnico Nacional, 07738, GAM, CDMX, México.*
[b] *Centro de Innovación y Desarrollo Tecnológico en Cómputo, Instituto Politécnico Nacional, 07738, GAM, CDMX, México.*

Resumen

En este trabajo se analizó la simetría de los histogramas de imágenes cifradas mediante la Transformada Negativa-Positiva (TNP), un aspecto relevante que podría afectar el objetivo del cifrado de imágenes al buscar histogramas uniformes. Para el análisis teórico, se describió el comportamiento de los píxeles después del cifrado como un experimento binomial, donde la cantidad de píxeles para un nivel específico se definió mediante una variable aleatoria con distribución binomial. Esto permitió demostrar que los valores esperados de la cantidad de píxeles en dos niveles simétricos (por ejemplo, 0 y 255, 1 y 254, etc.) son iguales y corresponden al promedio de ambos niveles, lo que provoca una reflexión horizontal en el histograma, haciéndolo simétrico. Además, la simetría fue verificada numéricamente mediante el cifrado de la imagen de Baboon con cinco tamaÃ±*osdebloquesdi f erentesymedianteunapruebadebondadya juste*, *dondeseobtuvoqueeltamaÃ±odelbloquein f luyeenlaindependenciadel*

Palabras Clave: Cifrado, experimento binomial, histograma, imágenes, transformación negativa-positiva.

Abstract

This work analyzed the symmetry of histograms in images encrypted using the Negative-Positive Transform (NPT). This important factor could influence the goal of achieving uniform histograms in image encryption. For the theoretical analysis, pixel transformations after encryption was modeled as a binomial experiment, where the number of pixels at a specific level was represented by a random variable following a binomial distribution. This approach demonstrated that the expected number of pixels at two symmetrical levels (e.g., 0 and 255, 1 and 254) are equal and correspond to the average of both levels. This results in a horizontal reflection in the histogram, making it symmetrical. The symmetry was further verified through numerical experiments by encrypting the Baboon image using five different block sizes and performing a goodness-of-fit test, which showed that block size affects the independence of the experiment's trials.

Keywords: Encryption, binomial experiment, histogram, images, negative-positive transformation.

1. Introducción

La transformación negativa-positiva (TNP) es una técnica comúnmente integrada en criptosistemas para cifrar imágenes JPEG, siendo utilizada en diversas propuestas (Aryal *et al.*, 2017; Imaizumi *et al.*, 2017; Imaizumi y Kiya, 2018; Aryal *et al.*, 2018; Motomura *et al.*, 2023). Su compatibilidad con la compresión con pérdida de información en estas imágenes es la razón principal de su aplicación (El Saj *et al.*, 2021). La TNP opera antes de ejecutar la compresión y mediante un cifrado por bloques de píxeles (Sirichotedumrong *et al.*, 2019). Su funcionalidad se ha implementado tanto en imágenes a color como en escala de grises (Ahmad y Shin, 2023; Kenta *et al.*, 2015).

Principalmente la TNP se aplica en el ámbito de la protección de datos (Li y Lo, 2020), no solo de imágenes JPEG. También se utiliza en el cifrado de fotogramas en vídeos con compresión MJPEG (Shimizu *et al.*, 2018) y para cifrar imágenes que no se comprimen con el estándar JPEG (Zhang *et al.*, 2021). También se emplea para cifrar imágenes que sirven controlar el acceso a modelos de redes neuronales convolucionales (Maungmaung y Kiya, 2021).

*Autor para correspondencia: rfloresca@ipn.mx
Correo electrónico: mcardonal2022@cic.ipn.mx (Manuel Alejandro Cardona-López), jchimale@ipn.mx (Juan Carlos Chimal-Eguía), vsilvag@ipn.mx (Víctor Manuel Silva-García), rfloresca@ipn.mx (Rolando Flores-Carapia).

Historial del manuscrito: recibido el 01/09/2024, última versión-revisada recibida el 27/11/2024, aceptado el 27/11/2024, publicado el 26/04/2025. **DOI:** https://doi.org/10.29057/icbi.v13iEspecial.13581

Sin embargo, los trabajos mencionados anteriormente no suelen incluir mediciones criptográficas (Singh y Singh, 2022), como el análisis del histograma. Este análisis es importante porque evalúa la uniformidad del histograma, una característica que indica que los valores de los píxeles aparecen el mismo número de veces a lo largo de la imagen, lo cual es uno de los indicadores de un cifrado seguro (Ghadirli *et al.*, 2019). Dado que en ocasiones la TNP es la última operación de cifrado en algunos criptosistemas (Chuman *et al.*, 2019), el histograma resultante adquirirá la forma producida por la TNP. Asimismo, la mayoría de las operaciones que conforman los algoritmos en trabajos previos se limitan a cambiar la posición de los píxeles, pero no alteran su valor como lo hace la TNP. Por esta razón, es la única técnica que podría llegar a modificar el histograma.

Por las razones expuestas, resulta importante analizar la forma que adopta el histograma de una imagen tras su cifrado con la TNP, para evaluar tanto el alcance como las limitaciones que esta técnica impone sobre el histograma, un aspecto fundamental para medir la seguridad de las imágenes cifradas. En este contexto, el presente trabajo se centra en examinar cómo se distribuyen las intensidades de color de los píxeles al concluir el cifrado. Dado que la TNP se basa en una variable aleatoria de Bernoulli, el análisis se lleva a cabo mediante un experimento binomial. Además, se incluye la verificación de los resultados teóricos.

El trabajo se organiza de la siguiente manera: en la sección 2 se presentan las herramientas teóricas utilizadas para el análisis de la simetría; la sección 3 expone el desarrollo del análisis teórico de la simetría del histograma; en la sección 4 se verifica dicho análisis, y finalmente, las conclusiones se presentan en la sección 5.

2. Herramientas teóricas

A continuación se presentan las herramientas teóricas empleadas en el desarrollo de este trabajo. En primer lugar, se introduce la distribución de Bernoulli, ya que el método de cifrado de la TNP utiliza una variable aleatoria que sigue dicha distribución. Posteriormente, se describe en qué consiste el cifrado con la TNP y cómo se aplica sobre las imágenes. En la subsección sobre el experimento binomial, se detallan las características que lo componen, dado que el análisis teórico de la simetría del histograma se basa en su aplicación sobre los píxeles de la imagen antes y después de ser cifrada. Finalmente, se explica la prueba de bondad y ajuste, utilizada para verificar los resultados teóricos, midiendo la simetría de los histogramas de la imagen cifrada.

2.1. Distribución de Bernoulli

Una variable aleatoria discreta X con distribución de Bernoulli es aquella que solo puede tomar uno de dos posibles valores. Uno de ellos, denominado "éxito"($X = 1$), ocurre con una probabilidad p, mientras que el otro, denominado "fracaso"($X = 0$), ocurre con una probabilidad $q = 1 - p$, donde $0 < p < 1$. En el presente trabajo, la salida $X = 1$ indica que el bloque seleccionado será cifrado modificando los valores de todos los píxeles que lo componen, mientras que $X = 0$ significa que los valores de los píxeles se mantendrán intactos.

2.2. La transformación negativa-positiva

Es una técnica de cifrado por bloques, que actúa simultáneamente sobre todos los píxeles que pertenecen a un mismo bloque. La transformación puede asignar un nuevo valor a todos los píxeles o mantener el valor original de todos ellos. Denotando al bloque número j como B_j, mientras que $b_j(i)$ se refiere al píxel número i de dicho bloque, y $b'_j(i)$ al mismo píxel después de la transformación.

En el caso de que los píxeles de una imagen puedan tomar hasta 256 intensidades diferentes, cuando la transformación requiere modificar estos valores, se realiza mediante el cálculo del complemento a 255 de cada uno de ellos. Esto se expresa como $b'(i) = 255 - b(i)$. Además, la decisión sobre qué bloques deben ser modificados y cuáles deben mantenerse intactos se toma de manera aleatoria, de acuerdo con lo indicado por la variable aleatoria X, con una probabilidad de $p = q = 0{,}5$. Todo lo anterior se describe en (1).

$$b'(i) = \begin{cases} 255 - b(i), & \text{si } X = 1 \\ b(i), & \text{si } X = 0 \end{cases} \tag{1}$$

2.3. Experimento binomial

Para que un experimento probabilístico sea considerado binomial, debe cumplir con las siguientes características (Taufiq *et al.*, 2020):

- El experimento consta de n ensayos idénticos y repetidos.
- Cada ensayo solo puede dar lugar a uno de dos posibles resultados: uno denominado éxito y el otro fracaso.
- En cada ensayo, la probabilidad de éxito es p, mientras que la de fracaso es $1 - p$. Estas probabilidades permanecen constantes a lo largo de los n ensayos.
- Los ensayos son independientes entre sí.
- La variable aleatoria Y representa el número de éxitos en los n ensayos, con $Y = 0, 1, 2, \ldots, n$, y sigue una distribución binomial.

Para un experimento binomial con probabilidad de éxito p, la probabilidad de obtener k éxitos en n ensayos, denotada como $P(Y = k)$, está dada por (2), donde ! indica el factorial de un número; por ejemplo, $n! = 1 \times 2 \times \cdots \times n$.

$$P(Y = k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k} \tag{2}$$

Además, el valor esperado de la variable Y está dado por $E[Y] = np$ y su varianza $\sigma^2 = n(p - p^2)$.

2.4. Prueba de bondad y ajuste

Es una prueba de hipótesis estadística que se utiliza para comparar si los datos observados en un experimento tienen determinada distribución (Rolke y Gongora, 2021). Es decir, se evalúa la cercanía de una distribución teórica con la información recopilada. La hipótesis nula es H_0: los datos siguen la

distribución teórica, donde el estadístico de prueba es χ calculado como se define en (3). Suma los cuadrados de las diferencias entre las frecuencias observadas del experimento, O_i, y los valores esperados de la distribución, E_i.

$$\chi = \sum_{i=1}^{d} \frac{(O_i - E_i)^2}{E_i} \tag{3}$$

El estadístico sigue una distribución χ^2 con $d-1$ grados de libertad, donde d indica el número de categorías en las que se dividen los datos. En el caso de los histogramas de las imágenes a color el número de categorías d =256, que corresponde a los niveles de intensidad diferentes de un píxel. Para ese número de categorías, se dice, al nivel de significancia de 0,05, que los datos siguen una distribución teórica si $\chi < 291$ (Musanna *et al.*, 2022).

3. Análisis de la simetría del histograma

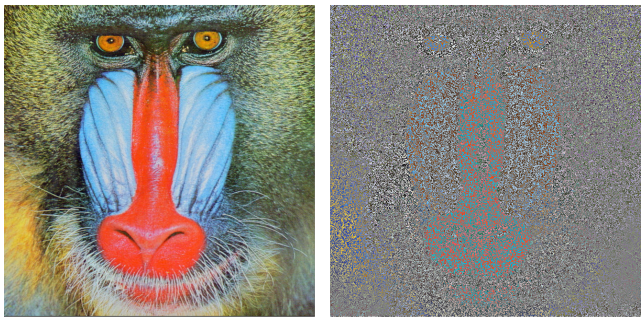
En esta sección se presenta el análisis teórico que explica las razones por las cuales el histograma de una imagen cifrada con la TNP muestra simetría. Primero, se realiza un experimento binomial para analizar el cambio en el número de píxeles con una determinada intensidad como resultado del cifrado. Posteriormente, utilizando los resultados de este experimento, se calcula el valor esperado del número de píxeles para un par de intensidades simétricas.

3.1. Un experimento binomial sobre los píxeles

Sea k_f el número de píxeles en una imagen que inicialmente tienen una intensidad igual a f. Cabe destacar que en el caso de imágenes a color de 24 bits, existen 256 intensidades diferentes para cada color, por lo que $0 \leq f \leq 255$. Para fines prácticos, cuando se hace referencia al valor f, se enfoca a los valores del píxel dentro de un canal de color específico, ya sea rojo, verde o azul. El experimento consiste en observar el número de píxeles que cambiaron su valor después de que la imagen fue cifrada con la TNP y que inicialmente tenían el valor f. Este experimento se considera binomial, ya que cumple con las características mencionadas en la subsección 2.3, como se explica a continuación.

- El experimento consiste en k_f ensayos idénticos, en los cuales se verifica si cada uno de los k_f píxeles ha cambiado su valor tras el proceso de cifrado.
- Cada ensayo tiene dos posibles resultados: un ”éxito”si el píxel cambió su valor, y un ”fracaso”si mantuvo el valor original.
- En cada ensayo, la probabilidad de éxito es $p = 0{,}5$, y la de fracaso también es 0,5. Estas probabilidades permanecen constantes, ya que la transformada opera con una variable aleatoria de Bernoulli con dichas probabilidades.
- Los ensayos son independientes, dado que no todos los valores k_f están ubicados en el mismo bloque, lo que implica que no todos pueden cifrarse en el mismo bloque.
- La variable aleatoria Q representa el número de píxeles que cambiaron su valor en los k_f ensayos, con $Q = 0, 1, 2, \ldots, k_f$.

Para ilustrar lo anterior, se presenta un ejemplo utilizando la imagen de Baboon a color de 512×512 píxeles, que se puede apreciar en la figura 1(a). En este caso, se trabajó con el canal de color rojo en la intensidad $f = 0$, la cual tiene una frecuencia de $k_0 = 56$, lo que establece el número de ensayos del experimento en $n = 56$. El experimento se repitió 500 veces para observar el número de éxitos en cada caso, es decir, cuántos píxeles con valor inicial de 0 cambiaron su valor tras ser cifrados mediante la TNP, utilizando bloques de 1×1 píxeles. En la figura 1(b) se ilustra el cifrado resultante en uno de los experimentos. La gráfica de estos resultados se presenta en la figura 2. Además, se comprobó que la distribución resultante se ajusta a una distribución binomial (Katsis y Toman, 1999), utilizando la prueba de bondad de ajuste, la cual arrojó un valor p de 0.99998. Dado que este valor es superior a 0.05, se acepta que sigue una distribución binomial.



(a) (b)

Figura 1: Imagen de Baboon utilizada para verificar los resultados teóricos. (a) Imagen original. (b) Imagen cifrada con la NTP en bloques de 1×1 píxeles.

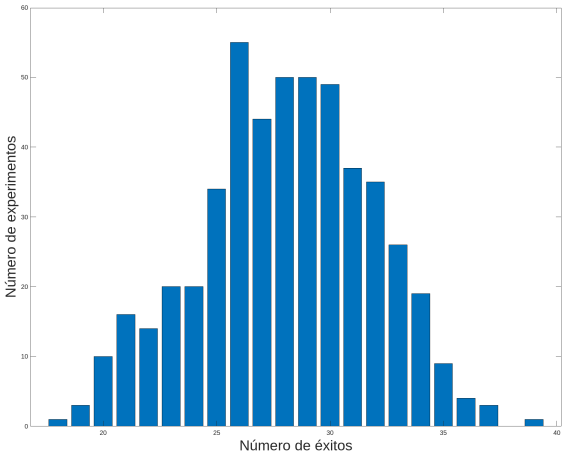


Figura 2: Número de píxeles que cambiaron su valor (éxitos) después del cifrado con la TNP, considerando un total de 56 píxeles (ensayos) con valor inicial cero, en 500 experimentos reproducidos.

3.2. El valor esperado de dos frecuencias simétricas

Dado que en la sección anterior se demostró que la variable aleatoria Q sigue una distribución binomial, su valor esperado

de éxitos es $E[Q] = np$. Esto implica que, en promedio, la cantidad de píxeles que cambiaron su valor f es la mitad de los existentes, como lo indica (4). Asimismo, la frecuencia k_f se habría reducido a la mitad debido a este cambio.

$$E[Q] = k_f \times 0{,}5 \tag{4}$$

Sin embargo, aunque el número de píxeles con valor f disminuyó bajo el experimento mencionado, es importante recordar que este no es el único experimento que puede observarse durante el cifrado de la imagen con la TNP. También se puede analizar, de manera análoga, la variable aleatoria R, que representa el número de píxeles que cambiaron su valor original de $255 - f$. Es decir, se está observando el nivel de intensidad simétrico a f. Dado que este experimento cumple las mismas características que el previamente presentado en la subsección 3.1, se puede afirmar que R sigue una distribución binomial, cuyo valor esperado se expresa en (5). De este modo, también se espera que, en promedio, la mitad de los píxeles cambien, y solo la mitad mantenga la intensidad $255 - k$.

$$E[R] = k_{255-f} \times 0{,}5 \tag{5}$$

En cuanto a los valores que cambiaron, de acuerdo con la definición de la transformación en (1), el cifrado se realiza con la operación $255 - (255 - f)$, lo que resulta en f. En otras palabras, los píxeles que inicialmente tenían el valor $255 - f$ y que cambiaron su valor después del cifrado con la TNP, lo hicieron adoptando el valor f. Por lo tanto, se espera que la cantidad de píxeles que tomen este valor sea $k_{255-f} \times 0{,}5$.

En consecuencia, la variable S, expresada en (6), representa el número de píxeles en la imagen cifrada con la TNP que obtuvieron el valor f. Al restar k_f con la variable Q se obtiene los píxeles que originalmente tenían dicho valor y no cambiaron tras el cifrado, mientras que la variable R corresponde a los píxeles que originalmente no tenían el valor f, pero lo adquirieron como resultado del proceso de cifrado.

$$S = k_f - Q + R \tag{6}$$

Por lo tanto, el valor esperado de los píxeles con valor f, se muestra en (7) sobre la variable S. Mediante la propiedad de linealidad del valor esperado, el resultado es la suma de los valores esperados de Q y R, que fueron calculados previamente en (4) y (5), respectivamente.

$$E[S] = k_f - k_f \times 0{,}5 + k_{255-f} \times 0{,}5 \tag{7}$$

Simplificando los resultados, se obtiene en (8) el valor esperado de los píxeles con valor k después del cifrado con la TNP, que indica que este corresponde al promedio entre la cantidad de píxeles que inicialmente tenían el valor k y aquellos con su valor simétrico $255 - k$.

$$E[S] = (k_f + k_{255-f}) \times 0{,}5 \tag{8}$$

De manera similar, podemos realizar el análisis para la frecuencia k_{255-f}, donde la variable T representa el número de píxeles en la imagen con valor $255 - f$ después de haber sido cifrada con la TNP, como se indica en (9). En este caso, se debe considerar tanto el número de píxeles que cambiaron su valor inicial f a $255 - f$, representado por la variable Q, como el número de píxeles que no cambiaron su valor inicial $255 - f$, restando de la cantidad inicial k_{255-f} con aquellos que cambiaron su valor representados por R.

$$T = Q + k_{255-f} - R \tag{9}$$

Respecto el cálculo del valor esperado de T, de manera análoga a lo realizado con la variable S, se suman los valores esperados de las variables involucradas, Q y R, como se muestra en (10), obteniendo el resultado final en (11).

$$E[T] = k_f \times 0{,}5 + k_{255-f} - k_{255-f} \times 0{,}5 \tag{10}$$

$$E[T] = (k_f + k_{255-f}) \times 0{,}5 \tag{11}$$

Como se observa en (8) y (11), los valores esperados de S y T son iguales, es decir, $E[S] = E[T]$. En otras palabras, después de cifrar la imagen con la TNP, se espera que la cantidad de píxeles con valor f sea la misma que la cantidad de píxeles con su valor simétrico $255 - f$. Además, la cantidad esperada corresponde al promedio de las frecuencias iniciales k_f, k_{255-f} para las intensidades f y $255 - f$ respectivamente.

Ejemplificando lo anterior, se presenta el caso con $f = 0$ y su respectivo valor simétrico 255, por lo que después del cifrado, se espera que las frecuencias para ambos valores sean las mismas y además el promedio entre ellas dos. Inicialmente la frecuencia para el nivel de intensidad 0 es $k_0 = 56$, mientras que la frecuencia para el valor 255 es $k_{255} = 536$, esto cuando la imagen no se ha cifrado. Lo esperado es que ambas tengan la misma frecuencia, cuyo promedio es igual a 296. En la tabla 1 se muestra el promedio de píxeles con valor 0 y 255 cifrando la figura 1 con hasta con 500 llaves diferentes y promediando el valor de cada intensidad en cada una de las resultantes 500 imágenes cifradas.

Tabla 1: Promedio de píxeles con valor 0 y 255 obtenido a partir de diversas versiones cifradas de la imagen de Baboon mediante la TNP, utilizando 50, 150, 300 y 500 llaves diferentes

Veces cifrada	Píxeles con valor 0	Píxeles con valor 255
0	56	536
50	296.9800	295.0200
150	297.9533	294.0467
300	297.1767	294.8233
500	296.8360	295.1640
Esperado	296	296

4. Resultados y discusión

En esta sección se verifica experimentalmente los resultados teóricos presentados anteriormente, con el fin de comprobar que los histogramas efectivamente adoptan una forma simétrica. Además, se analizan las limitaciones prácticas de la teoría, como la influencia en la simetría del tamaÃ±*odelbloqueseleccionadoparaelcifrado*.

4.1. Verificación de la simetría del histograma

Para ilustrar los resultados teóricos sobre la simetría del histograma, donde se espera que el número de píxeles sea el mismo para cada par de intensidades de color simétricas (es decir, 0 y 255, 1 y 254, 2 y 253, etc.), y además que dicho número sea igual al promedio de cada par, se cifró la imagen de Baboon de la figura 1(a) utilizando la TNP. El cifrado se aplicó considerando bloques de 1×1, como se muestra en la figura 1(b), y también se analizaron bloques de píxeles de 4×4, 8×8, 16×16 y 32×32, visualizados en la figura 3. La verificación de la simetría se llevó a cabo específicamente en los histogramas del canal rojo de la imagen de Baboon, los cuales se presentan en la figura 4, correspondientes a las imágenes de las figuras 1 y 3.

Para verificar la simetría de cada histograma, se aplicó una prueba de bondad de ajuste en cada uno de ellos, donde los valores esperados correspondían al promedio de cada par de intensidades simétricas, y los observados eran los proporcionados por el histograma analizado. Los resultados se presentan en la tabla 2. Para considerar que un histograma se ajusta a una distribución simétrica, el valor del estadístico χ^2 debe ser menor a 308, esto para una distribución χ^2 con 255 grados de libertad. En los bloques de menor tamaÃ±o, *específicamente* 1×1, 4×4 y 8×8, la prueba fue superada, lo que indica que, en general, el histograma puede considerarse simétrico, ya que las frecuencias obtenidas para cada intensidad son cercanas a los valores esperados según (4) y (5). Para los bloques de 16×16 y 32×32, el valor de χ indica que los histogramas no pueden considerarse simétricos. Esto se debe a que el tamaÃ±o *de los bloques influye directamente en la independencia de los ensayos de Bernoulli, una cuestión que se analiza con mayor detalle en la subse*

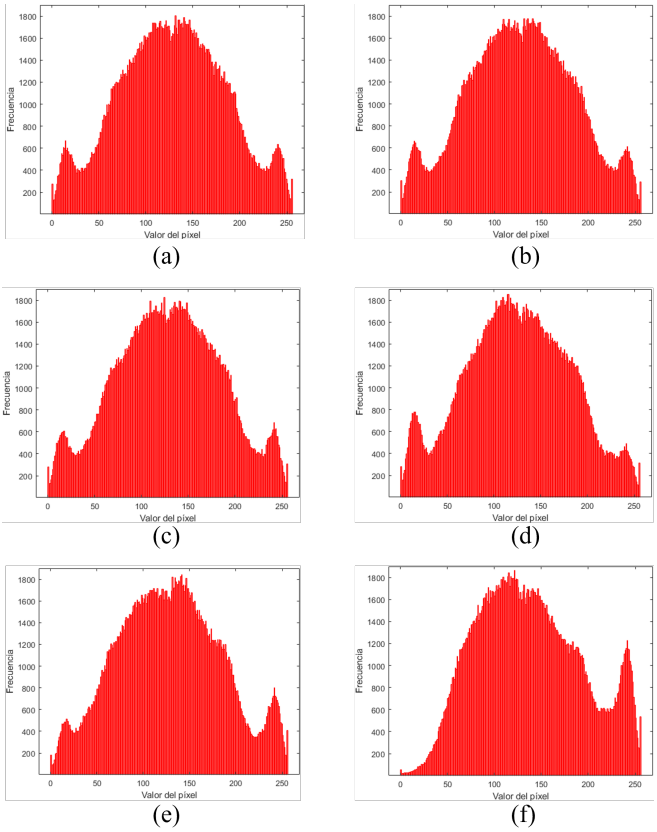


Figura 4: Histogramas del canal rojo de las imágenes cifradas de Baboon con diferentes tamaÃ±os de bloques. (a) Histograma de la Figura 1(b). (b) Histograma de la Figura 3(a). (c) His
Figura 4: Histogramas del canal rojo de las imágenes cifradas de Baboon con diferentes tam

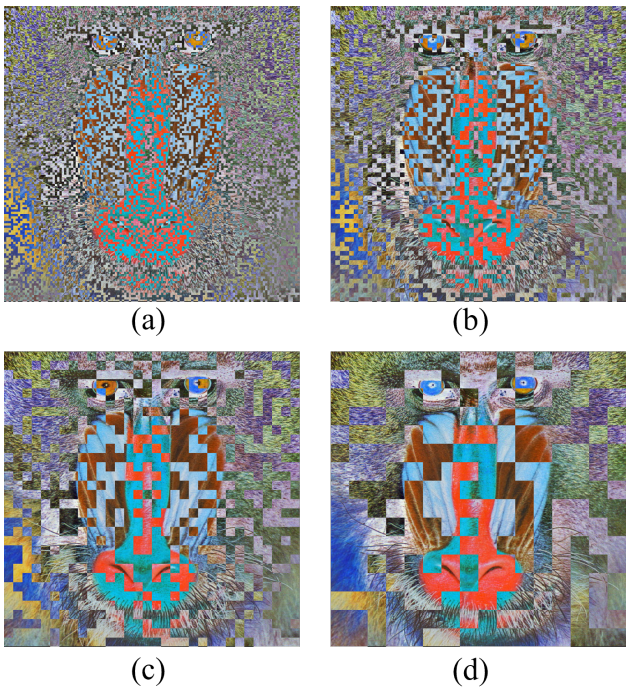


Figura 3: Cifrado de la imagen de Baboon con la TNP en diferentes tamaÃ±os de bloques. (a) Bloque de 4×4 píxeles. (b) Bloque de 8×8 píxeles. (c) Bloque de 16×16 píxeles. (d) Bloque de 32×32 píxeles.

Tabla 2: Resultados de la prueba de bondad y ajuste respecto a la simetría de los histogramas presentados en la figura 4

TamaÃ±o *bloque*	Valor χ	Cumple con $\chi < 291$
1×1	128.5	Sí
4×4	180.9	Sí
8×8	190.3	Sí
16×16	1759.5	No
32×32	2115.2	No

4.2. La independencia de los ensayos por tamaÃ±o de bloque

En la subsección 3.1 se abordó un experimento binomial aplicado a los píxeles, donde cada ensayo consistía en observar el valor de un píxel, y en el cuarto punto se menciona la independencia de los ensayos, es decir, que cada píxel pudiera cambiar su valor sin influir en el valor de los píxeles vecinos. No obstante, dado que la TNP realiza el cifrado por bloques, dos o más píxeles con el mismo valor pueden encontrarse en el mismo bloque. De esta manera, si uno de ellos cambia su valor como resultado del cifrado, automáticamente los demás píxeles dentro del mismo bloque también lo harán. Esto sugiere que los píxeles con el mismo valor no necesariamente habrán sido afectados de manera independiente, ya que si la TNP indica que no deben cambiar su valor, esta instrucción se aplica a todos los píxeles del bloque, lo que genera una dependencia en la manera en que se modifican, al menos entre los píxeles dentro de un mismo bloque.

Además, como se observa en la tabla 3, a medida que el tamaÃ±*odelbloqueaumenta, tambiénlohaceelnúmerodepíxelesconelmismovalordent*[illegible]*lo, enbloquesde*4×4, considerando únicamente aquellos que contienen al menos un píxel con valor 0, se encuentra un promedio de 1.6 píxeles con ese valor. Sin embargo, en bloques de 32 × 32, el promedio asciende a 5 píxeles con valor 0, aproximadamente el 10 % de k_0. Estos píxeles cambian o se mantienen simultáneamente, según lo determine la transformada, lo que podría influir en su comportamiento independiente.

Un hecho similar ocurre en los bloques que contienen al menos un píxel con valor 255. En bloques de 4×4, se encuentra un promedio de un píxel por bloque, por lo que la transformada afecta a un único píxel a la vez. No obstante, a medida que el tamaÃ±*odelbloqueaumenta, tambiénlohacelacantidaddepíxelesconvalor*255, *alcanzandounpromediode*15*píxelesenlosbloquesde*32×32.

Sin embargo, el análisis de la independencia de los ensayos de Bernoulli puede considerarse a nivel de bloque y no únicamente a nivel de píxel, dado que la transformada cifra cada bloque de manera independiente. En este contexto, para lograr una simetría en el histograma, es necesario que los píxeles con un mismo valor se distribuyan de manera uniforme en todos los bloques donde aparecen. Es decir, no debe haber bloques que concentren solo un píxel con ese color mientras otros bloques concentran un porcentaje significativamente mayor. Este hecho sería equivalente a que los píxeles se comporten de manera independiente, ya que si en un bloque cierto número de píxeles cambia, en otro bloque es posible que no lo hagan en la misma proporción, manteniendo así un equilibrio entre ellos. Para evaluar cómo se distribuyen las intensidades en todos los bloques en los que aparecen se analizó su varianza en la tabla 4.

Tabla 3: Promedio del número de píxeles con valor 0 y 255 por bloque considerando solo aquellos bloques que contienen al menos un píxel con ese valor

TamaÃ±*obloque*	Promedio valor 0	Promedio valor 255
1 × 1	1	1
4 × 4	1.6970	1.6242
8 × 8	2.6667	3.0455
16 × 16	3.7333	6.8718
32 × 32	5.0909	15.3143

Tabla 4: Varianza del número de píxeles con valor 0 y 255 por bloque considerando solo aquellos bloques que contienen al menos un píxel con ese valor

TamaÃ±*obloque*	Promedio valor 0	Promedio valor 255
1 × 1	0	0
4 × 4	0.5928	1.0620
8 × 8	2.0333	9.3351
16 × 16	7.7810	69.7756
32 × 32	11.4909	533.5160

4.3. La influencia del tamaÃ±odelaimagenenlasimetría

El grado de simetría de un histograma también puede verse influenciado por el tamaÃ±*odelaimagen.Laspruebasanterioressere*[illegible] 512×512 píxeles. A continuación, se presenta un análisis basado en dos imágenes de menor tamaÃ±*o*, 256×256 píxeles. La principal diferencia con respecto al caso anterior es que el tamaÃ±*odelamuestraparalosensayossereduceaunacuartaparte, yaq*[illegible]

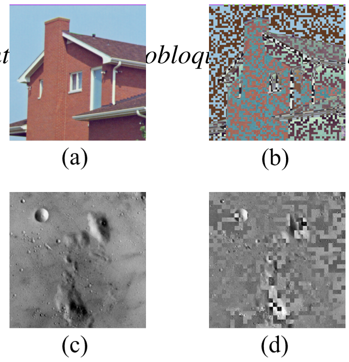


Figura 5: Cifrado de imágenes de 256×256 píxeles con la TNP en diferentes ta-[illegible] píxeles. (c) Imagen en escala de grises de Moon. (d) Cifrado de (c) en bloques de 8×8 píxeles.

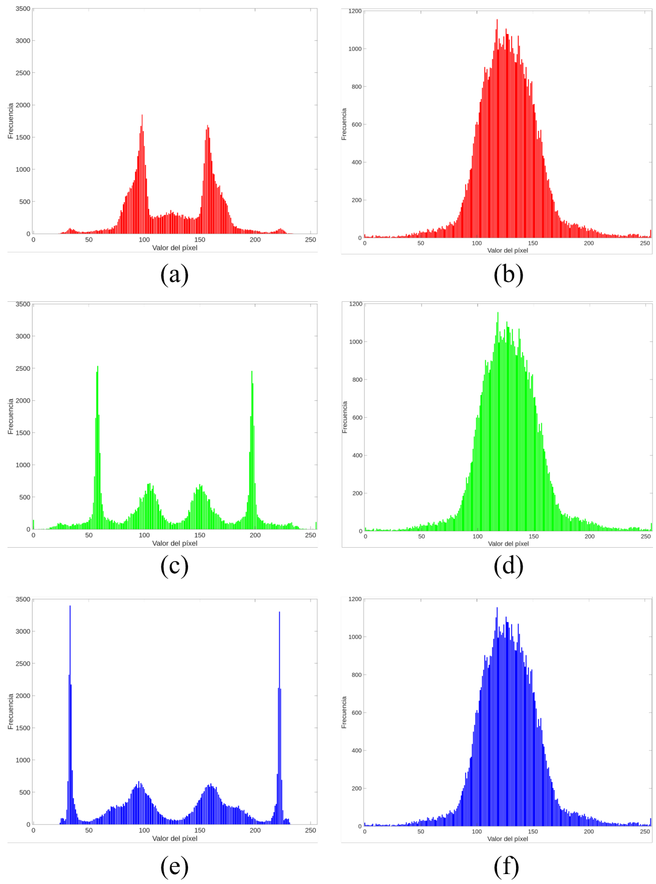


Figura 6: Histogramas de las imágenes cifradas de la figura 5. (a) Histograma del canal rojo de la Figura 5(b). (b) Histograma del canal rojo de la Figura 5(d). (c) Histograma del canal verde de la Figura 5(b). (d) Histograma del canal verde de la Figura 5(d). (e) Histograma del canal azul de la Figura 5(b). (f) Histograma del canal azul de la Figura 5(d).

La imagen de la luna, al ser en escala de grises, presenta los mismos histogramas en todos sus canales de color, como se observa en la figura 6(b,d,f). Por otro lado, los histogramas de la [illegible] canales, también visibles en la figura 6(a,c,e).

Para cuantificar la simetría de cada histograma, se aplicó la prueba de bondad de ajuste. Los resultados, presentados en [illegible]

del cifrado por bloques de 4×4 píxeles aún aprueban la prueba de simetría, mientras que los de la figura 6(b,d,f) provenientes de bloques de 8×8 ya no cumplen con este criterio. Esta situación contrasta con la imagen de Baboon, que sí logró mantener la simetría aún al cifrarla con bloques de 8×8 píxeles. Por tanto, a medida que aumenta el tamaÃ±o de la muestra, es decir, el número de píxeles, la simetría del histo[illegible]or, a[illegible] se más gra

Tabla 5: Resultados de la prueba de bondad y ajuste respecto a la simetría de los histogramas presentados en la figura 6

Histograma	Valor χ	Cumple con $\chi < 291$
(a)	198.6	Sí
(c)	163.9	Sí
(e)	129.4	Sí
(b)	337.5	No
(d)	337.5	No
(f)	337.5	No

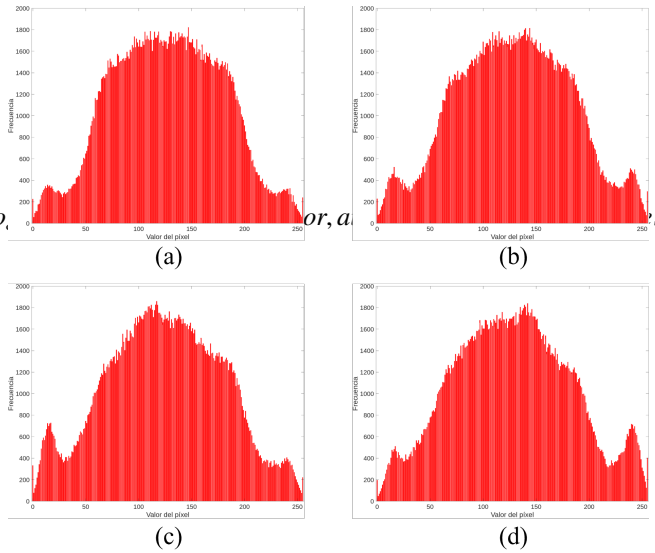


Figura 7: Histogramas de las imágenes comprimidas con JPEG de la Figura 3. (a) Histograma del canal rojo de la Figura 3(a) comprimida. (b) Histograma del canal rojo de la Figura 3(b) comprimida. (c) Histograma del canal rojo de la Figura 3(c) comprimida. (d) Histograma del canal rojo de la Figura 3(d) comprimida.

4.4. *Impacto de la compresión con pérdida en la simetría del histograma*

La compresión con pérdida de información también impacta la simetría del histograma. En particular, se analizaron las imágenes de la figura 3, las cuales, al ser cifradas, mantenían histogramas con una forma simétrica, como se analizó en la tabla 2. Sin embargo, cuando estas imágenes se comprimen con pérdida al ser almacenadas en formato JPEG, se pierden datos, y los valores originales de los píxeles son reemplazados por otros similares, pero no idénticos. Esto afecta directamente la composición del histograma dado que la compresión altera su forma.

Los histogramas del canal rojo resultantes de las imágenes de la figura 3, comprimidas como JPEG, se muestran en la figura 7. Visualmente, la simetría sigue siendo predominante. No obstante, los histogramas fueron evaluados para comparar los niveles de color simétricos, donde lo esperado era que mantuvieran frecuencias equivalentes. Los resultados se muestran en la tabla 6, donde los bloques de 4×4 y 8×8 lograron pasar la prueba de bondad y ajuste nuevamente. Sin embargo, incluso en estos bloques, y particularmente en los de 16 y 32 píxeles, se observó un aumento en el valor de χ, lo que indica que la compresión con pérdida redujo la apariencia simétrica del histograma. A pesar de ello, para los histogramas de las imágenes cifradas bloques más peqAÃ±os, la simetría aún puede considerarse predominante.

Tabla 6: Resultados de la prueba de bondad y ajuste respecto a la simetría de los histogramas después de comprimir las imágenes de la figura 3

Bloque	Valor χ	Incremento	Cumple con $\chi < 291$
4×4	191.7	6 %	Sí
8×8	223.5	17 %	Sí
16×16	1780.1	1 %	No
32×32	2153.2	2 %	No

4.5. *Comparación de simetría con otras técnicas de cifrado*

Aunque el objetivo principal de una imagen cifrada es lograr un histograma uniforme, cuando se alcanza esta uniformidad, el histograma también tiende a adquirir una forma simétrica. En esta sección se analiza la influencia de una técnica ampliamente utilizada en el cifrado de imágenes: la sustitución. La sustitución seleccionada para su análisis y comparación con la TNP es la implementada en el estándar de cifrado AES.

La figura 8 muestra el resultado del cifrado de la imagen Baboon mediante esta técnica y los histogramas generados a partir de dicha imagen cifrada. Se observa que la simetría en los histogramas disminuye en comparación con los obtenidos al aplicar la TNP. Para cuantificar el grado de simetría del histograma, se empleó la prueba de bondad de ajuste, cuyos resultados se presentan en la tabla 7. Ninguno de los tres histogramas pudo considerarse simétrico, ya que ninguno logró superar la prueba. Asimismo, dado que la sustitución es una función biyectiva con una relación no lineal, los píxeles cifrados mediante esta técnica no pueden ser procesados por compresión con pérdida. Esto se debe a que, tras la descompresión, sería imposible recuperar los valores originales con precisión. Por el contrario, la TNP no requiere la conservación exacta de los valores originales tras la descompresión, lo que la hace compatible con técnicas de compresión con pérdida.

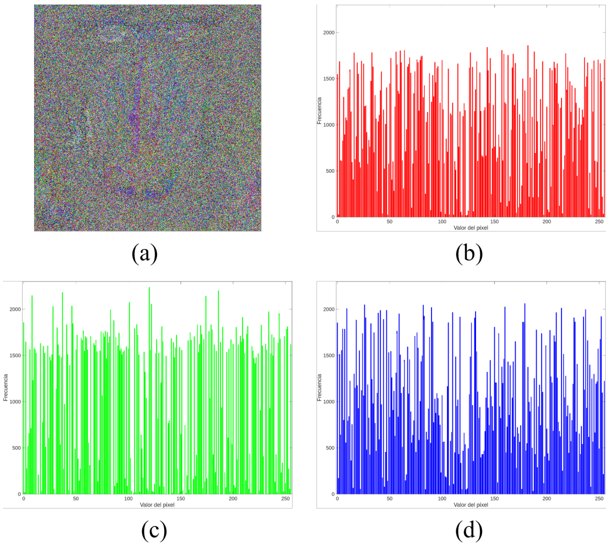


Figura 8: Cifrado de la imagen de Baboon con la caja de sustitución de AES. (a) Imagen cifrada con la sustitución. (b) Histograma del canal rojo de (a). (c) Histograma del canal verde de (a). (d) Histograma del canal azul de (a).

Tabla 7: Resultados de la prueba de bondad y ajuste respecto a la simetría de los histogramas presentados en la figura 8

Canal de color	Valor χ	Cumple con $\chi < 291$
Rojo	40330.9	No
Verde	66617.9	No
Azul	40511.7	No

5. Conclusiones

En el presente trabajo se analizó la simetría en los histogramas de imágenes cifradas con la TNP. La simetría observada en el histograma se debe a que el valor esperado del número de píxeles para cada par de niveles simétricos (por ejemplo, 0 y 255, 1 y 254, 2 y 253, etc.) es idéntico. Esto genera una reflexión horizontal respecto a las intensidades centrales (127 y 128). Además, el valor esperado para cada par de niveles simétricos corresponde a su promedio. En el campo del cifrado de imágenes, donde se busca una distribución uniforme en el histograma, se debe considerar cómo afecta este promedio para lograr dicho objetivo. Al cifrar la imagen con la TNP, se puede describir el cambio en los valores de los píxeles como un experimento binomial, donde la cantidad de píxeles con cualquier valor específico se representa mediante una variable aleatoria con distribución binomial. No obstante, la independencia de los ensayos, que en este contexto corresponde al cambio en el valor de cada píxel, puede verse afectada por el tamaÃ±odelbloqueutilizadoenelcifradoconlaTNP.Enbloquesmásgrandesde8×8, es probable que haya varios píxeles con el mismo valor dentro de un mismo bloque, lo que introduce dependencia entre esos píxeles al su valor. Además, otros factores que en conjunto pueden afectar la simetría de los histogramas es el tamaÃ±odelaimagen,específicamentelacantidaddepíxeles,debidoaqueinfluyeenlacantidaddeensayosdisponiblesenelexperimento.Asimism

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional de México (Secretaría Académica, SIP, CIC y CIDETEC) y al CONAHCyT por su apoyo en este trabajo.

Referencias

Ahmad, I. y Shin, S. (2023). Perceptual encryption-based privacy-preserving deep learning for medical image analysis. En *2023 International Conference on Information Networking (ICOIN)*, pp. 224–229, Bangkok, Thailand.

Aryal, A., Imaizumi, S., Horiuchi, T., y Kiya, H. (2017). Integrated algorithm for block-permutation-based encryption with reversible data hiding. En *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pp. 203–208, Kuala Lumpur, Malaysia.

Aryal, A., Imaizumi, S., Horiuchi, T., y Kiya, H. (2018). Integrated model of image protection techniques. *J. Imaging*, 4(1):1.

Chuman, T., Sirichotedumrong, W., y Kiya, H. (2019). Encryption-then-compression systems using grayscale-based image encryption for jpeg images. *IEEE Trans. Inf. Forensic Secur.*, 14(6):1515–1525.

El Saj, R., Sedgh Gooya, E., Alfalou, A., y Khalil, M. (2021). Privacy-preserving deep neural network methods: Computational and perceptual methods–an overview. *Electronics*, 10(11):1367.

Ghadirli, H. M., Nodehi, A., y Enayatifar, R. (2019). An overview of encryption algorithms in color images. *Signal Process*, 164:163–185.

Imaizumi, S. y Kiya, H. (2018). A block-permutation-based encryption scheme with independent processing of rgb components. *IEICE Trans. Inf. Syst.*, E101D(12):3150 ? 3157.

Imaizumi, S., Ogasawara, T., y Kiya, H. (2017). Block-permutation-based encryption scheme with enhanced color scrambling. En Sharma, P. y Bianchi, F. M., editores, *Image Analysis*, pp. 562–573, TromsÃ¸, Norway. Springer International Publishing.

Katsis, A. y Toman, B. (1999). Bayesian sample size calculations for binomial experiments. *J. Stat. Plan. Infer.*, 81(2):349–362.

Kenta, K., Masanori, K., Shoko, I., Sayaka, S., y Hitoshi, K. (2015). An encryption-then-compression system for jpeg/motion jpeg standard. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E98.A(11):2238–2245.

Li, P. y Lo, K.-T. (2020). Survey on jpeg compatible joint image compression and encryption algorithms. *IET Signal Process.*, 14:475–488.

Maungmaung, A. y Kiya, H. (2021). A protection method of trained cnn model with a secret key from unauthorized access. *APSIPA Trans. Signal Inf. Process.*, 10:e10.

Motomura, R., Imaizumi, S., y Kiya, H. (2023). Reversible data hiding in compressible encrypted images with capacity enhancement. *APSIPA Trans. Signal Inf. Proc.*, 12(1):e31.

Musanna, F., Dangwal, D., y Kumar, S. (2022). Novel image encryption algorithm using fractional chaos and cellular neural network. *J. Ambient Intell. Humanized Comput.*, 13(4):2205–2226.

Rolke, W. y Gongora, C. G. (2021). A chi-square goodness-of-fit test for continuous distributions against a known alternative. *Computat. Stat.*, 36(3):1885–1900.

Shimizu, K., Suzuki, T., y Kameyama, K. (2018). Cube-based encryption-then-compression system for video sequences. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E101.A(11):1815–1822.

Singh, K. N. y Singh, A. K. (2022). Towards integrating image encryption with compression: A survey. *ACM Trans. Multimed. Comput. Commun. Appl.*, 18(3):89.

Sirichotedumrong, W., Kinoshita, Y., y Kiya, H. (2019). Pixel-based image encryption without key management for privacy-preserving deep neural networks. *IEEE Access*, 7:177844–177855.

Taufiq, I., Sulistyowati, F., y Usman, A. (2020). Binomial distribution at high school: An analysis based on learning trajectory. *J. Phys.: Conf. Ser.*, 1521(3):032087.

Zhang, B., Xiao, D., y Xiang, Y. (2021). Robust coding of encrypted images via 2d compressed sensing. *IEEE Trans. Multimed.*, 23:2656–2671.