Lecturas Matemáticas
Volumen **41** (2) (2020), páginas 149-164
ISSN 0120-1980

Un algoritmo esteganográfico adaptativo para lograr mayor indetectabilidad

An adaptive steganographic algorithm to achieve greater undetectability

Yuniel Guzmán Bazán, Erodis Pérez Michel y Alicia Centurión Fajardo

University of Granma, Cuba

RESUMEN. Las técnicas esteganográficas son utilizadas para insertar imperceptiblemente información confidencial en un medio, llamado cubierta, sin llamar la atención de intrusos. Cuando se utilizan imágenes para insertar información secreta sin tener en cuenta las zonas idóneas, se provoca una mala calidad visual y falta de seguridad en el mensaje incrustado. En este artículo es objetivo presentar un nuevo algoritmo esteganográfico donde el proceso de incrustación de la información secreta se realiza seleccionando, en primer lugar, las zonas de alta intensidad de la imagen. Con el algoritmo propuesto se mejora el nivel de imperceptibilidad y seguridad del esteganograma analizado a través de los resultados obtenidos de las métricas: Relación Señal a Ruido Pico (PSNR), índice universal de la calidad de imagen (UIQI), fidelidad de imagen (IF) y la entropía relativa de Cachin (RE) entre el esteganograma y la imagen que sirve de cubierta, en comparación con los resultados de métodos previamente propuestos en la literatura.

***Palabras clave*:** Esteganografía, Seguridad de la información, Zonas de alta intensidad de la imagen.

ABSTRACT. Steganographic techniques are used to imperceptibly insert confidential information into a cover medium without attracting the attention of intruders. When images are used to insert secret information without taking into account the ideal areas, it causes poor visual quality and a lack of security in the embedded message. The objective of this article is to present a new steganographic algorithm where the process of embedding the secret information is carried out by selecting, first, the areas of high intensity of the image. With the proposed algorithm, the level of imperceptibility and

security of the analyzed steganogram is improved through the results obtained from the parameters: peak signal to noise ratio (PSNR), universal image quality index (UIQI), image fidelity (IF) and the relative Cachin entropy (RE) between the steganogram and the image that serves as cover, compared to the results of methods previously proposed in the literature.

***Key words*:** Steganography, High-intensity image areas, Information security.

2010 AMS Mathematics Subject Classification. Primary 65G20; Secondary 94A08, Third 68P30.

1. Introducción

Para cualquier organización la protección de la información es una tarea vital, por ello, se llevan a cabo investigaciones con el objetivo de poder transmitirla de manera segura a través de cualquier canal [29, 53, 50]. Cuando se utilizan canales públicos, un intruso puede interceptar la información transmitida, accediendo a contenidos sensibles o manipulando la información [34]. La criptografía es una alternativa para una transmisión confiable y segura de la información, pues se ocupa de las técnicas de cifrado o codificado para alterar las representaciones lingüísticas de los mensajes con el fin de hacerlos ininteligibles a receptores no autorizados [48, 2]. Otro de los métodos empleados para garantizar la seguridad de la información es la esteganografía [39], la cual inserta imperceptiblemente información confidencial en un medio de cobertura sin llamar la atención del intruso. Esta propiedad de ocultación que emplea la esteganografía la hace diferente de la criptografía, ya que se esfuerza por ocultar la presencia de un mensaje a un espía.

Las técnicas esteganográficas pueden ser aplicadas a cubiertas tales como archivos de texto, audio, video o imágenes y se exploran para proteger la privacidad de los datos y la propiedad intelectual de la reproducción [45, 40]. Los factores principales para la técnica de esteganografía de imagen son la capacidad, la imperceptibilidad, la indetectabilidad y la robustez [35, 7]. La capacidad oculta o la carga útil expresa la cantidad de datos ocultos en la imagen de portada. La robustez significa la defensa contra el ataque o cualquier manipulación por parte de los espías, mientras que la imperceptibilidad se usa para medir la calidad de la imagen midiendo la Relación Señal a Ruido Pico (PSNR).

Cuando se utilizan imágenes para insertar información secreta, este procedimiento se realiza ocultando la información dentro de la propia imagen y se obtiene como resultado una nueva imagen conocida como *stego imagen* [14]. Las técnicas de esteganografía para obtener la stego imagen se pueden clasificar en dos categorías: dominio de frecuencia [32, 1] y técnicas de dominio espacial [17, 21, 30]. En el primer caso, los datos secretos se insertan en los coeficientes del dominio de la frecuencia, mientras que en el segundo caso, la información secreta se inserta directamente en la intensidad de los píxeles de la imagen. De los métodos empleados en el dominio espacial destacan los conocidos como *sustitución del bit menos significativo* (LSB o Least Significant Bit) [24, 15, 31] y las técnicas esteganográficas adaptativas [13].

En la mayoría de los algoritmos esteganográficos basados en el método de los bits menos significativos, la elección de las posiciones de incrustación dentro de una imagen

depende principalmente de un generador de números pseudoaleatorio sin tener en cuenta el contenido de la imagen en sí. Al realizar el proceso de incrustación sin considerar las regiones *lisas/planas* de la imagen, se provoca una pobre calidad visual y falta de seguridad del mensaje incrustado [26]. Las técnicas esteganográficas adaptativas surgen para solventar este problema, pues se encargan de la selección de zonas idóneas para incrustar los mensajes, además, garantizan incrustar una mayor cantidad de información en los mensajes [18, 28]. Estas técnicas se basan en el hecho de que la vista de los seres humanos es más sensible a variaciones de la imagen en zonas lisas mientras que es más difícil que se detecte visualmente una alteración de la imagen en zonas con cambios de intensidad o alta frecuencia [6]. A partir de los componentes en alta y baja frecuencia en las imágenes, se puede hacer la analogía de que las frecuencias bajas se relacionan con las zonas de la imagen lisas donde cualquier variación de la imagen es más notable visualmente, y las frecuencias altas se asocian a los bordes o texturas donde es más difícil la percepción visual de alguna alteración en los valores de píxeles.

En este artículo, el proceso de incrustación de la información secreta se realiza descartando aquellas zonas de *intensidad homogéneas* en las cuales el proceso de incrustación puede resultar más perceptible. Para ello, se detectan aquellas regiones con cambios de intensidad: contornos, *blobs* oscuros (claros) rodeadas de regiones claras. Por consiguiente, la detección de regiones de interés estará basada en la selección de las zonas de alta intensidad en la imagen.

2. Antecedentes matemáticos

2.1. Permutación caótica. Mapa fraccional caótico

Según la literatura científica, varios autores [47, 49, 54] han propuesto novedosos algoritmos esteganográficos basados en mapas caóticos, los cuales son sistemas no lineales adecuados para diseñar esquemas de ocultamiento seguros [47]. De hecho, estos sistemas se caracterizan por un elevado comportamiento pseudoaleatorio, una alta sensibilidad a las condiciones iniciales y a los parámetros de control [20].

En este artículo se hará uso del mapa caótico lineal por partes (PWLCM, del inglés piecewise linear chaotic map) desarrollado por los autores [25], el cual está definido matemáticamente por

$$x_n = F(x_{n-1}) = \begin{cases} \dfrac{x_{n-1}}{\xi}, & \text{if} \quad 0 \le x_{n-1} < \xi, \\ \dfrac{x_{n-1}-\xi}{0.5-\xi}, & \text{if} \quad \xi \le x_{n-1} < 0.5, \quad \xi \in (0, 0.5). \\ F(1-x_{n-1}), & \text{if} \quad 0.5 \le x_{n-1} < 1, \end{cases} \tag{1}$$

Es preciso señalar que (1) representa un sistema dinámico no lineal que posee un comportamiento perfecto y altas propiedades dinámicas como son la distribución invariable, la ergodicidad, la función de autocorrelación, y el exponente positivo de Lyapunov, etc., [25].

Además, su comportamiento caótico está dado a partir de una condición inicial $x_0 \in (0, 1)$ y un parámetro de control ξ. Por cierto, la función (1) estará implícita en el algoritmo propuesto en este artículo, con el fin de construir n posiciones caóticas

$$\rho_i = \lfloor x_i 10^{14} \bmod. \, n \rfloor, \quad 1 \leq i \leq n, \tag{2}$$

las cuales se utilizarán para determinar las bloques de coeficientes [4, 8] donde será insertado el mensaje secreto que se desea proteger.

2.2. Medidas estadísticas para calcular la calidad y seguridad de la imagen

Cualquier procesamiento aplicado a una imagen puede causar una pérdida importante de información o calidad. Es por ello que la evaluación de la calidad de imágenes es un aspecto esencial dentro de las tareas de procesado [27, 37].

2.21. Relación Señal a Ruido Pico (PSNR)

Cuando se aplican técnicas esteganográficas a una imagen esta es sometida a cambios al incrustar el mensaje secreto en los píxeles de la imagen portadora. Por tanto, es imprescindible analizar los cambios, ya que afectan directamente la imperceptibilidad de la stego imagen de salida. Una de las métricas utilizadas para medir la calidad de la stego imagen mediante el análisis del error cuadrático medio entre la imagen cubierta y la stego imagen es la Relación Señal a Ruido Pico, a menudo abreviado PSNR [22]. De hecho, algunos autores utilizan esta métrica para evaluar la invisibilidad de un mensaje secreto [5], la imperceptibilidad [6] y la calidad visual[36, 46] de la stego imagen en comparación con la imagen cubierta. Debido a que las señales tienen un rango dinámico amplio, el PSNR mayormente se expresa en términos de la escala logarítmica de decibelio (db) para calcular la calidad de la imagen. Es decir, cuanto mayor sea el valor de PSNR, mejor será la reconstrucción de la imagen [16]. El PSNR está dado por [42]:

$$\begin{aligned} \text{PSNR} &= 10 \log_{10} \left(\frac{MAX_{\mathcal{C}}^2}{\text{MSE}} \right) \\ &= 20 \log_{10} \left(\frac{MAX_{\mathcal{C}}}{\sqrt{\text{MSE}}} \right) \\ &= 20 \log_{10} \left(MAX_{\mathcal{C}} \right) - 10 \log_{10} \left(MSE \right), \end{aligned}$$

donde $MAX_{\mathcal{C}}$ es el valor del píxel máximo posible de la imagen cuando los píxeles se representan utilizando 8 bits por muestra, esto es 255. Por su parte MSE es el error cuadrático medio definido por

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [\mathcal{S}(i, j) - \mathcal{C}(i, j)]^2,$$

donde $\mathcal{C}$ es la imagen cubierta de tamaño $m \times n$, mientras que $\mathcal{S}$ representa la stego imagen.

2.22. Índice de calidad de imagen universal (UIQI)

Otras métricas que a menudo se usan para medir la calidad de una imagen son las basadas en el Sistema Visual Humano (HVS). El Índice Universal de Calidad de Imagen (UIQI), propuesto por Wang y Bovik en [51], es una de estas métricas. Esta medida es universal en el sentido de que no tiene en cuenta las condiciones de visualización o el observador individual [9]. Además, no utiliza los métodos tradicionales de suma de errores [55]. UIQI tiene un rango dinámico de valores que varía entre -1 y 1, cuanto más cerca de 1, mejor calidad de imagen.

$$\text{UIQI} = \frac{4\sigma_{\mathcal{CS}}}{\sigma_{\mathcal{C}}^2 + \sigma_{\mathcal{S}}^2} \frac{\overline{\mathcal{C}}\,\overline{\mathcal{S}}}{\overline{\mathcal{C}}^2 + \overline{\mathcal{S}}^2},$$

donde

$$\overline{\mathcal{C}} = (mn)^{-1} \sum_{\gamma \in [1,m]\times[1,n]} \mathcal{C}(\gamma),$$

$$\overline{\mathcal{S}} = (mn)^{-1} \sum_{\gamma \in [1,m]\times[1,n]} \mathcal{S}(\gamma),$$

$$\sigma_{\mathcal{C}}^2 = (mn)^{-1} \sum_{\gamma \in [1,m]\times[1,n]} \left(\mathcal{C}(\gamma) - \overline{\mathcal{C}}\right)^2,$$

$$\sigma_{\mathcal{S}}^2 = (mn)^{-1} \sum_{\gamma \in [1,m]\times[1,n]} \left(\mathcal{S}(\gamma) - \overline{\mathcal{S}}\right)^2,$$

$$\sigma_{\mathcal{CS}} = (mn)^{-1} \sum_{\gamma \in [1,m]\times[1,n]} \left[\left(\mathcal{C}(\gamma) - \overline{\mathcal{C}}\right)\left(\mathcal{S}(\gamma) - \overline{\mathcal{S}}\right)\right].$$

2.23. Fidelidad de imagen (IF)

La fidelidad a la imagen es una medida que muestra una relación consistente con la calidad percibida por la percepción visual humana. Además, esta métrica mide la similitud entre la imagen de portada $\mathcal{C}$ y la stego imagen $\mathcal{S}$ después de incrustar el mensaje [42]. Cuanto más cerca de 1, mejor. Está definido por [23, 38, 42] como:

$$\text{IF} = 1 - \sum_{\gamma \in [1,m]\times[1,n]} \left(\mathcal{C}(\gamma) - \mathcal{S}(\gamma)\right)^2 \Big/ \sum_{\gamma \in [1,m]\times[1,n]} \mathcal{C}(\gamma)^2.$$

2.24. Seguridad de un sistema esteganográfico. Entropía relativa de Cachin (RE)

La seguridad de un sistema esteganográfico es importante para una comunicación exitosa sin ser detectado. De acuerdo con la definición dada por Cachin en [10], se dice que un sistema esteganográfico es ε -seguro, si la divergencia Kullback-Leibler (KL) entre la imagen de portada y stego imagen es casi ε y se define en términos de la entropía relativa como:

$$\text{RE}\left(P_{\mathcal{C}} || P_{\mathcal{S}}\right) = \sum P_{\mathcal{C}} \left|\log \frac{P_{\mathcal{C}}}{P_{\mathcal{S}}}\right|,$$

donde $P_{\mathcal{C}}$ y $P_{\mathcal{S}}$ representan la distribución de la imagen de portada y la stego imagen, respectivamente. Además, se dice que un sistema esteganográfico es

- ε-seguro si RE $(P_{\mathcal{C}}||P_{\mathcal{S}}) \leq \varepsilon$,
- Perfectamente seguro si RE $(P_{\mathcal{C}}||P_{\mathcal{S}}) = 0$.

En resumen, cuanto más cercano a cero esté el valor de RE $(P_{\mathcal{C}}||P_{\mathcal{S}})$, mayor será el nivel de seguridad.

3. Esquema propuesto

El nuevo algoritmo esteganográfico que se propone tiene como objetivo lograr mayor indetectabilidad en el proceso de incrustación de la información secreta. Para ello, se propone en primer lugar, seleccionar las zonas de alta intensidad de la imagen mediante el siguiente procedimiento.

3.1. Detección de las zonas de alta intensidad

Para la detección de las zonas con cambios de intensidad se emplearán los módulos ImageChops, ImageOps, ImageEnhance de la librería PIL(Python Imaging Library) destinada al procesamiento de imágenes digitales. El proceso de selección de zonas con cambios de intensidad es el siguiente:

Paso 1: Invertir los colores de la imagen: se procede a invertir todos los colores de los píxeles y los valores de luminosidad de la imagen. Las áreas oscuras se vuelven claras, y las claras, oscuras. Las tonalidades se reemplazan por sus colores complementarios.

Paso 2: Restar imagen: el procedimiento de realzar zonas en una imagen dada, a través de la diferencia con otra imagen, suele ser de mucha utilidad, pues permite realzar información de bordes verticales u horizontales. En el caso de las imágenes empleadas para el experimento este procedimiento se utiliza para resaltar las zonas donde existen en importantes cambios de intensidad. La operación se realiza de la siguiente forma: imagen invertida − imagen original. La definición matemática de la resta de dos imágenes es otra imagen definida por $0 \leq T(r) \leq 255$, en la cual se evitan los valores negativos.

Paso 3: Convertir a escala de grises: esta transformación tiene gran utilidad al permitir resaltar de mejor manera las regiones de puntos de interés.

Paso 4: Invertir imagen: en este paso, esta transformación convierte las zonas *lisas/-planas* de la imagen a blanco y las zonas de alta intensidad en negro, contribuyendo a un alto contraste entre las regiones de interés y las que no lo son.

Paso 5: Ajuste del contraste y el brillo de la imagen: se aumentan los valores de brillo y contraste para resaltar los detalles en las imágenes y cambiar la definición de los bordes entre áreas claras y oscuras.

3.2. Proceso de inserción de la información confidencial

Paso 1: Dividir las zonas de alta intensidad en bloques de 8×8 bytes.

Paso 2: Seleccionar, según las posiciones caóticas (ρ_i, $1 \leq i \leq n$), el bloque correspondiente.

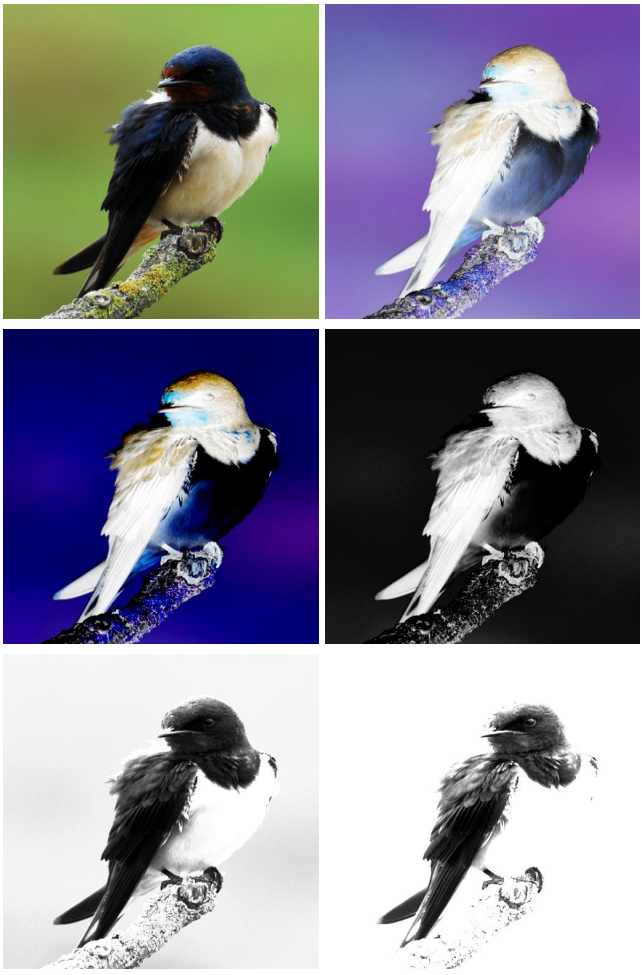

Figura 1. Proceso de detección de las zonas de alta intensidad (de izquierda-derecha y arriba-abajo)

Figura 2. Selección de los bloques de alta intensidad

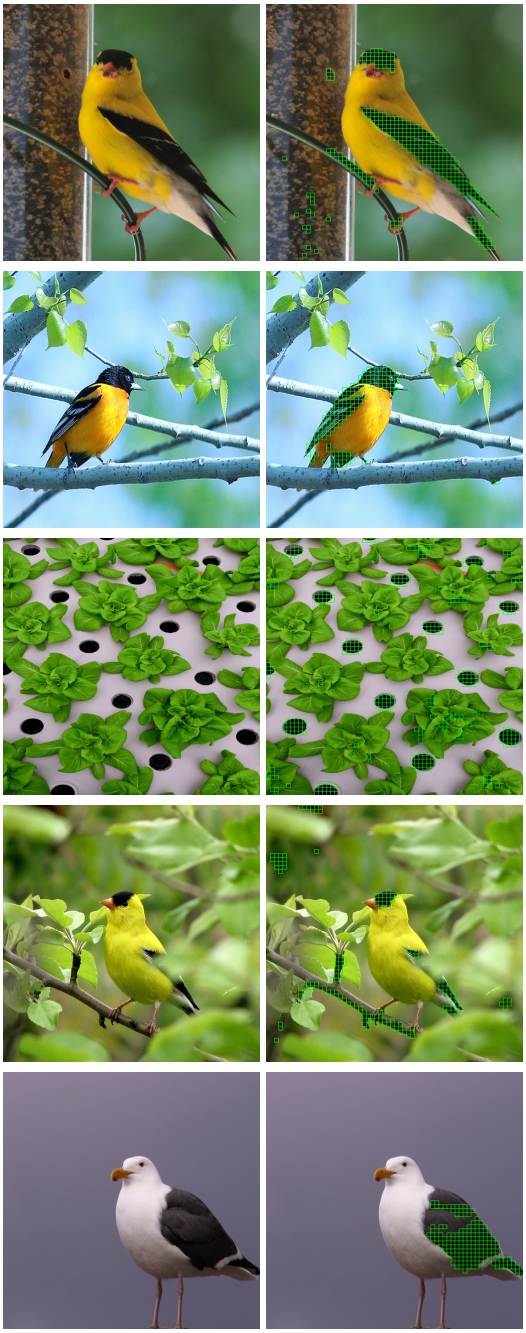

Figura 2. (Continuación)

Paso 3: Insertar los bit secretos en los LSB de cada uno de los elementos de los bloques seleccionados.

3.3. Proceso de extracción de la información confidencial

Paso 1: Dividir las zonas de alta intensidad en bloques de 8×8 bytes.

Paso 2: Seleccionar, según las posiciones caóticas (ρ_i, $1 \leq i \leq n$), el bloque correspondiente.

Paso 3: Extraer los bits secretos en los LSB de cada uno de los elementos de los bloques seleccionados.

4. Análisis y discusión de los resultados

La seguridad de la información a través de la esteganografía depende en gran medida del nivel de imperceptibilidad. Los sistemas esteganográficos deben generar una imagen esteganográfica lo suficientemente inocente de tal manera que no llame la atención a intrusos. Por tanto, el grado de distorsión o imperceptibilidad de una stego imagen en relación con la imagen original juega un papel fundamental para comprobar el éxito del proceso de ocultamiento de la información.

Para este primer análisis experimental se recolectaron 50 imágenes a color con tamaño (512×512) de cuatro conjunto de datos diferentes: image dataset of 1500 RGB-BMP images, transformed from Caltech birds dataset in JPEGC format [3], image dataset of 1500 RGB-BMP images, transformed from NRC dataset in TIFF format [3], image database [41], available in the University of Southern California and image dataset available at [33]. Para los resultados experimentales se utilizaron varias claves diferentes generadas aleatoriamente. El algoritmo propuesto fue probado ocultando un mensaje de tamaños adaptativos según el tipo de imagen. El algoritmo propuesto será comparado con los métodos presentados por Gupta [19] y Srilakshmi [44] utilizando las métricas de PSNR, UIQI, IF y RE.

4.1. Prueba de imperceptibilidad

En este primer experimento se procederá a comparar, a través del PSNR, el nivel de imperceptibilidad y distorsión. En la siguiente tabla se registran los resultado de 8 imágenes de las 50 seleccionadas. En la primera columna se registra el nombre de las imágenes y en las otras 3 los valores de PSNR correspondientes a los métodos de Gupta, Srilakshmi y el método propuesto.

Los resultados experimentales mostrados en la tabla 1 evidenciaron que el algoritmo propuesto produjo stego imágenes de buena calidad con buenos resultados en valores de PSNR. En el 90 % porciento de los casos los valor de PSNR correspondientes al método propuesto son superiores a los valores de PSNR de los métodos propuestos por Gupta y Srilakshmi, respectivamente.

Tabla 1. Valores de PSNR

Imagen	Gupta	Srilakshmi	Método propuesto
C0038.bmp	67,8477257266376	67,832231793618	67,9071120075435
C0150.bmp	64,04229467915	64,0386341984096	64,1548950439141
C0101.bmp	72,2202776155675	72,3277994834681	72,3803710781645
C0125.bmp	72,2202776155675	72,3277994834681	72,3803710781645
NB0174.bmp	68,1910373713257	68,1342951306345	69,7546400360665
C0040.bmp	70,8014828168798	70,8996151303302	71,0268278812892
C0087.bmp	63,5911438347365	63,5334749291606	63,7936400031651
C0041.bmp	64,8185820914832	64,812404725678	64,8871194354679
C0570.bmp	69,2007832441838	69,2092697047621	69,2341170252847

4.2. Prueba de calidad

Generalmente la calidad de la imagen basada en el Sistema Visual Humano (HVS) se mide mediante el Índice de Calidad de la Imagen (UIQI), que fue propuesto por Wang y Bovik en [52]. Esta medida es universal en el sentido de que no tiene en cuenta las condiciones de visualización ni al observador individual, además, no utiliza los métodos tradicionales de suma de errores [56]. El rango dinámico de UIQI está entre -1 y 1. Para imágenes idénticas, su valor será 1.

Tabla 2. Valores de UIQI

Imagen	Gupta	Srilakshmi	Método propuesto
C0038.bmp	1	1	1
C0150.bmp	1	1	1
C0101.bmp	1	1	1
C0125.bmp	1	1	1
NB0174.bmp	1	1	1
C0040.bmp	1	1	1
C0087.bmp	1	1	1
C0041.bmp	1	1	1
C0570.bmp	1	1	1

Este segundo experimento, como se puede apreciar en la tabla 2, muestra que no existen diferencias entre las imágenes de portada y stego imagen, ya que los valores de UIQI son exactamente 1 para los 3 métodos que se comparan.

4.3. Prueba de similitud

La fidelidad de la imagen es una medida que muestra una relación consistente con la calidad percibida por la percepción visual humana. Además, la medida es una métrica de la similitud entre la imagen de portada y la stego imagen después de la inserción del mensaje [43].

Si la stego imagen es una aproximación cercana a la imagen de portada, entonces el valor de IF sería cercano a la unidad. En el tercer experimento se encuentran los valores de IF para los métodos que se comparan. Se puede observar en la tabla 3 que los valores de IF son muy cercanos a la unidad para los tres métodos, lo que muestra que existe una alta similitud entre la imagen de portada y la stego imagen después de la inserción de los bits secretados. Es válido destacar que aunque existe una diferencia mínima, el método propuesto es superior en todos los casos de muestra, pues presenta los valores más cercanos a la unidad.

Tabla 3. Valores de IF

Imagen	Gupta	Srilakshmi	Método propuesto
C0038.bmp	0,999998808756459	0,999998804498976	0,999998824934891
C0150.bmp	0,999998187794008	0,999998186265934	0,999998234175551
C0101.bmp	0,999999837483703	0,999999841457855	0,999999843365447
C0125.bmp	0,999999815093716	0,999999814025606	0,999999834114291
NB0174.bmp	0,999999360573109	0,999999352163936	0,999999553901636
C0040.bmp	0,999999662256871	0,999999669802873	0,999999679334664
C0087.bmp	0,999998361775097	0,999998339876436	0,999998436406319
C0041.bmp	0,999998114008331	0,999998111323805	0,999998143538122
C0570.bmp	0,999999437916	0,999999439013285	0,999999442213698

4.4. Prueba de seguridad

La seguridad de un sistema esteganográfico se define en términos de la entropía relativa (RE) donde P_C y P_S representan la distribución de la imagen de cobertura y stego respectivamente. Esta medida estadística fue propuesta por Cachin en [11, 12]

Tabla 4. Valores de RE

Imagen	Gupta	Srilakshmi	Método propuesto
C0038.bmp	0	0	0
C0150.bmp	0	0	0
C0101.bmp	0	0,00000507513667264561	0
C0125.bmp	0,0000038147478916	0,000013978488962	0,000033109663747
NB0174.bmp	0	0	0
C0040.bmp	0	0	0
C0087.bmp	0,000020759058080	0,0000087509416869	0
C0041.bmp	0,0000012735288041	0,0000051183237051	0
C0570.bmp	0	0	0

En el cuarto experimento observamos que los valores de la entropía relativa son cercanos a cero, lo que afirma que el sistema esteganográfico obtenido a partir del algoritmo propuesto es suficientemente seguro. Aunque con una diferencia mínina, en un solo caso el

método propuesto fue inferior a los otros métodos con los cuales se compara. En los demás casos los valores de entropía relativa obtenidos por el método propuesto fueron iguales o superiores.

5. Conclusiones

En esta contribución, proponemos un algoritmo esteganográfico adaptativo que logra mayor indetectabilidad a partir de la selección de zonas idóneas para ocultar la información. A partir de los resultados experimentales se puede apreciar cuan efectivo resulta seleccionar zonas idóneas para la incrustación de mensajes secretos, en nuestro caso, zonas de alta intensidad. Los valores obtenidos de PSNR, UIQI, IF y RE demuestran que en la stego imagen no existen anomalías detectables con respecto a la imagen de portada. Además, los valores obtenidos para la entropía relativa muestran que el sistema esteganográfico obtenido por el algoritmo propuesto es suficientemente seguro.

Agradecimientos

Los autores agradecen todos los señalamientos por parte de los revisores, pues esto permitió mejorar la primera versión de este artículo.

Referencias

[1] Ahmed A Abdelwahab & Lobna A Hassaan, *A discrete wavelet transform based technique for image data hiding*, 2008 National Radio Science Conference, IEEE, 2008, pp. 1-9.

[2] Roy Pramono Adhie, Yonatan Hutama, A Saleh Ahmar, MI Setiawan, et al., *Implementation cryptography data encryption standard (des) and triple data encryption standard (3des) method in communication system based near field communication (nfc)*, Journal of Physics: Conference Series, vol. 954, IOP Publishing, 2018, p. 012009.

[3] M Al-Jarrah, *Rgb-bmp steganalysis dataset*, Mendeley Data **1** (2018).

[4] Larry C Andrews, *Special functions of mathematics for engineers*, vol. 49, Spie Press, 1998.

[5] Randa Atta & Mohammad Ghanbari, *A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set*, Journal of Visual Communication and Image Representation **53** (2018), 42-54.

[6] Abdelhamid Awad Attaby, Mona FM Mursi Ahmed& Abdelwahab K Alsammak, *Data hiding inside jpeg images with high resistance to steganalysis using a novel technique: Dct-m3*, Ain Shams Engineering Journal **9** (2018), no. 4, 1965-1974.

[7] Junlan Bai, Chin-Chen Chang, Thai-Son Nguyen, Ce Zhu& Yanjun Liu, *A high payload steganographic algorithm based on edge detection*, Displays **46** (2017), 42-51.

[8] Yun-Ru Bai, Dumitru Baleanu & Guo-Cheng Wu, *A novel shuffling technique based on fractional chaotic maps*, (2018).

[9] Bulent Bayraktar, Tytus Bernas, J Paul Robinson & Bartek Rajwa, *A numerical recipe for accurate image reconstruction from discrete orthogonal moments*, Pattern Recognition **40** (2007), no. 2, 659-669.

[10] C. Cachin, *An information-theoretic model for steganography*, **1525** (1998), 306-318.

[11] Christian Cachin, *An information-theoretic model for steganography*, International Workshop on Information Hiding, Springer, 1998, pp. 306-318.

[12] _____, *An information-theoretic model for steganography*, Information and Computation **192** (2004), no. 1, 41-56.

[13] Rajarathnam Chandramouli, Grace Li & Nasir D Memon, *Adaptive steganography*, Security and Watermarking of Multimedia Contents IV, vol. 4675, International Society for Optics and Photonics, 2002, pp. 69-78.

[14] Abbas Cheddad, Joan Condell, Kevin Curran & Paul Mc Kevitt, *Digital image steganography: Survey and analysis of current methods*, Signal processing **90** (2010), no. 3, 727-752.

[15] Dinu Coltuc & Jean-Marc Chassery, *Very fast watermarking by reversible contrast mapping*, IEEE Signal processing letters **14** (2007), no. 4, 255-258.

[16] Biswajita Datta, Upasana Mukherjee & Samir Kumar Bandyopadhyay, *Lsb layer independent robust steganography using binary addition*, Procedia Computer Science **85** (2016), 425-432.

[17] Nameer N El-Emam, *Hiding a large amount of data with high security using steganography algorithm*, Journal of Computer Science **3** (2007), no. 4, 223-232.

[18] Avinash K Gulve & Madhuri S Joshi, *An image steganography method hiding secret data into coefficients of integer wavelet transform using pixel value differencing approach*, Mathematical Problems in Engineering **2015** (2015).

[19] Pragya Gupta & Jayti Bhagat, *Image steganography using lsb substitution facilitated by shared password*, International Conference on Innovative Computing and Communications, Springer, 2019, pp. 369-376.

[20] Milia Habib, Bassem Bakhache, Dalia Battikh & Safwan El Assad, *Enhancement using chaos of a steganography method in dct domain*, 2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), IEEE, 2015, pp. 204-209.

[21] Mamta Juneja & Parvinder S Sandhu, *An improved lsb based steganography technique for rgb color images*, International Journal of Computer and Communication Engineering **2** (2013), no. 4, 513.

[22] Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial & Brendan Halloran, *Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research*, Neurocomputing **335** (2019), 299-326.

[23] A. Khamruia & J. K. Mandal, *A genetic algorithm based steganography using discrete cosine transformation (GASDCT)*, Procedia Technology **10** (2013), no. 2013, 105-111.

[24] Ya-Lin Lee & Wen-Hsiang Tsai, *A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations*, IEEE Transactions on circuits and systems for video technology **24** (2013), no. 4, 695-703.

[25] Shujun Li, Guanrong Chen & Xuanqin Mou, *On the dynamical degradation of digital piecewise linear chaotic maps*, International journal of Bifurcation and Chaos **15** (2005), no. 10, 3119-3151.

[26] Weiqi Luo, Fangjun Huang & Jiwu Huang, *Edge adaptive image steganography based on lsb matching revisited*, IEEE Transactions on information forensics and security **5** (2010), no. 2, 201-214.

[27] Mina Ayman Saleh Yanni Makar, Ajit Deepak Gupte & Ajit Venkat Rao, *Measuring spherical image quality metrics based on user field of view*, April 30 2019, US Patent 10,277,914.

[28] Aref Miri & Karim Faez, *An image steganography method based on integer wavelet transform*, Multimedia Tools and Applications **77** (2018), no. 11, 13133-13144.

[29] Ayman Mostafa & Lutz Lampe, *Optimal and robust beamforming for secure transmission in miso visible-light communication links*, IEEE Transactions on Signal Processing **64** (2016), no. 24, 6501-6516.

[30] KA Moustafa & W Badawy, *(color/gray) image in color cover hiding using modification of spatial domain hiding method*, Future Generation Communication and Networking (FGCN 2007), vol. 1, IEEE, 2007, pp. 56-61.

[31] Masoud Nosrati, Ali Hanani & Ronak Karimi, *Steganography in image segments using genetic algorithm*, 2015 Fifth International Conference on Advanced Computing & Communication Technologies, IEEE, 2015, pp. 102-107.

[32] Hardik Patel & Preeti Dave, *Steganography technique based on dct coefficients*, International Journal of Engineering Research and Applications **2** (2012), no. 1, 713-717.

[33] Eko Hari Rachmawanto, Christy Atika Sari, Heru Agus Santoso, Fauzi Adi Rafrastara, Edi Sugiarto, et al., *Block-based Arnold chaotic map for image encryption*, 2019 International Conference on Information and Communications Technology (ICOIACT), IEEE, 2019, pp. 174-178.

[34] Diego Renza, L Ballesteros, M Dora & Ramiro Rincón, *Improved pixel hiding method for steganography of gray images within color images*, Ingeniería y Ciencia **12** (2016), no. 23, 145-162.

[35] Subhrajit Sinha Roy, Abhishek Basu & Avik Chattopadhyay, *Intelligent copyright protection for images*, Chapman and Hall/CRC, 2019.

[36] Aditya Kumar Sahu & Gandharba Swain, *A novel n-rightmost bit replacement image steganography technique*, 3D Research **10** (2019), no. 1, 2.

[37] Umme Sara, Morium Akter & Mohammad Shorif Uddin, *Image quality assessment through fsim, ssim, mse and psnr-a comparative study*, Journal of Computer and Communications **7** (2019), no. 3, 8-18.

[38] M. Sengupta, P. Mandal, T. Das & A. Dey, *A novel hash based technique for thermal image authentication*, Procedia Technology **10** (2013), 147-156.

[39] Frank Y Shih, *Digital watermarking and steganography: fundamentals and techniques*, CRC press, 2017.

[40] Gulshan Shrivastava, Aakanksha Pandey & Kavita Sharma, *Steganography and its technique: Technical overview*, Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, Springer, 2013, pp. 615-620.

[41] USC SIPI, *The usc-sipi image database*, (2016).

[42] A. Soria-Lorente & S. Berres, *A secure steganographic algorithm based on frequency domain for the transmission of hidden information*, Security and Communication Networks **2017, Article ID 5397082** (2017), 1-14.

[43] Anier Soria-Lorente & Stefan Berres, *A secure steganographic algorithm based on frequency domain for the transmission of hidden information*, Security and Communication Networks **2017** (2017).

[44] P Srilakshmi, Ch Himabindu, N Chaitanya, SV Muralidhar, MV Sumanth & K Vinay, *Text embedding using image steganography in spatial domain*, International Journal of Engineering & Technology **7** (2018), no. 3, 1-4.

[45] Mansi S Subhedar & Vijay H Mankar, *Current status and key issues in image steganography: A survey*, Computer science review **13** (2014), 95-113.

[46] K Vaishakh, A Pravalika, DV Abhishek, NP Meghana & Gaurav Prasad, *A semantic approach to text steganography in sanskrit using numerical encoding*, Recent Findings in Intelligent Computing Techniques, Springer, 2019, pp. 181-192.

[47] Milad Yousefi Valandar, Milad Jafari Barani, Peyman Ayubi & Maryam Aghazadeh, *An integer wavelet transform image steganography method based on 3d sine chaotic map*, Multimedia Tools and Applications **78** (2019), no. 8, 9971-9989.

[48] Laura Vegh & Liviu Miclea, *Secure and efficient communication in cyber-physical systems through cryptography and complex event processing*, 2016 International Conference on Communications (COMM), IEEE, 2016, pp. 273-276.

[49] Gurjit Singh Walia, Shikhar Makhija, Kunwar Singh & Kapil Sharma, *Robust stego-key directed lsb substitution scheme based upon cuckoo search and chaotic map*, Optik **170** (2018), 106-124.

[50] Xingyuan Wang, Lintao Liu & Yingqian Zhang, *A novel chaotic block image encryption algorithm based on dynamic random growth technique*, Optics and Lasers in Engineering **66** (2015), 10-18.

[51] Zhou Wang & Alan C Bovik, *A universal image quality index*, IEEE Signal Processing Letters **9** (2002), no. 3, 81-84.

[52] Zhou Wang & Alan C. Bovik, *A Universal Image Quality Index*, IEEE Signal Processing Letters, (2002) vol. 9, no. 3, 81-84.

[53] Xiaoming Xu, Biao He, Weiwei Yang, Xiangyun Zhou & Yueming Cai, *Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers*, IEEE Transactions on Information Forensics and Security **11** (2015), no. 2, 373-387.

[54] Gyan Singh Yadav & Aparajita Ojha, *Chaotic system-based secure data hiding scheme with high embedding capacity*, Computers & Electrical Engineering **69** (2018), 447-460.

[55] Y. Zheng & Q. Zheng, *Objective image fusion quality evaluation using structural similarity*, Tsinghua Science and Technology **14** (2009), no. 9, 703-709.

[56] Youzhi Zheng & Zheng Qin, *Objective image fusion quality evaluation using structural similarity*, Tsinghua Science & Technology **14** (2009), no. 6, 703-709.

Recibido en septiembre de 2020. Aceptado para publicación en octubre de 2020.

MSc. Yuniel Guzmán Bazán
Departamento de Tecnología
Universidad de Granma
Bayamo, Cuba
e-mail: yguzmanb@udg.co.cu

Erodis Pérez Michel
Departamento de Tecnología
Universidad de Granma
Bayamo, Cuba
e-mail: eperezm@udg.co.cu

MSc. Alicia María Centurión Fajardo
Departamento de Ciencias Básicas e Informática Aplicada
Universidad de Granma
Bayamo, Cuba
e-mail: acenturionf@udg.co.cu