Método de esteganografía a través de la dimensión fractal y el algoritmo de LSB; una nueva perspectiva en imágenes RGB

Steganography Method through Fractal Dimension and LSB Algorithm; a New Perspective on RGB Images.

Héctor Caballero Hernández[1], Vianney Muñoz Jiménez[2], Marco A. Ramos[3], Marcelo Romero Huertas[4]

Universidad Autónoma del Estado de México, Facultad de Ingeniería, Cerro de Coatepec, Paseo Universidad s/n, Universitaria, 50130 Toluca de Lerdo, Estado de México
[1]hcaballeroh240@profesor.uaemex.mx, [2]vmunozj@uaemex.com, [3]maramos@uaemex.mx, [4]mromeroh@uaemex.mx

Fecha de recepción: 29 de junio de 2018
Fecha de aceptación: 9 de abril de 2019

Resumen. Los métodos de esteganografía actualmente recurren a la combinación de técnicas de ocultamiento de información con el propósito de incrementar la cantidad de datos embebidos en los estego-objetos, así como de reducir la probabilidad de que sean descubiertos los datos por medio de técnicas de estego-análisis, o en su defecto implementar sistemas de criptografía para evitar que se conozca los contenidos de los datos ocultos. En este trabajo se presenta una nueva forma de la aplicación de la teoría fractal a través del cálculo de la dimensión de los fractales, que en combinación con el método LSB aplicado a imágenes RGB permite ofrecer un nivel elevado de seguridad, para garantizar la privacidad de los datos ocultos. En los experimentos ejecutados se observa que la codificación no genera errores en la recuperación de los datos, no presenta deformaciones visuales y satisfacen las métricas de calidad PSNR, MSE, SNR y SIMM.

Palabras clave: Esteganografía, LSB, fractales, dimensión fractal.

Summary. Steganography methods currently resort the combination of information hiding techniques with the purpose of increasing the amount of data embedded in the stego-objects, as well reducing the probability that the data will be discovered employing steganalysis or failing implement cryptography systems avoid knowing the data contents. In this work, we present a new form of the application of fractal theory through the calculation of the dimension of the fractals that, in combination with the LSB method applied to RGB images, allows offer a high level of security, guaranteeing the privacy of the fractals hidden data. In the executed experiments it is observed that the coding does not generate errors in the recovery of the data, does not present visual deformations and satisfies the quality metrics PSNR, MSE, SNR and SIMM.

Keywords: Steganography, LSB, fractals, fractal dimension.

1 Introducción

El manejo de información para su transmisión en métodos digitales requiere de procedimientos que garanticen su traslado de forma segura, dado que una gran cantidad de los sectores de la población utiliza medios digitales para enviar y recibir información. En el presente trabajo se aborda una nueva perspectiva sobre el ocultamiento de la información a través de la teoría fractal y la técnica LSB (Least Significative Bit) en imágenes RGB.

1.1 Métodos de esteganografía

La esteganografía se define como la ciencia y el arte del ocultamiento de la información, estudia los métodos de envío de información para que pase desapercibida [1]. En esteganografía existe el objeto portador, que es la entidad en la cual se insertará el mensaje a ocultar y el estego objeto, que es la unión del mensaje con el objeto portador. Las técnicas más importantes que se emplean son las de sustitución del bit menos significativo (LSB, por sus siglas en inglés) y las que utilizan técnicas en el dominio de la frecuencia ([2], [3]). A continuación, se describen las más destacadas.

El método LSB modifica el bit de menor peso de un byte del objeto portador. Teóricamente la sustitución del bit menos significativo no distorsiona el objeto, desde el punto de percepción humano [4]. El método PVD (Pixel Value Differencing) [9], está basado en la sustitución de los valores de la diferencia de los bloques de dos píxeles continuos en una imagen, por otros similares en los cuales se incluyen bits de datos ocultos [5].

Las técnicas más importantes en el dominio de la frecuencia son DFT (Discrete Fourier Transformation), DCT (Discrete Cosine Transformation Discrete) y DWT (Wavelet Transformation). Una ventaja de estas técnicas sobre las técnicas de dominio espacial es que la información está menos expuesta a la compresión, recorte y al procesamiento de la imagen [6].

1.2 Definición de fractal

El término fractal fué propuesto por Benoit Mandelbrot. Su dimensión métrica es representada por un número fraccionario. Los fractales se pueden representar como conjuntos matemáticos cuyos patrones son similares entre sí. Los fractales pueden ser exactamente iguales en todas las escalas. Estos objetos tienen una dimensión fractal que generalmente excede su dimensión topológica y está comprendida entre números enteros y fraccionarios [7]. La dimensión fractal se puede calcular a través de la ecuación (1).

$$D_{MB} = \lim_{\varepsilon \to 0} \frac{logN(\varepsilon)}{log\frac{l}{\varepsilon}} \tag{1}$$

Donde D es la dimensión euclidiana, MB es la dimensión Minkowski-Bouligand, l es el número de dimensión, N es el número de objetos auto-similares y ε es el lado lineal.

1.3 Métricas para medición de calidad en imágenes

Las métricas de medición de calidad permiten conocer las modificaciones que existen entre dos imagen, una de esta métricas es MSE (Mean Squared Error) [9], se define como error cuadrático medio, donde $f(x,y)$ es una señal portadora, $\hat{f}(x,y)$ es una señal procesada, M y N es el tamaño de la señal en 2D. La ecuación (2) representa el MSE.

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left[f(x,y) - \hat{f}(x,y)\right]^2 \tag{2}$$

La métrica PSNR (Peak Signal to Noise Ratio) se define como un límite, en donde se aproxima la relación con el receptor de errores, por el sistema de visión humano. Un PSNR alto implica que la semejanza entre la imagen portadora y la imagen reconstruida es alta [9]. El PSNR se define en la ecuación (3), donde *L* representa el número de intensidades.

$$PSNR(dB) = 10log_{10}L^2/MSE \tag{3}$$

La métrica SSIM (Structural Similarity Index) determina la similitud entre dos imágenes [10]. Generalmente se utiliza el índice MSSIM (SSIM medio) para evaluar la calidad de una imagen, $f(x,y)$ representa la imagen portadora y $\hat{f}(x,y)$ la imagen distorsionada, f_j y $\hat{f}_j$ son el contenido de la ventana local jth, y W es el número de ventanas locales de la imagen. La ecuación (4) representa a MSSIM.

$$MSSIM\left(f(x,y), \hat{f}(x,y)\right) = \frac{1}{W}\sum_{j=1}^{w} SSIM\,(f_j, \hat{f}_j) \tag{4}$$

2 Revisión del estado del arte

Algunos de los trabajos que han abordado el empleo del método LSB es el de Eswari et al. [11], en el 2014 aplican el algoritmo de Zhang para embeber información dentro de imágenes fractales además de combinar su técnica con RSA(*Rivest, Shamir y Adleman*). Los resultados obtenidos del PSNR son superiores a 42 dB.

En Desai et al. [12] en el 2014 utilizan criptografía y watermarking, emplean el fractal de Mandelbrot para compresión de la imagen a embeber. La imagen por ocultar se divide en secciones de acuerdo con la ecuación fractal propuesta y posteriormente se embebe mediante DTC. Las pruebas se realizaron en imágenes en escala de gris y RGB, los histogramas de la imagen portadora y la estego-imagen presentan diferencias nulas.

Nehete et al. [13] en el 2014 aplican el análisis de segmentación de texturas y color en imágenes, aprovechan las variantes de tonos de piel de un conjunto de rostros humanos, la técnica de esteganografía aplicada es DWT sobre el modelo YCbCr.

Stoyanova et al. [14] en el 2015, aplican una modificación sobre LSB, emplean una llave criptográfica, la cual permite el control de la inserción de datos y la recuperación de estos mediante el sistema Rijndael. El PSNR de las estego-imágenes es superior a 54 dB, tomando en cuenta que usan los 3 primeros bits significativos. Las métricas de comprobación de calidad de la imagen que aplican son MSE, SNR, PSNR y SSIME.

En Hussain et al. [15] en el 2016, proponen como mecanismo de ocultamiento la técnica de LSB y criptografía empleando operaciones XOR y el método SHA de 256 bits, además agregan *pseudo ramdom number*, más la inclusión de técnicas *Hash* para ocultar información.

En el 2016 Ouyang et al. [16] combinan LSB con XOR, obtiene resultados sobresalientes en imágenes de 512x512 píxeles al embeber imágenes del tamaño de un 25% con relación al de la portadora, sus pruebas arrojan niveles superiores de 55 dB de PSNR.

Geetha et al. [17] presenta un análisis de la aplicación de la teoría del caos y teoría fractal para esteganografía, en el cual se observan los alcances para los métodos de compresión a través de fractales. Varias de las propuestas analizadas combinan métodos como LSB, DCT, DWT, entre otras.

3 Metodología

En la Fig. 1 se presenta la propuesta para el método de esteganografía, el primer bloque representa el análisis del texto que se va a ocultar en la imagen portadora, en el segundo bloque, se genera el cálculo de las dimensiones fractales a través de la formación de una lista de fractales deterministas, esta lista se conforma en función del tamaño del alfabeto extraído. Posteriormente, se eligen los fractales que obtuvieron un mayor número de diferencias en su dimensión. En el tercer bloque, se obtiene la relación entre la dimensión fractal y los símbolos mediante vectores que representen la cantidad de objetos auto similares que conformaron las dimensiones elegidas. En el bloque 4 se insertan los datos y las reglas de extracción mediante la técnica LSB, en el bloque 5 se calcula la calidad de la estego-imagen, y el último bloque se recuperan los datos insertados en la imagen.

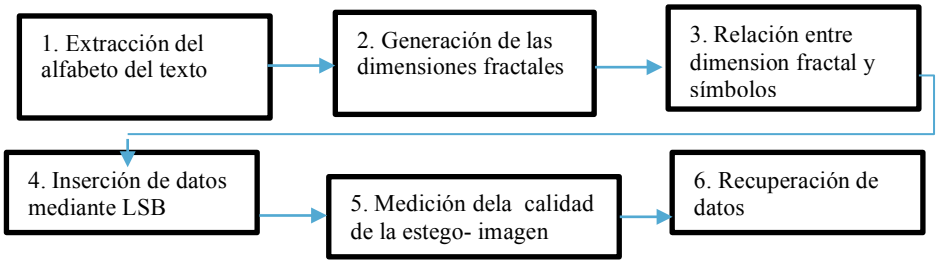

Figura 1. Metodología para esteganografía y codificación.

3.1 Cálculo de la dimensión fractal

El procedimiento del análisis del mensaje consiste en obtener un alfabeto. Terminado el proceso extracción del alfabeto, se genera una lista de ecuaciones de fractales deterministas para calcular su dimensión fractal, la lista es del tamaño de la cantidad de los símbolos extraídos del mensaje.

La lista de ecuaciones de las dimensiones fractales se introducen a un *bucle* en donde la entrada para cada ecuación son los números de objetos auto similares de los cuales se desea calcular su dimensión, es necesario establecer una alta precisión numérica antes del punto decimal, para que las diferencias sean apreciables. El límite de objetos auto similares está en función de las capacidades del lenguaje en el que se codifique, los resultados de cada ecuación se almacenan en una lista de arreglos. Al finalizar el *bucle*, se obtienen las dimensiones fractales que contengan mayores variaciones y se selecciona la ecuación con mayor número de variación. Al finalizar el proceso, se selecciona el vector que contenga un número similar de elementos con respecto al tamaño del alfabeto, como se muestra en la secuencia que se expone en la Fig. 2.

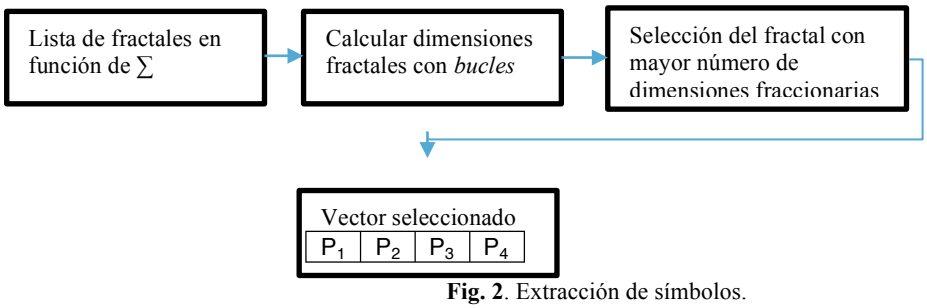

Fig. 2. Extracción de símbolos.

3.2 Asignación de la dimensión fractal con símbolos e inserción de datos a través de LSB

El procedimiento de asignación del vector seleccionado (P_x) con el alfabeto ($\sum$) se desarrolla a través de la generación de un segundo vector (S_x) formado por caracteres aleatorios como se muestra en la Fig. 3 bloque 1, para realizar la sustitución del alfabeto original. El primer vector se emplea para generar las reglas de recuperación del mensaje mediante una operación matemática que relacione el símbolo original con el valor de una posición del vector. En las reglas de recuperación se debe indicar la ecuación que represente el fractal elegido (a través de una expresión regular), Fig. 3 bloque 2. Una vez que se ha generado la sustitución de símbolos y la generación de reglas de recuperación se procede a generar la inserción de datos con LSB, Fig. 3 bloque 3. Los estego objetos son analizados con las métricas PSNR, SNR, MSE, y SIMM para comprobar su integridad estructural.

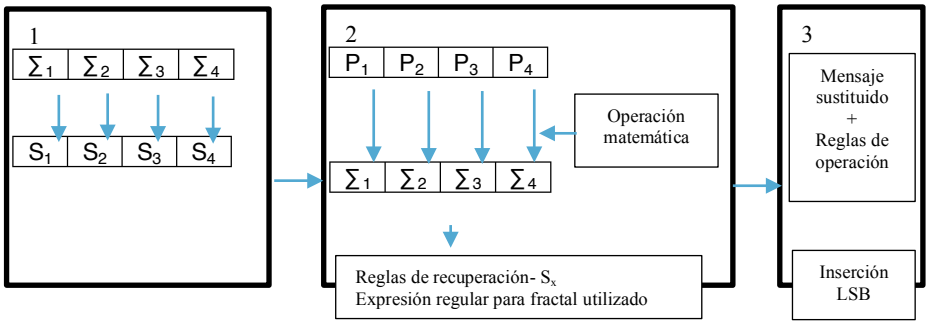

Fig. 3. Asignación de vectores y reglas de recuperación con inserción de datos codificados.

3.3 Recuperación de la información

La recuperación de la información embebida en la estego-imagen requiere emplear el proceso inverso de LSB para obtener los datos, los cuales se encuentran codificados, por lo tanto es necesario leer la regla que indica el tipo de fractal empleado para recalcular el vector de la dimensión fractal elegido previamente. Posteriormente se decodifican las reglas de recuperación de los símbolos mediante el vector obtenido y la operación inversa con que se codificaron, y así, se sustituyen los símbolos codificados con los obtenidos.

4 Resultados experimentales

En esta sección se presentan los resultados obtenidos a través del método propuesto de esteganografía y codificación, el cual se codificó en Python para Mac OS High Sierra. Las características del experimento fueron las siguientes.

1. Imágenes Lena y parrot RGB, formato JPG con un tamaño 512 x 512 píxeles.
2. Insertar 10,000 bytes en la primera ronda y posteriormente insertar 16,300 bytes para cada imagen portadora.

3. Aplicar las métricas PSNR, SNR, MSE, y SIMM.
4. Recuperar la información.

El texto de prueba contiene 30 símbolos (no se han incluido por su longitud), el fractal elegido para calcular su dimensión es el pentácopo, debido a que permitió obtener 4 variantes de su dimensión fractal, las cuales fueron: 1.8617159595009178…34, 1.8617159595009176…94, 1.8617159595009182...16 y 1.8617159595009180…75. Se tomaron 50 dígitos de precisión antes de punto decimal, debido a que las variaciones de la dimensión fractal suelen ser infinitesimales, no se consiguió mayor precisión debido a que las variables empleadas no soportaban mayor cantidad de precisión.

El vector de solución empleado fue [4, 6, 9, 13, 19, 27, 28, 39, 48, 55, 79, 96, 97, 100, 104, 111, 115, 159, 192, 193, 194, 195, 200, 201, 202, 208, 209, 216, 223, 231, 319, 324, 326] y corresponde a la segunda variación de la dimensión fractal. La operación de selección para generar las reglas de recuperación de símbolos fue una multiplicación entre el valor ASCII de los símbolos con los elementos del vector de posiciones.

En la Tabla 1, se presenta la comparación de los resultados obtenidos, las imágenes Lena0 y parrot0 representan a las imágenes con 10,000 bytes embebidos mientras que Lena1 y parrot1 representan a las imágenes con 16,300 bytes embebidos. Como puede observase para Lena0 los valores de PSNR y SNR se mantienen por encima de los 40 dB, mientras que el MSE se mantiene por debajo de los 2 puntos y SIMM está dos milésimas debajo de 1. En parrot0 se observa que los valores en PSNR y SNR son ligeramente superiores a Lena0 en ambos canales, mientras que el MSE es mejor que en Lena0 y el SIMM solo está 3 milésimas debajo de 1, por lo tanto, no se observan distorsiones en la imagen original. En Lena1 solo los valores del SNR en los tres canales descienden ligeramente por debajo de 40 dB, el MSE supera los 2 puntos y SIMM se mantiene, mientras que en parrot1, en los tres canales el PSNR y el SNR se mantiene por encima de los 40 dB y el MSE está ligeramente encima de los 2 puntos, mientras que SIMM indica un descenso de solo 4 milésimas con respecto a 1.

Imagen	PSNR canal R	SNR canal R	PSNR canal G	SNR canal G	PSNR canal B	SNR canal B	MSE	SIMM
Lena0	44.15	40.58	47.27	40.62	44.15	40.58	1.898	0.998
Parrot0	46.72	42.55	48.33	43.14	46.72	42.55	1.670	0.997
Lena1	43.53	39.97	46.08	39.43	43.53	39.97	2.285	0.998
Parrot1	45.68	41.50	46.83	41.65	45.68	41.50	2.053	0.996

Tabla 1. Resultados obtenidos en los experimentos.

En la Fig. 4, se presentan los resultados visuales de parrot y Lena, en la columna 1 y 3 se encuentra la imagen portadora, mientras que en las columnas 2 y 3 se encuentran los resultados de las estego-imágenes, en la fila 1 están las estego-imágenes con 10,000 bytes embebidos y en la fila 2 a las que se les insertaron 16,300 bytes. Como se puede observar no existen distorsiones con respecto a la imagen portadora.

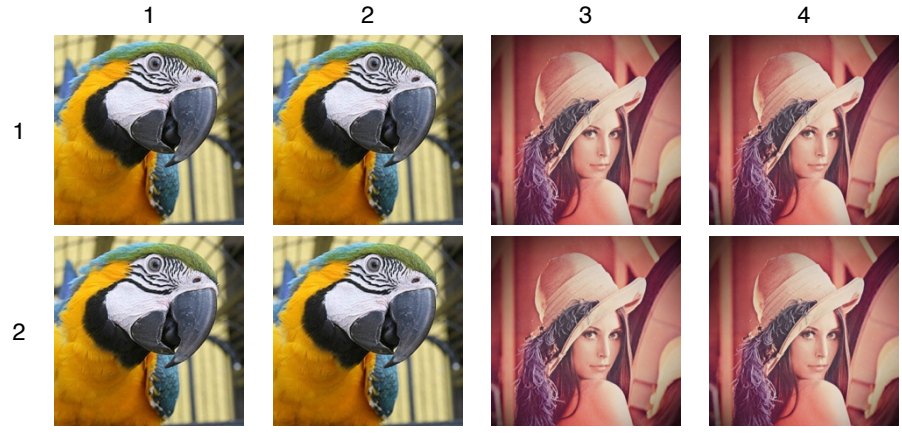

Figura 4. Comparación entre imagen portadora (columnas 1 y 3) y estego-imagen (columnas 2 y 4) con 10,000 bytes (fila 1) y 16,300 bytes (fila 2) embebidos respectivamente.

5 Conclusiones y trabajo a futuro

En este trabajo se puede observar que las ventajas de la codificación por medio de la dimensión fractal permite crear alfabetos variables en función del objeto a ocultar, para reforzar la seguridad de los datos a embeber dentro del proceso de esteganografía. LSB permite insertar tasas relevantes de información en imágenes RGB, en los experimentos realizados se comprobó que el sistema de codificación no deformó la imagen a nivel visual, además de que los niveles de PSNR se mantuvieron por encima de los 40 dB. La métrica SIMM en cualquiera de los casos nunca bajo de 0.99 puntos, mientras que el MSE superó por muy poco los 2 puntos, por lo tanto, comprueba que la estego-imagen no muestra alteraciones visuales. Como trabajo a futuro se propone el análisis de fractales no deterministas, la reducción del tiempo de inserción en las imágenes, así como el desarrollo de un mecanismo con mayor eficiencia para generar los vectores de los fractales, también se estudiarán las técnicas que permitan incrementar la cantidad de datos ocultos sin afectar la calidad de la estego-imagen y por último superar las limitaciones de la precisión del software para la generación de números fraccionarios.

Agradecimientos.

Agradecemos el apoyo brindado por el CONACYT a través de la asignación de la beca con número de registro 445998 para estudios de posgrados.

Referencias

[1] Katzenbeisser, S. and Peticolas F. A. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 2000.

[2] Singhal, S. and Rathore, R. S. Detailed Review of Image Based Steganographic Techniques. *IJCST*, v. 6, 93–95 pp, 2015.

[3] Sofloo A. G. and Aguayi, M. Steganography in Least Significant Bit. Journal of Innovative Research in Engineering Sciences, v. 3, 8–14 pp, 2017.

[4] Das, S.; Das, S.; Bandyopadhyay, B and Sanyal, S. Steganography and steganalysis: Different Approaches. *Journal of Innovative Research in Engineering Sciences*, 2010.

[5] T. Dhruw and D. N. Tiwari. Different Method used in Pixel Value Differencing Algorithm. *IOSR Journal of Computer Engineering*, 102–109 pp, 2016.

[6] Djebba, F.; Ayad, B.; Meraim, K. A.; and Hamam, H. Comparative Study of Digital Audio Steganography Techniques. *EURASIP Journal on Audio, Speech, and Music Processing*, 1–16 pp, 1 2012.

[7] Tawfiq Abdulkhaleq Abbas and Hassanein Karim Hamza. Steganography using fractal images technique. Steganography Using Fractal Images Technique, 4(2):52–61, 2014.

[8] D. Salomon and G. Motta. Handbook of Data Compression. Springer, 2010.

[9] R. C. Gonzalez and R. E. Woods. Digital Image Processing. Upper Saddle River: Pearson education, 2008.

[10] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing, 13(4):1–13, 2004.

[11] Eswari, G. S.; Leelavathy, N. and Rani, U. S. Fractal image Steganography Using non Linear Model. *International Journal of Innovative Research in Computer and Communication Engineering*, v. 2(1), 2644–2649 pp, 2014.

[12] Desai, H. V. and Desai, A. V. Image Steganography using Mandelbrot Fractal. *Trans Stellar*, v. 4, 71–79 pp, 2014.

[13] Nehete, D. and Bhide, A. Bhide. Skin Tone Based Secret Data Hiding in Images. International Journal of Current Engineering and Technology, 18–24 pp, 2014.

[14] Stoyanova, V. and Tacheva, Z. Research of the characteristics of a Steganography Algorithm Based on LSB Method of Embedding Information in Images. *Technics Technologies Education Safety*, 1–4 pp, 2015.

[15] Hussain, M. J. and Rafat K. F. Secure Steganography for digital images. *International Journal of Advanced Computer Science and Applications*, 15 pp, 2016.

[16] Ouyang, L.; Park J. H. Kau and H. Performance of efficient steganographic methods for image and text, v. 7(1), 29–33 pp, 2016.

[17] Geethaa, G. and Thamizhchelvyb, K. Application of Chaos and Fractals in Image Stegnography a Review. *International Journal of Control Theory and Applications*, v. 9(45), 95– 106 pp, 2016.