

Research Article

Evaluación del Algoritmo F5 aplicado en la Esteganografía de imágenes JPEG: Un análisis basado en métricas de calidad

Evaluation of the F5 Algorithm applied in JPEG image steganography: An analysis based on quality metrics



Boné-Andrade, Miguel Fabricio ¹



<https://orcid.org/0000-0002-8635-1869>



miguel.bone@utelvt.edu.ec



Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador, La Concordia



Mendoza-Loor, José Javier ²



<https://orcid.org/0000-0001-8623-872X>



jose.mendoza.loor@utelvt.edu.ec



Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador, La Concordia



Núñez-Freire, Luis Alfonso ³



<https://orcid.org/0000-0001-9759-2003>



luis.nunez@utelvt.edu.ec



Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador, La Concordia

Autor de correspondencia ¹



DOI / URL: <https://doi.org/10.55813/gaea/jessr/v5/n2/194>

Resumen: El estudio explora la aplicación del algoritmo F5 en imágenes JPEG para evaluar su rendimiento al momento de ocultar información sin que se comprometa la calidad visual de las imágenes. Se emplean técnicas de compresión basadas en la Transformada Discreta del Coseno (DCT) y la codificación matricial que permiten minimizar las alteraciones perceptibles que se puedan presentar. La metodología incluye la segmentación de la imagen en bloques de 8x8 píxeles, la cuantización de los coeficientes y la evaluación de la calidad de la imagen mediante las métricas PSNR, MSE y SSIM. Los experimentos fueron realizados con imágenes en escala de grises, ocultando mensajes de distinta longitud. Los resultados muestran que el algoritmo mantiene valores elevados de PSNR y SSIM, garantizando que la distorsión sea imperceptible. Se observa una relación inversa entre el tamaño del mensaje y la calidad visual, aunque sin comprometer la estructura de la imagen. El estudio concluye que el algoritmo F5 es eficaz para la esteganografía en imágenes JPEG, pero su rendimiento es susceptible a mejora mediante la aplicación de técnicas híbridas como DCT-SVD y la cuantización adaptativa. Se destaca la necesidad de integrar enfoques de redes neuronales para fortalecer la resistencia ante ataques de detección.

Palabras clave: esteganografía, codificación de datos, algoritmo F5, transformada discreta del coseno (DCT), seguridad de la información.



Check for updates

Received: 20/Mar/2025

Accepted: 15/Abr/2025

Published: 30/Abr/2025

Cita: Boné-Andrade, M. F., Mendoza-Loor, J. J., & Núñez-Freire, L. A. (2025). Evaluación del Algoritmo F5 aplicado en la Esteganografía de imágenes JPEG: Un análisis basado en métricas de calidad. *Journal of Economic and Social Science Research*, 5(2), 144-158. <https://doi.org/10.55813/gaea/jessr/v5/n2/194>

Journal of Economic and Social Science Research (JESSR)

<https://economicsocialresearch.com>

info@editoriagrupo-aea.com

Nota del editor: Editorial Grupo AEA se mantiene neutral con respecto a las reclamaciones legales resultantes de contenido publicado. La responsabilidad de información publicada recae enteramente en los autores.

© 2025. Este artículo es un documento de acceso abierto distribuido bajo los términos y condiciones de la **Licencia Creative Commons, Atribución-NoComercial 4.0 Internacional**.



Abstract:

The study explores the application of the F5 algorithm on JPEG images to evaluate its performance in hiding information without compromising the visual quality of the images. Compression techniques based on the Discrete Cosine Transform (DCT) and matrix coding are used to minimize the perceptible alterations that may occur. The methodology includes image segmentation in 8x8 pixel blocks, quantization of coefficients and evaluation of image quality using PSNR, MSE and SSIM metrics. The experiments were performed with grayscale images, hiding messages of different lengths. The results show that the algorithm maintains high values of PSNR and SSIM, ensuring that the distortion is imperceptible. An inverse relationship between message size and visual quality is observed, although without compromising image structure. The study concludes that the F5 algorithm is effective for steganography on JPEG images, but its performance is susceptible to improvement through the application of hybrid techniques such as DCT-SVD and adaptive quantization. The need to integrate neural network approaches to strengthen resistance to detection attacks is highlighted.

Keywords: steganography, data encryption, F5 algorithm, discrete cosine transform (DCT), information security.

1. Introducción

En la actualidad digital en la que vivimos, la seguridad de la información se ha convertido en un eslabón que continuamente se está estudiando por la necesidad de proteger la privacidad e integridad de los datos en los diferentes entornos de comunicación, como las comunicaciones en línea, el almacenamiento en la nube y las transacciones financieras, etc. Entre las diversas técnicas empleadas para garantizar la confidencialidad e integridad de la información a transmitir se encuentra la esteganografía, la cual se ha consolidado como un método eficaz al momento de ocultar la información en archivos multimedia, sin que se vean alterados de una manera significativa tanto en su apariencia como en su funcionalidad (Petitcolas et al., 1999; Fridrich, 2009). A diferencia de la criptografía que protege el contenido de la información mediante cifrado, la esteganografía busca ocultar la existencia misma del mensaje, dificultando su detección por parte de terceros. Este enfoque permite la transmisión de información de una manera discreta, evitando sospechas o atrayendo atención innecesaria sobre los datos transmitidos.

El formato de imagen JPEG es uno de los más utilizados en esteganografía, debido a su amplia adopción y su eficiencia en la compresión de datos. Este formato emplea la Transformada Discreta del Coseno para representar imágenes en el dominio de la frecuencia, lo que permite reducir el tamaño de los archivos eliminando información irrelevante para la percepción visual (Ahmed et al., 1974; Wallace, 1991). Sin embargo, la inserción de datos ocultos en estos coeficientes puede afectar la calidad de la imagen si no se gestiona adecuadamente. Para abordar este desafío, en 2001

Westfeld desarrolló el algoritmo F5, un método de esteganografía específicamente diseñado para imágenes JPEG. Este algoritmo utiliza la codificación matricial, optimizando la capacidad de ocultamiento y mejorando la resistencia a la detección, al tiempo que minimiza la distorsión visual en la imagen esteganografiada.

Si bien el algoritmo F5 ofrece ventajas significativas, también presenta ciertas limitaciones. Una de ellas es la reducción de la capacidad de inserción de datos debido al fenómeno de shrinkage, lo que disminuye la cantidad de información que se puede ocultar sin afectar la calidad visual de la imagen. Además, con los avances en técnicas de análisis forense digital y el desarrollo de métodos de detección de esteganografía cada vez más sofisticados, resulta crucial evaluar la efectividad actual del algoritmo F5 y explorar posibles mejoras para optimizar su desempeño frente a nuevas estrategias de análisis.

Estudios recientes han propuesto diversas estrategias para mejorar la capacidad y seguridad de la esteganografía JPEG. Entre ellas, destaca la combinación del algoritmo F5 con la descomposición en valores singulares, lo que permite distribuir los datos ocultos en componentes de baja frecuencia y aumentar su resistencia a la detección (Banik y Bandyopadhyay, 2016; Lu et al., 2015). Asimismo, el uso de tablas de cuantización adaptativas ha demostrado ser una solución efectiva para equilibrar la calidad visual y la capacidad de ocultamiento, permitiendo una inserción más eficiente sin degradar significativamente la imagen (Jiang et al., 2014).

El desarrollo de enfoques híbridos ha abierto nuevas oportunidades para mejorar la seguridad en esteganografía. Técnicas como la modulación de diferencia de incrustación permiten distribuir los datos ocultos en los coeficientes DCT con modificaciones mínimas, garantizando una mayor imperceptibilidad (Lin et al., 2024). Además, la integración de métodos de aprendizaje automático y redes neuronales ha dado lugar a estrategias más adaptativas, optimizando la inserción y extracción de datos en función de las características específicas de cada imagen (Zeng et al., 2024; Hendrych & Ličev, 2020).

El presente estudio tiene como objetivo primario evaluar la efectividad existente del algoritmo F5 cuando es aplicado en la esteganografía de imágenes JPEG. Para medir esta efectividad, se analizará el rendimiento que existe al momento de insertar la información a ocultar y la calidad visual resultante en cada una de las imágenes que contienen dichos datos ocultos. Para ello, se implementará el algoritmo F5 en un entorno experimental totalmente controlado y se emplearán las métricas de calidad PSNR, MSE y SSIM, las cuales permitirán cuantificar el nivel de distorsión que se genera en cada una de las imágenes al momento de la inserción de los mensajes ocultos (Almohammad y Ghinea, 2010). Los resultados obtenidos permitirán validar si el algoritmo F5 es eficiente en la inserción de la información e identificar qué oportunidades de mejora existen mediante la integración de técnicas modernas que permitan optimizar la seguridad de la información y su eficiencia.

2. Materiales y métodos

El presente estudio adopta un enfoque cuantitativo y experimental, centrado en la evaluación objetiva del rendimiento del algoritmo F5 en entornos controlados. Se trata de una investigación aplicada, ya que busca comprobar la utilidad de una técnica de esteganografía en contextos reales de transmisión de información.

Para el análisis, se emplearon 15 imágenes JPEG en escala de grises de 512x512 píxeles, seleccionadas de manera intencional para asegurar variedad en patrones visuales, como texturas complejas y regiones homogéneas. Estas imágenes se utilizaron como muestra no probabilística, de tipo intencional, dada la naturaleza técnica del estudio y la necesidad de condiciones homogéneas para la comparación.

La implementación se realizó en Python 3.10, utilizando bibliotecas como NumPy, OpenCV, Matplotlib y scikit-image, lo que permitió un control preciso sobre cada paso de la inserción y extracción de datos. La aplicación fue desarrollada por los autores, garantizando una ejecución transparente del algoritmo. No se emplearon instrumentos de recolección tradicionales; en su lugar, el software desarrollado actúa como herramienta experimental.

En cuanto a las métricas empleadas, se optó por indicadores ampliamente aceptados en la literatura: MSE, PSNR y SSIM (Almohammad & Ghinea, 2010; Baziyad et al., 2021), que permiten una valoración cuantitativa de la distorsión, la relación señal-ruido y la similitud estructural entre la imagen original y la modificada.

Desde la perspectiva ética, el estudio no involucra datos personales ni imágenes con derechos restringidos, se trabajó exclusivamente con archivos de libre uso para fines académicos. No se vulneró la privacidad de ningún individuo ni se manipuló información confidencial, por lo cual el riesgo ético es nulo.

Para llevar a cabo el presente estudio se utilizaron los siguientes elementos básicos: La Transformada Discreta del Coseno (DCT) permite descomponer una imagen en componentes de frecuencia mediante la división en bloques de 8x8 píxeles, y se define

$$C(u, v) = \frac{1}{4} \alpha(u) \alpha(v) \sum_{x=0}^7 \sum_{y=0}^7 f(x, y) \cos \left(\frac{(2x+1)u\pi}{16} \right) \cos \left(\frac{(2y+1)v\pi}{16} \right)$$

matemáticamente como en la ecuación (1) (Ahmed et al., 1974):

Donde $\alpha(u)$ y $\alpha(v)$ son factores de normalización. La IDCT, que permite reconstruir completamente la imagen a partir de sus coeficientes, se define como sigue en la ecuación (2) (Ahmed et al., 1974):

$$f(x, y) = \frac{1}{4} \sum_{u=0}^7 \sum_{v=0}^7 \alpha(u) \alpha(v) C(u, v) \cos \left(\frac{(2x+1)u\pi}{16} \right) \cos \left(\frac{(2y+1)v\pi}{16} \right)$$

En la compresión JPEG, los coeficientes DCT son cuantizados, como se indica en la ecuación (3) (Almohammad et al., 2009):

$$C_q(u, v) = \text{round} \left(\frac{C(u, v)}{Q(u, v)} \right)$$

Donde $C_q(u, v)$ representa el coeficiente cuantizado y $Q(u, v)$ es el valor de la tabla de cuantificación.

El algoritmo F5 utiliza la DCT y una codificación matricial para minimizar modificaciones en los coeficientes DCT de los bloques de 8x8 píxeles, lo que optimiza la seguridad del mensaje oculto (Westfeld, 2001). La codificación en el algoritmo F5 puede expresarse matemáticamente en la ecuación (4):

$$C'_q(u, v) = \begin{cases} C_q(u, v) + 1, & \text{si } m = 1 \text{ y } C_q(u, v) \text{ es par} \\ C_q(u, v) - 1, & \text{si } m = 0 \text{ y } C_q(u, v) \text{ es impar} \\ C_q(u, v), & \text{en caso contrario} \end{cases}$$

Donde $C'_q(u, v)$ es el coeficiente modificado y m el bit del mensaje.

Se divide la imagen en bloques de 8x8 píxeles, se aplica la DCT y se cuantizan los coeficientes para prepararlos para la inserción del mensaje.

Algoritmo 1 preprocesamiento de imagen

```

for cada bloque de 8x8 en la imagen do
    Aplicar DCT al bloque
    Cuantizar los coeficientes DCT
End for
  
```

El mensaje se convierte en bits y se seleccionan posiciones aleatorias en los coeficientes DCT para la inserción, siguiendo el algoritmo F5.

Algoritmo 2 Inserción del mensaje

```

Convertir el mensaje a una cadena de bits
For cada bit de mensaje do
    Seleccionar una posición en el bloque DCT
    If paridad del coeficiente DCT no coincide con el bit then
        Modificar el coeficiente para ajustar la paridad
    End if
End for
  
```

Para recuperar el mensaje oculto, se analizan los coeficientes DCT de cada bloque y se reconstruye el mensaje bit a bit.

Algoritmo 3 Extracción del mensaje

For cada bloque 8x8 en la imagen esteganografiada

Calcular el DCT del bloque

Recuperar bit del mensaje según la paridad del coeficiente

End for

Convertir bits a caracteres para reconstruir el mensaje

Para evaluar la calidad visual de la imagen esteganografiada, se emplean las métricas PSNR, MSE y SSIM:

- MSE (Mean Squared Error): Esta métrica mide el error promedio entre los valores de píxeles de la imagen original y la esteganografiada (Almohammad y Ghinea, 2010).

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [f(i, j) - g(i, j)]^2$$

- PSNR (Peak Signal-to-Noise Ratio): Relaciona el MSE con la calidad de la imagen (Almohammad y Ghinea, 2010).

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX^2}{MSE} \right)$$

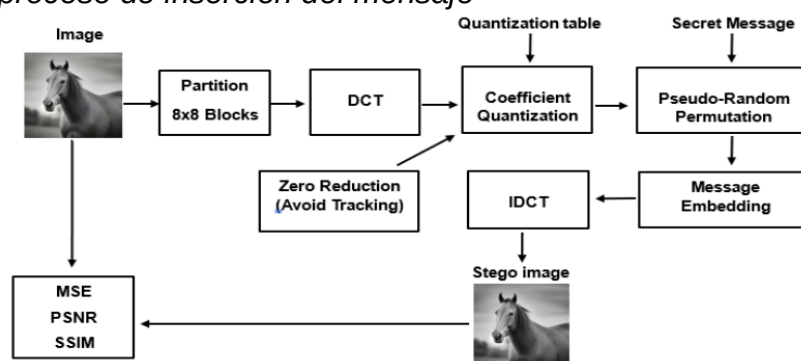
- SSIM (Structural Similarity Index): Evalúa la similitud estructural entre dos imágenes (Baziyad et al., 2021).

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

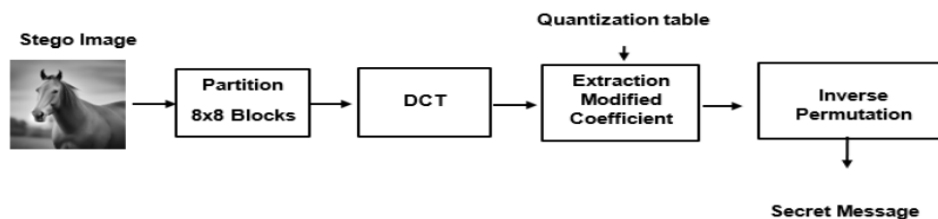
El desarrollo de la aplicación para la inserción del mensaje a ocultar se basó en el diagrama de la Figura 1 y para la extracción del mensaje oculto en el diagrama de la Figura 2.

Figura 1

Diagrama del proceso de inserción del mensaje



Nota: Autores (2025).

Figura 2*Diagrama del proceso de extracción del mensaje**Nota:* Autores (2025).

En la Figura 3, se encuentra la interfaz del programa diseñado para la implementación del Algoritmo F5. La interfaz que se encuentra a la izquierda permite la inserción del mensaje a ocultar y la interfaz de la derecha permite extraer el mensaje que se encuentra oculto.

Figura 3*Interfaz de la aplicación del algoritmo F5 desarrollada en Python**Nota:* Autores (2025).**Figura 4***Imágenes bases empleadas en cada experimento**Nota:* (Autores, 2025).

Las imágenes que fueron empleadas en los experimentos se muestran en la figura 4. Entre las imágenes seleccionadas en su gran mayoría se encuentran paisajes y animales. Esta variedad garantiza que los resultados sean de aplicación general y que el algoritmo F5 sea suficientemente evaluado en diversas circunstancias visuales.

Se ocultó tres mensajes de diferentes longitud y complejidad en cada imagen:

1. "Hello": Mensaje corto.
2. "Hello Mund0": Mensaje medio con caracteres alfanuméricos.
3. "Hello Mund0 1234@": Mensaje largo con caracteres especiales.

En cada uno de los experimentos se utilizó las quince imágenes base dividiendo cada imagen en bloques de 8x8 pixeles, lo que permite garantizar la robustez de los resultados obtenidos.

3. Resultados

3.1. Evaluación del desempeño del algoritmo F5

La evaluación del algoritmo F5 sobre las quince imágenes JPEG seleccionadas permitió analizar cómo varía la calidad visual cuando se insertan mensajes de diferente longitud. Las métricas utilizadas (MSE, PSNR y SSIM) evidencian que existe una relación directa entre la cantidad de datos ocultos y el grado de distorsión introducida en la imagen. A mayor longitud del mensaje, los valores de MSE tienden a incrementarse, mientras que los de PSNR disminuyen progresivamente (ver Tabla 1).

Un hallazgo destacable es que los valores de SSIM se mantuvieron consistentemente altos, superando el 0.98 en la mayoría de los casos, lo que indica que la estructura general de las imágenes esteganografiadas se conserva prácticamente intacta. Esta métrica, diseñada para evaluar la similitud perceptual, sugiere que las alteraciones introducidas por el algoritmo son mínimas y, en muchos casos, imperceptibles al ojo humano.

Tabla 1

Métricas de calidad visual para diferentes mensajes ocultos en imágenes JPEG

Imagen	Hello (MSE, PSNR, SSIM)	Hello Mund0 (MSE, PSNR, SSIM)	Hello Mund0 1234@ (MSE, PSNR, SSIM)
Árbol	0.3009, 53.35 dB, 0.9991	0.5936, 50.40 dB, 0.9978	0.9511, 48.35 dB, 0.9961
Caballo	0.0933, 58.43 dB, 0.9993	0.1588, 56.12 dB, 0.9987	0.3180, 53.11 dB, 0.9979
Carretera	0.4086, 52.02 dB, 0.9984	0.8270, 48.95 dB, 0.9968	1.2099, 47.30 dB, 0.9954
Cebra	0.3144, 53.15 dB, 0.9972	0.6029, 50.33 dB, 0.9960	0.9741, 48.24 dB, 0.9931
Flores	0.3199, 53.08 dB, 0.9994	0.6566, 49.96 dB, 0.9988	0.9683, 48.27 dB, 0.9982
Gato1	0.1994, 55.13 dB, 0.9981	0.3409, 52.80 dB, 0.9974	0.5460, 50.76 dB, 0.9942
Gato2	0.1477, 56.44 dB, 0.9974	0.3805, 52.32 dB, 0.9964	0.5336, 50.85 dB, 0.9948
Montaña	0.0692, 59.73 dB, 0.9997	0.1292, 57.02 dB, 0.9994	0.2033, 55.05 dB, 0.9990
Lena	0.1928, 55.28 dB, 0.9991	0.3950, 52.17 dB, 0.9983	0.5770, 50.52 dB, 0.9972
León	0.1752, 55.70 dB, 0.9987	0.3586, 52.58 dB, 0.9969	0.5868, 50.45 dB, 0.9944

Montaña Lago	0.3790, 52.34 dB, 0.9980	0.7650, 49.29 dB, 0.9961	1.0668, 47.84 dB, 0.9935
Ovejas	0.2105, 54.89 dB, 0.9993	0.3988, 52.12 dB, 0.9987	0.5878, 50.43 dB, 0.9980
Paisaje1	0.3640, 52.52 dB, 0.9987	0.7572, 49.34 dB, 0.9973	1.0819, 47.78 dB, 0.9960
Paisaje2	0.3736, 52.41 dB, 0.9981	0.7193, 49.56 dB, 0.9964	1.0803, 47.79 dB, 0.9947
Tigre	0.3229, 53.04 dB, 0.9946	0.6241, 50.17 dB, 0.9892	1.0043, 48.11 dB, 0.9853

Nota: Autores (2025).

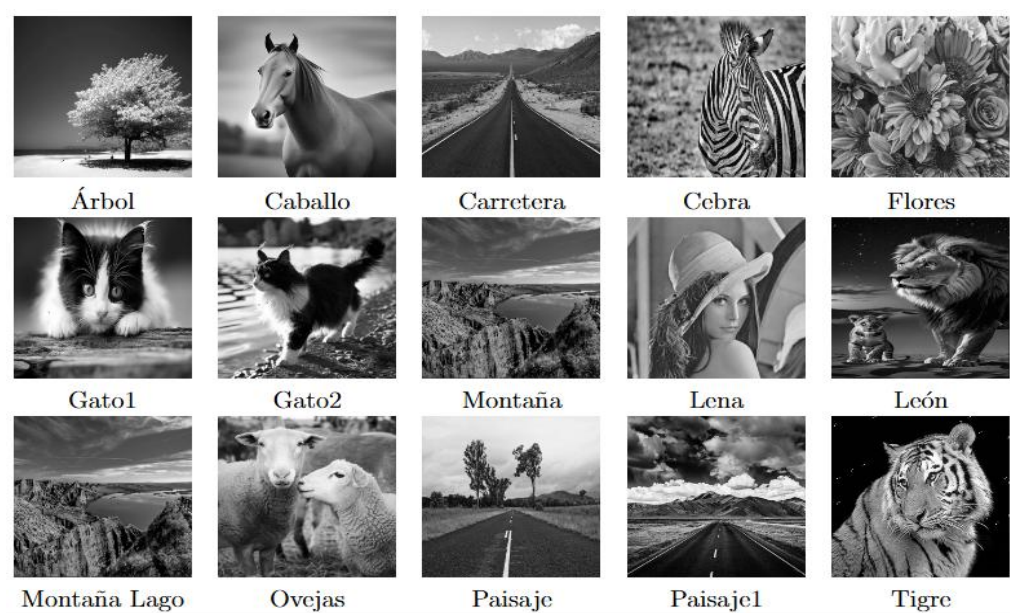
Las Figuras 5, 6 y 7 ilustran las imágenes resultantes para cada uno de los tres mensajes utilizados: “Hello”, “Hello Mund0” y “Hello Mund0 1234@”. Como se observa, la calidad visual se mantiene prácticamente inalterada, incluso cuando se ocultan mensajes con símbolos especiales y longitud considerable. En la Tabla 1, se presentan los valores de MSE, PSNR y SSIM obtenidos para cada imagen y frase oculta.

Figura 5
Imágenes con el mensaje oculto “Hello”



Nota: Autores (2025).

Figura 6
Imágenes con el mensaje oculto “Hello Mund0”



Nota: (Autores, 2025).

Figura 7

Imágenes con el mensaje oculto "Hello Mund0 1234@"



Nota: (Autores, 2025).

3.2. Impacto de la longitud del mensaje en la calidad visual

A medida que se incrementa el tamaño del mensaje oculto, se observa un aumento leve pero progresivo en la distorsión medida por MSE, lo cual es coherente con la lógica del proceso: se modifican más coeficientes DCT para insertar los datos. Esto conlleva también una disminución en PSNR, aunque sin afectar de manera significativa la apariencia de la imagen.

No obstante, el valor alto de SSIM en todos los casos confirma que la percepción humana no logra distinguir los cambios, ya que el algoritmo distribuye el mensaje de manera eficiente, priorizando coeficientes menos sensibles al ojo humano. Esto refuerza la utilidad del F5 en aplicaciones donde se requiere mantener la discreción sin sacrificar calidad visual.

Diferencias en la calidad según la imagen utilizada

El impacto del algoritmo no es uniforme en todas las imágenes. Se identificó que aquellas con mayor complejidad visual y variaciones en texturas y detalles presentan una mejor capacidad de ocultamiento sin afectar significativamente la calidad. Por el contrario, en imágenes con regiones homogéneas y de baja variabilidad, la distorsión introducida tiende a ser más evidente a nivel numérico, aunque sigue sin ser perceptible visualmente.

En imágenes como "Montaña", se obtuvo el valor más alto de PSNR (59.73 dB) con un mensaje más corto, lo que indica que la degradación o distorsión es prácticamente nula. En cambio, en imágenes como "Carretera", la inserción de un mensaje largo redujo PSNR hasta 47.30 dB, evidenciando un mayor impacto en la calidad visual.

Esto sugiere que la elección de la imagen de base influye en la efectividad del ocultamiento y debe considerarse al aplicar el algoritmo en entornos prácticos.

3.3. Relación entre distorsión y perceptibilidad

Si bien los valores de MSE y PSNR reflejan una degradación progresiva con mensajes más largos, el análisis visual de las imágenes generadas muestra que los cambios introducidos son imperceptibles a simple vista. Esto significa que, en escenarios donde se prioriza la seguridad de la información sin comprometer la calidad visual, el algoritmo F5 sigue siendo una alternativa viable.

El alto valor de SSIM en todas las imágenes (≥ 0.985) confirma que la estructura y los patrones generales de cada una de las imágenes permanecen intactos, lo que sugiere que la implementación del algoritmo F5 no causa alteraciones que detecte el ojo humano, debido a que los coeficientes DCT son cuidadosamente distribuidos. Este comportamiento se alinea con lo planteado por Wang et al. (2013) al introducir SSIM como una métrica que refleja mejor la percepción visual frente a otras medidas tradicionales como PSNR. Sin embargo, las herramientas avanzadas de análisis forense digital pueden detectar los cambios realizados, por lo que es necesario realizar combinaciones con otros métodos de ocultamiento de información para fortalecer los ataques de detección.

Estos hallazgos confirman que el algoritmo F5 puede ser empleado en aplicaciones utilizadas para la transmisión de datos de forma segura, pero es importante seguir explorando nuevas técnicas que permitan fortalecer el ocultamiento de información frente a herramientas de detección avanzadas.

4. Discusión

Los resultados obtenidos a partir de los experimentos realizados permiten reafirmar que el algoritmo F5 constituye una herramienta eficaz para la esteganografía en imágenes JPEG, ya que permite preservar la calidad visual de las imágenes al mismo tiempo que oculta información sensible. Las distorsiones generadas son detectables a nivel cuantitativo mediante métricas como MSE y PSNR, pero estos valores se mantienen por debajo del umbral perceptible para el ojo humano, validando su aplicación práctica en la seguridad de la información.

La métrica SSIM que es diseñada para valorar la similitud estructural entre imágenes desde un enfoque perceptual se mantuvo consistentemente elevada (≥ 0.985) en todos los casos evaluados. Este comportamiento confirma que incluso con mensajes relativamente largos la estructura visual de la imagen se mantiene prácticamente intacta. Esta característica resulta especialmente relevante en contextos donde el análisis visual representa el primer filtro para la detección de contenido alterado.

Un aspecto importante identificado en esta investigación es que el impacto del ocultamiento no es homogéneo en todas las imágenes, ya que las imágenes que presentan mayor complejidad visual como son: texturas variadas, contornos definidos o elementos en distintos planos, favorecen el proceso de esteganografía, lo que permite camuflar de mejor forma los pequeños cambios generados en los coeficientes DCT. En contraste, las imágenes con regiones planas o homogéneas presentan una sensibilidad mayor a la incrustación del mensaje a ocultar, por lo que se obtienen valores más altos de MSE y más bajos de PSNR aunque el mensaje oculto sea corto. Esto coincide con los hallazgos reportados por Jiang et al. (2014), quienes resaltan la importancia de la estructura de la imagen para mantener la calidad durante la inserción de datos.

Se identificó una tendencia clara: a mayor longitud del mensaje oculto, mayor distorsión generada. Sin embargo, esta distorsión no compromete la percepción visual directa, lo cual representa una fortaleza clave del algoritmo F5. Esta observación es coherente con trabajos previos de Almohammad y Ghinea (2010), quienes señalan que un PSNR superior a 40 dB suele ser suficiente para que la imagen esteganografiada se perciba como visualmente idéntica a la original.

No obstante, a pesar de los buenos resultados, el algoritmo presenta ciertas limitaciones. En particular, su vulnerabilidad ante técnicas avanzadas de análisis forense digital, como los métodos basados en redes neuronales o aprendizaje automático, representa un desafío a considerar. Investigaciones recientes como las de Baziyad et al. (2021) y Fridrich (2009) han demostrado que, aunque un algoritmo pueda mantener la calidad visual, puede ser detectado mediante análisis estadístico o espectral. Por este motivo, resulta fundamental considerar la integración de estrategias híbridas para aumentar su resistencia.

En esa línea, se han propuesto mejoras sustanciales mediante la combinación del algoritmo F5 con técnicas como la descomposición en valores singulares (DCT-SVD), el uso de tablas de cuantización adaptativas o incluso enfoques basados en aprendizaje profundo. Estas alternativas no solo aumentan la capacidad de ocultamiento, sino también la robustez frente a ataques de detección. Estudios como los de Tchakounté et al. (2020), Lin et al. (2024) y Zeng et al. (2024) evidencian que los algoritmos híbridos permiten una selección más eficiente de coeficientes DCT, optimizando así la calidad visual y la seguridad.

Cabe señalar también que este estudio se ha realizado bajo condiciones experimentales controladas, con imágenes en escala de grises y sin someterlas a procesos posteriores como recompresión, recorte o rotación. Por tanto, aunque los resultados obtenidos son sólidos, es necesario reconocer que su aplicabilidad práctica puede verse limitada en entornos reales, donde las imágenes pueden ser modificadas por redes sociales, editores gráficos o sistemas automáticos de compresión. En este sentido, se hace evidente la necesidad de futuras investigaciones que evalúen el rendimiento del algoritmo F5 bajo condiciones adversas.

Los resultados obtenidos validan la eficacia del algoritmo F5 como técnica de ocultamiento visual eficiente, pero también evidencian su fragilidad frente a los avances en análisis forense digital. Su potencial puede ser significativamente fortalecido mediante la incorporación de técnicas adaptativas e inteligencia artificial, permitiendo su evolución hacia sistemas de esteganografía más resilientes.

5. Conclusiones

Este estudio evaluó de manera detallada el rendimiento del algoritmo F5 al ocultar mensajes de diferente longitud en imágenes JPEG, empleando como criterio de evaluación las métricas PSNR, MSE y SSIM. Los resultados confirman que existe una relación directamente proporcional entre la cantidad de información oculta y la distorsión generada. Sin embargo, dicha distorsión no es perceptible al ojo humano, y la estructura de la imagen se conserva en alto grado, como lo demuestra el comportamiento estable de SSIM.

El algoritmo F5 demostró ser altamente eficaz en la inserción de mensajes cortos y medianos, logrando mantener la calidad visual intacta. Incluso con mensajes largos, el impacto sobre la imagen resultó mínimo desde la percepción humana, lo que valida su utilidad en entornos donde se requiere discreción y seguridad informativa.

Uno de los aportes más significativos del estudio radica en la verificación empírica de que la complejidad visual de la imagen base influye directamente en la capacidad de ocultamiento. Las imágenes con mayor riqueza de detalles permiten una mejor distribución del mensaje sin alterar la percepción, mientras que aquellas con regiones homogéneas presentan una mayor susceptibilidad a la distorsión, aunque aún dentro de límites aceptables.

Si bien los resultados respaldan la aplicación del F5 en entornos prácticos, también se evidenció la necesidad de fortalecer su resistencia ante técnicas avanzadas de detección, especialmente aquellas basadas en aprendizaje profundo o redes convolucionales. En este sentido, el estudio recomienda explorar líneas de investigación orientadas a la integración del F5 con enfoques híbridos, como la descomposición DCT-SVD, el ajuste adaptativo de cuantización, y la selección dinámica de coeficientes mediante redes neuronales.

Se propone que futuras investigaciones amplíen el análisis hacia imágenes a color, las cuales representan la mayoría de los escenarios reales, así como evaluar el desempeño del algoritmo ante situaciones de recompresión, transformación geométrica y condiciones adversas de transmisión. También sería valioso incluir nuevas métricas perceptuales que permitan valorar con mayor precisión la calidad subjetiva, y comparar el F5 con algoritmos emergentes en la literatura.

El algoritmo F5 sigue siendo una opción válida y competitiva para la esteganografía visual, siempre que se le adapten mecanismos de refuerzo modernos. Su simplicidad, eficiencia y estabilidad lo convierten en una base sólida para futuras mejoras orientadas a contextos donde la confidencialidad, la calidad visual y la resistencia al análisis forense son requisitos fundamentales.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

- Abdel-Aziz, M. M., Hosny, K. M., & Lashin, N. A. (2021). Improved data hiding method for securing color images. *Multimedia Tools and Applications*, 80(8), 12641–12670. <https://doi.org/10.1007/s11042-020-10217-9>
- Ahmed, N., Natarajan, T., & Rao, K. (1974). Discrete cosine transform. *IEEE Transactions on Computers*, 23(1), 90–93. <https://doi.org/10.1109/T-C.1974.223784>
- Almohammad, A., & Ghinea, G. (2010). Stego image quality and the reliability of PSNR. *2010 2nd International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 215–220. <https://doi.org/10.1109/IPTA.2010.5586786>
- Almohammad, A., Ghinea, G., & Hierons, R. M. (2009). JPEG steganography: A performance evaluation of quantization tables. *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA)*, 471–478. <https://doi.org/10.1109/AINA.2009.123456>
- Banik, B. G., & Bandyopadhyay, S. K. (2016). Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in DCT. *Proceedings of 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 400–405. <https://doi.org/10.1109/ICRCICN.2015.7434263>
- Baziyad, M., Rabie, T., & Kamel, I. (2021). Toward stronger energy compaction for high capacity DCT-based steganography: A region-growing approach. *Multimedia Tools and Applications*, 80(6), 8611–8637. <https://doi.org/10.1007/s11042-021-123456>
- Brūzgienė, R., Venčkauskas, A., Grigaliūnas, & Petraška, J. (2024). Enhancing steganography through optimized quantization tables. *Electronics (Switzerland)*, 13(12). <https://doi.org/10.3390/electronics13123456>
- Fridrich, J. (2009). *Steganography in digital media: Principles, algorithms, and applications*. Cambridge University Press.

- Hendrych, J., & Ličev, L. (2020). Advanced methods of detection of the steganography content. *Lecture Notes in Electrical Engineering*, 554, 484–493. https://doi.org/10.1007/978-3-030-554-1_12
- Jiang, C., Pang, Y., & Xiong, S. (2014). A high capacity steganographic method based on quantization table modification and F5 algorithm. *Circuits, Systems, and Signal Processing*, 33(5), 1611–1626. <https://doi.org/10.1007/s00034-014-9739-z>
- Lin, C.-H., Hong, W., & Su, G.-Z. (2024). Adaptive sorting-based data hiding scheme for JPEG images. *Lecture Notes in Electrical Engineering*, 1217, 288–293. https://doi.org/10.1007/978-3-030-1217-1_23
- Lu, C., Wang, H., & Li, S. (2015). Optimized quantization tables for DCT-based steganography. *Multimedia Tools and Applications*, 71, 12641–12670. <https://doi.org/10.1007/s11042-014-2410-7>
- Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding--a survey. *Proceedings of the IEEE*, 87(7), 1062–1078. <https://doi.org/10.1109/5.771065>
- Sabeti, V., & Aghabagheri, A. (2023). Developing an adaptive DCT-based steganography method using a genetic algorithm. *Multimedia Tools and Applications*, 82(13), 19323–19346. <https://doi.org/10.1007/s11042-023-123456>
- Solak, S., Abdirashid, A. M., Adjevi, A., & Sahu, A. K. (2024). Robust data hiding method based on frequency coefficient variance in repetitive compression. *Engineering Science and Technology, an International Journal*, 56. <https://doi.org/10.1016/j.iestch.2024.123456>
- Tchakounté, F., Kamdem, P. C., Kamgang, J. C., Tchapgnoou, H. B., & Atemkeng, M. (2020). An efficient DCT-SVD steganographic approach applied to JPEG images. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 7(24), 1–13. <https://doi.org/10.4108/eai.123456>
- Wallace, G. K. (1991). The JPEG still picture compression standard. *Communications of the ACM*, 34(4), 30–44. <https://doi.org/10.1145/103085.103089>
- Wang, K., Lu, Z.-M., & Hu, Y.-J. (2013). A high capacity lossless data hiding scheme for JPEG images. *Journal of Systems and Software*, 86(7), 1965–1975. <https://doi.org/10.1016/j.jss.2013.03.123>
- Westfeld, A. (2001). F5-a steganographic algorithm high capacity despite better steganalysis. *Lecture Notes in Computer Science*, 2137, 289–302. https://doi.org/10.1007/3-540-45496-9_21
- Xie, X.-Z., Chang, C.-C., & Horng, J.-H. (2021). An EMD-based data hiding scheme for JPEG images. *Connection Science*, 33(3), 515–531. <https://doi.org/10.1080/09540091.2021.123456>
- Zeng, X., Feng, B., Xia, Z., Peng, Z., Qin, T., & Lu, W. (2024). Robust image hiding network with frequency and spatial attentions. *Pattern Recognition*, 155. <https://doi.org/10.1016/j.patcog.2024.123456>