A Review of Steganography Techniques for Digital Information Transmission for Secure Channels with Digital Images

H. Caballero-Hernández, V, Muñoz-Jiménez, M. Ramos, A. Morales-Reyes, and M. Romero-Huertas

***Abstract*—The methods of hiding information developed for steganography have evolved in the direction of increasing the volume of embedded data, imperceptibility and reliability, preserving the quality of the digital image to go unnoticed. The essential methods combined symmetric or asymmetric cryptography to find security techniques. The purpose of this paper is to show different approaches used for steganography; an exciting combination of mathematical algorithms is taught to keep the essential principles of hiding information. This paper shows a compilation on the development and application of different steganography methods that have been presented in the area of information security to analyze the progress that has been made, encompassing validation methods of steganography techniques, which include metrics of quality such as PSNR, MSE, SSIM among others and statistical techniques such as analysis by histogram, RS, chi-square, among others; these techniques are great importance because they set the standard to verify the reliability and robustness of signal that contains hidden message.**

***Index Terms*—Fractals, Information security, Payload.**

I. Introducción

PARA transmitir información digital sobre un canal de comunicación público es necesario que ésta vaya protegida para evitar que sea manipulada, alterada o consultada por medios externos no autorizados. Es por ello que, a finales de la década 2010, existió un incremento notable en el desarrollo de métodos y técnicas de encriptación y de ocultamiento de la información. La esteganografía ha tomado alta relevancia en medios de comunicación como redes de computadoras y servicios de telecomunicaciones, permitiendo hacer uso de señales digitales tales como audio, texto, vídeo o imágenes, las cuales participan como portadoras de la información oculta, gracias a que la esteganografía propone algoritmos para incrustar la información de forma segura.

H. Caballero-Hernández Universidad Autónoma del Estado de México, Facultad de Ingeniería, Toluca de Lerdo, México, hcaballero240@profesor.uaemex.mx.

V. Muñoz-Jiménez Universidad Autónoma del Estado de México, Facultad de Ingeniería, Toluca de Lerdo, México, vmunozj@uaemex.mx.

M. A. Ramos Universidad Autónoma del Estado de México, Facultad de Ingeniería, Toluca de Lerdo, México (e-mail: maramos@uaemex.mx.

A. Morales-Reyes Instituto Nacional de Astrofísica, Óptica y Electrónica, Luis Enrique Erro 1, Puebla, México, aliciamoralesr@gmail.com.

M. Romero-Huertas Universidad Autónoma del Estado de México, Facultad de Ingeniería, Universitaria, Toluca de Lerdo, México, mromerohg@uaemex.mx.

La esteganografía en imágenes digitales consiste en incrustar la información secreta en un objeto portador, obteniendo como resultado un *estego-objeto* quien conserva la calidad del objeto de portada.

II. Esteganografía

La esteganografía se define como la ciencia y el arte del ocultamiento de la información, que estudia los métodos de envío de información, con la finalidad de que ésta pase desapercibida y sin un previo intercambio de datos (estego-llave) [1]. En un sistema de esteganografía existen atacantes pasivos y activos o maliciosos [2], considerando que un atacante puede probar la existencia de un mensaje oculto dentro de una imagen portadora. En el desarrollo de un modelo formal de seguridad para la esteganografía, se asume que un atacante tiene un poder computacional ilimitado, que puede ser capaz de realizar cualquier ataque o manipulación sobre la información. Si el atacante no puede confirmar su hipótesis de que existen datos ocultos en el objeto portador, entonces, el sistema puede considerarse teóricamente seguro.

En esteganografía existen elementos importantes a identificar tales como: el *objeto portador* (imagen portadora) representando a la entidad en la cual se incrusta información (mensaje), y el *estego-objeto* (estego-imagen), que representa el resultado de la fusión del mensaje incrustado en el objeto portador [3]. Existen distintas clasificaciones de las técnicas de ocultamiento de información entre las que destacan: los canales encubiertos, el anonimato, el Watermarking y la esteganografía. La diferencia entre las dos últimas áreas estriba en que en la esteganografía no importa la robustez de la señal incrustada, mientras que en Watermarking es fundamental debido a que generalmente están orientados a la protección de información [4][5].

Los métodos de esteganografía de mayor uso son aquellos en los que se sustituyen los bits menos significativos del *objeto portador* por los datos del mensaje a ocultar, y los métodos que utilizan técnicas en el dominio de la frecuencia [6][7]. Estos métodos son ampliamente utilizados por la robustez que ofrecen contra ataques estadísticos.

A continuación, se presentan los métodos de esteganografía más destacados y utilizados en la literatura aplicados a imágenes digitales. Para facilitar la lectura del documento, en la Tabla I se muestran los acrónimos empleados durante la presente investigación.

TABLA I
ACRÓNIMOS

Acrónimo	Significado
AES	Advanced Encryption Standard
AMBTC	Absolute Moment Block Truncation Coding Compression
BBPVD	Blocks Based Pixel Value Differencing
BER	Bit Error Rate
BCT	Block Truncation Coding
BPCS	Bit Plane Complexity Segmentation Steganography
BPIS	Secure Block Permutation Image Steganography
CMYK	Cyan, Magenta, Yellow and Key
CPLD	Complex Programmable Logic Device
DCT	Discrete Cosine Transformation
DFT	Discrete Fourier Transformation
DWT	Discrete Wavelet Transformation
EMD	Exploiting Modification Direction
ENMPP	Expected Number of Modifications per Pixel
ERBP	Enhanced Resilient Back-Propagation
FPGA	Field-programmable Gate Array
GIF	Graphics Interchange Format
IDWT	Inverse Discrete Wavelet Transformation
JPEG	Joint Photographic Experts Group
JPEG2000	Joint Photographic Experts Group 2000
LSB	Least Significant Bit
LZW	Lempel-Ziv-Welch
M-LSB	Modified Least Significant Bit
MSE	Mean Squared Error
MSSIM	Medium Structural Similarity Index
NCC	Normalized Cross Correlation
NFC	Near Field Communication
ORPSA	Optimal Reference Point Selection Approach
PMM	Pixel Mapping Method
PNG	Portable Network Graphics
PRN	Pseudo Ramdom Number
PRNG	Pseudo Random Number Generator
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Differencing
RGB	Red Blue Green
RS	Regular-singular
RSA	Rivest, Shamir y Adleman
SOM	Self-Organizing Maps
SSIM	Structural Similarity Index
SVD	Singular Value Descomposition
TIFF	Tagged Image File Format
TSM	Two-sides match
VQ	Vector Quantization
YCbCr	Luma Chrominance Blue and Red
YIQ	Y in-phase quadrature

El método LSB, también conocido como el bit menos significativo, consiste en modificar únicamente el bit de menor peso de un byte de información en el objeto portador. La sustitución del bit menos significativo no distorsiona el objeto portador, desde el punto de percepción humano. Una de las ventajas que presenta este método es que no aumenta el tamaño del objeto modificado, sin embargo, este puede ser detectado bajo un análisis espectral o estadístico [8]. En la Fig. 1, se muestra un ejemplo de la selección de los bits menos significativos de un pixel en una imagen RGB.

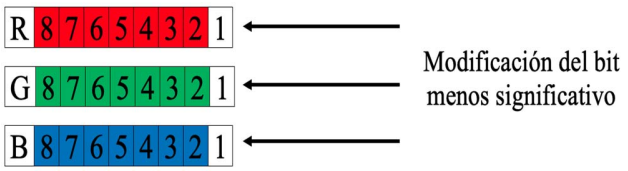

Fig. 1. Selección de los bits menos significativos de un pixel RGB para LSB

El método PVD, consiste en obtener la diferencia entre dos píxeles continuos de la imagen portadora, y sustituir esa diferencia por datos ocultos, de tal forma que la diferencia sea similar o igual a la inicial para evitar ser descubiertos. Generalmente este método es aprovechado para imágenes a escala de gris [9]. El proceso de PVD se puede observar en la Fig. 2, en ésta se presentan cuatro casos en cómo se puede seleccionar el pixel para obtener la diferencia y sustituirla por datos del mensaje a ocultar mediante el método PVD.

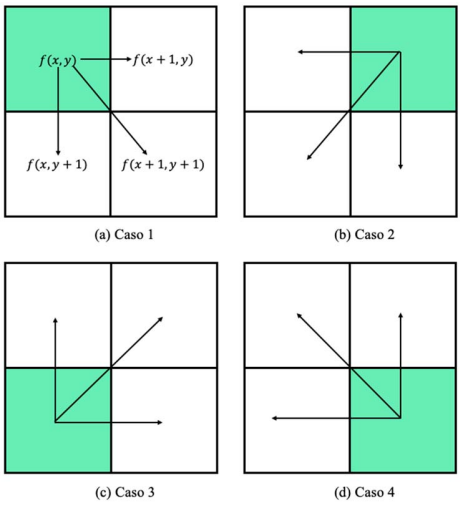

Fig. 2. Proceso de modificación de píxeles utilizando PVD [10].

El método PMM [11], permite ocultar datos en imágenes a escala de gris. La selección de incrustación de píxeles se basa en una función matemática que depende del valor de intensidad del pixel, tomando en cuenta una vecindad de ocho píxeles seleccionados en sentido contrario a las manecillas del reloj. Los píxeles seleccionados, así como sus vecinos se encuentren dentro de los límites de la imagen portadora. Antes de la incrustación de datos, se asignan bloques de dos o cuatro bits del mensaje secreto en cada uno de los píxeles vecinos en función de las características que presenta dicho pixel [12].

El algoritmo de Watershed segmenta la imagen portadora, para determinar en qué región puede incrustar datos del mensaje. Generalmente, se elige para imágenes que presentan texturas homogéneas y cuyo gradiente de intensidad es débil. Este algoritmo es altamente utilizado en procesamiento de imágenes médicas para el análisis de manchas de proteínas que se observan con técnicas de captura en geles de dos dimensiones [13].

BBPVD es una modificación del método PVD, este algoritmo toma bloques de dos, cuatro y ocho píxeles como referencia para incrementar la capacidad de incrustación de datos. Lo anterior, mejora la capacidad de ocultamiento de información en la imagen portadora y la calidad general de la estego-imagen [14].

El método BPCS es un método propuesto por Eiji Kawaguchi y Richard Eason en el año 1998, en el Instituto de Tecnología de Kyushu, Universidad de Maine. Surge como alternativa a los métodos de esteganografía que cuentan con una capacidad de incrustación menor al 10%, el método BPCS se aproxima al 50% de incrustación. Sus autores muestran que la modificación de nitidez de la imagen portadora permite incrustar

significativamente más información y que los planos de bits para imágenes a escala de gris son mejores que los planos de bits binarios. Por otro lado, el método permite que los datos se oculten de forma aleatoria, haciendo uso de una función de compresión para elevar la dificultad de ser localizados por herramientas de estegoanálisis [15].

El método de esteganografía EMD consiste en que cada dígito secreto en un sistema notacional del tipo $(2n+1)-\text{ary}$ de una relación binaria, es llevado por n píxeles en la imagen portadora, donde n es un parámetro del sistema y sólo incrementa o disminuye un pixel por uno. Cada grupo de n píxeles contiene $2n$ posibles formas de modificación, por lo que las $2n$ formas de modificación se suman, esto permite formar valores diferentes de un dígito secreto $(2n+1)-\text{ary}$ [16], lo anterior se ilustra en la Fig. 3.

	$[g_1, g_2 + 1]$	
$[g_1-1, g_2]$	$[g_1, g_2]$	$[g_1, +1 g_2]$
	$[g_1, g_2 - 1]$	

Fig. 3. Diagrama de incrustación de EMD cuando n=2.

El método TSM usa la información lateral superior izquierda de una imagen en los píxeles vecinos, para ayudar a la estimación en los píxeles en donde se va a realizar la incrustación de datos. El estego-objeto está incrustado en el orden del barrido de la señal, a excepción de los píxeles de la primera fila y la primera columna [17], como se muestra en la Fig. 4.

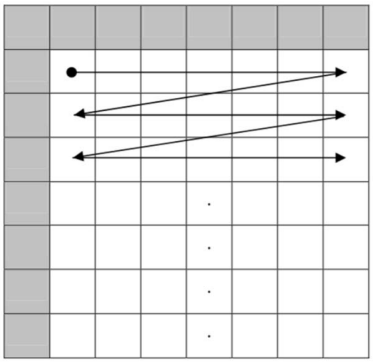

Fig. 4. Proceso de incrustación de datos con TSM [17].

Las técnicas más utilizadas en el dominio de la frecuencia son DFT, DCT y DWT [18]. La ventaja que presentan estas técnicas sobre las técnicas de dominio espacial, radica en que la información está menos expuesta a la compresión, recorte y al procesamiento de la imagen.

DFT es una técnica basada en transformaciones matemáticas que convierten los píxeles a través de una descomposición en senos y cosenos para dar el efecto de difundir la ubicación de los valores de los píxeles sobre una región de la imagen. Con este tipo de técnica se descompone una función periódica en sus harmónicos (espectro de frecuencias). Al combinar las funciones harmónicas en base 2D, es posible sintetizar funciones arbitrarias espaciales. La DFT otorga un rango dinámico de espectro muy superior en comparación a lo que los sistemas de visualización llegan a reproducir [19].

La DCT oculta el mensaje secreto en el bit menos significativo del coeficiente del coseno discreto de una imagen digital [20], además se basa en descomponer la imagen en bloques de 8x8 píxeles; de izquierda a derecha y de arriba hacia abajo, esta técnica es aplicada en cada bloque de la imagen. Los bloques de 8x8 píxeles se transforman en una matriz de 8x8 coeficientes DCT. Cada coeficiente DCT representa cuanto se necesita escalar un determinado conjunto de funciones que tienen una base de 2D para generar los píxeles originales como se ilustra en la Fig. 5.

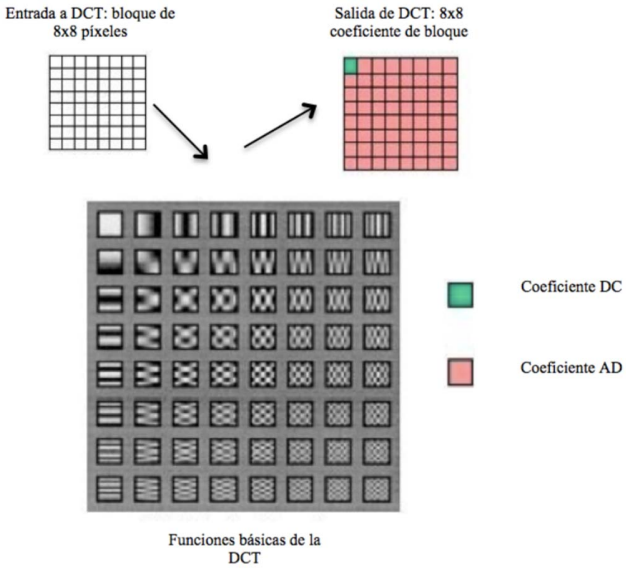

Fig. 5. Diagrama de la DCT [21].

La técnica DWT es una transformada matemática la cual permite la descomposición de imágenes en ondas llamadas ondículas a diferentes frecuencias, las técnicas en el dominio de la frecuencia son aprovechadas no sólo en imágenes digitales sino también en audio y en video [22]. Las sub-bandas que genera esta técnica están espaciadas de forma logarítmica en frecuencia y representan la descomposición de banda de octava. El proceso de descomposición está dado por la sub-banda LL1 (compuesta por LL2, HL2, LH2 y HH2) y representa los componentes de baja frecuencia en sus posiciones horizontal y vertical de la imagen. La sub-banda HH1 representa los componentes de alta y baja frecuencia de las posiciones horizontal y vertical de la imagen. La sub-banda LH1 contiene los componentes horizontales y verticales de alta frecuencia respectivamente. Finalmente, la sub-banda HL1 contiene los componentes horizontales y verticales de alta y baja frecuencia respectivamente.

A. Métricas de Evaluación de Calidad en Imágenes Digitales

Las métricas de medición de calidad permiten conocer la distorsión que existe entre dos imágenes cuando estas han sido tratadas por la aplicación de filtro u otras operaciones que pueden ser espaciales o vectoriales. Entre las métricas más utilizada se tiene a MSE [23], el error cuadrático medio, toma $f(x,y)$ la cual es la imagen portadora, $\hat{f}(x,y)$ es la estego-imagen, MN representa el tamaño de la imagen en 2D. La Ecuación (1) determina el MSE.

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

El PSNR 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 estego-imagen es alta [23]. El PSNR se define por la Ecuación (2), donde L es número de intensidades.

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

La métrica SSIM determina la similitud entre dos imágenes [24]. Generalmente se utiliza el índice MSSIM quien evalúa la calidad de una imagen. $f(x,y)$ representa la imagen portadora y $\hat{f}(x,y)$ la estego-imagen, 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. MSSIM se obtiene a través de la Ecuación (3).

$$MSSIM\left(f(x,y), \hat{f}(x,y)\right) = \frac{1}{W}\sum_{j=1}^{w} SSIM\,(f_j, \hat{f}_j) \quad (3)$$

La correlación cruzada normalizada NCC, es ampliamente utilizada como métrica para verificar la similitud o desemejanza entre dos imágenes [25]. Una de las ventajas de NCC sobre la correlación cruzada es que, es menos sensible a los cambios lineales en la amplitud de la iluminación en las dos imágenes comparadas. La NCC está confinada a un rango entre -1 y 1 para evaluar el rendimiento de la correlación normalizada. Donde f es la imagen, $\bar{t}$ es la media y $\bar{f}_{u,v}$ es la media de $f(x,y)$ en la región debajo de la imagen, dada por la Ecuación (4).

$$\gamma(u,v) = \frac{\sum_{x,y}[f(x,y) - \bar{f}_{u,v}][t(x-u,y-v) - \bar{t}]}{\left\{\sum x,y\left[f(x,y) - \bar{f}_{u,v}\right]^2 \sum_{x,y}[t(x-u,y-v) - \bar{t}]^2\right\}^{0.5}} \quad (4)$$

La prueba chi de Pearson o también conocida como chi cuadrada es una prueba no paramétrica que mide la diferencia entre una distribución observada y una teórica, con el objetivo de definir las diferencias existentes entre ambas. Se utiliza también para probar la independencia de dos variables entre sí [26].

La Ecuación (5) define el cálculo de la prueba de Pearson. Donde f_0 es la frecuencia del valor observado y f_c es la frecuencia del valor esperado.

$$\chi^2 \sum \frac{(f_0 - f_c)^2}{f_c} \quad (5)$$

La entropía es una medida estadística de aleatoriedad que se puede utilizar para caracterizar la textura de la imagen de entrada. Shannon define la entropía como una medida de incertidumbre de la información contenida en un sistema. La entropía de una variable aleatoria está definida en términos de una distribución de probabilidad, la cual mostrar una buena medida de incertidumbre [27]. La Ecuación (6) representa la entropía, en donde p es la probabilidad de ocurrencia de un suceso y log_2 es un logaritmo binario, el símbolo negativo es empleado para que la probabilidad resultante sea positiva.

$$-\sum(p * log_2(p)) \quad (6)$$

El coeficiente de correlación de dos variables aleatorias es una medida de su dependencia lineal [28]. Si cada variable tiene N observaciones escalares, el coeficiente de correlación de Pearson se define por la Ecuación (7). Donde A y B representan las variables aleatorias de las cuales se requiere conocer su dependencia lineal.

$$r = \frac{\sum_m\sum_n(A_{mn} - \bar{A})(b_{mn} - \bar{B})}{\sqrt{(\sum_m\sum_n(A_{mn} - \bar{A})^2)(\sum_m\sum_n(B_{mn} - \bar{B})^2)}} \quad (7)$$

La técnica RS fue propuesta por Fridrich y Goljan para la detección del método LSB. Esta técnica parte de una función *f* que mide la suavidad de los cambios entre píxeles de una imagen, el valor aumenta al modificar el bit menos significativo de cada pixel, debido a que las diferencias se medirán de forma estadística entre los píxeles adyacentes. R y S son bloques que están relacionados entre sí y que aumentan el valor de *f*, esta función mapea un grupo de n píxeles vecinos $(x_1, x_2, \ldots, x_n)$ los cuales están dentro de números los reales, se cuenta con una operación de volteo invertible denominada F, para formar un grupo de pixeles denominado G, el cual es clasificado dentro de tres tipos: R, S y U, como se muestra en la Ecuación (8).

$$\begin{aligned} &\text{Grupos regulares: } G \in R \Leftrightarrow f\big(F(G)\big) > f(G) \\ &\text{Grupos singulares: } G \in S \Leftrightarrow f\big(F(G)\big) < f(G) \\ &\text{Grupos inutilizables: } G \in U \Leftrightarrow f\big(F(G)\big) = f(G) \end{aligned} \quad (8)$$

Donde $F(G)$ significa aplica la operación F en cada elemento de G. Los diferentes volteos pueden conducir a diferentes píxeles y la asignación de volteo para cada pixel in G obtenido por una máscara M. Los bloques regulares son los que representan valores iguales según una función de estimación, y los bloques singulares son los que representan un cambio no esperado [29].

En las siguientes secciones, se presenta una revisión del estado del arte de esteganografía para imágenes en escala de gris e imágenes RGB.

III. Estado del Arte de Esteganografía para Imágenes en Escala de Gris

Diversas investigaciones se han enfocado en la generación de algoritmos esteganográficos, entre ellos está el trabajo de Wu et al. [30] del 2011, proponen un modelo adaptativo basándose en diferencia de valores de píxeles y descomposición de esquemas, logrando con ello, una baja distorsión en la imagen portadora y obteniendo mejores resultados que los métodos PVD, EMD, TSM, entre otros. Por otro lado, las investigaciones de Lee et al. [31] en el 2011, utilizan el algoritmo TPVD para el ocultamiento de información, empleando imágenes JPEG2000

logrando incrustar imágenes en escala de gris reduciendo el tamaño de los vectores, además de utilizar VQ para recuperar el valor residual de la compresión generada por JPEG2000, demostrando que la aplicación de TPVD en la imagen portadora, genera cambios imperceptibles dentro de la estego-imagen.

En el 2012, Gajendra et al. [32] trabajan con aplicaciones web para generar un algoritmo usando una clave como identificador único, además de aplicar la técnica guarda los datos en una estego-imagen, de esta forma, se asegura que los datos se transporten desapercibidos y que se requiera forzosamente la clave única para recuperarlos.

En el 2013, publican la técnica BPIS combinada con LSB en el trabajo de Al-Bahadili [33], en ella, refuerzan la seguridad de los datos ocultos convirtiéndolos en una secuencia binaria a la cual dividen en bloques de tamaño n. Dichos bloques son permutados por una función aleatoria y concatenándolos para formar una cadena final. El vector de permutación es dependiente de una estego-llave para ser generado, presenta una complejidad de orden $O(N!)$. BPIS trabaja con imágenes BMP, obteniendo resultados de PSNR superiores a 40 dB. Esta técnica se basa en el método LSB para incrustar datos, generando números aleatorios para modificar el orden en cómo se escriben los datos en los bloques de la imagen, la información oculta es codificada en ASCII.

En el 2013, Elgabar et al. [34], reportan que las imágenes con formato GIF obtienen resultados menos satisfactorios que en formato JPEG, esto es porque en las imágenes JPEG es posible incrustar tasas elevadas de datos. Los autores presentan una tasa de incrustación cercana a los 32,000 bytes de datos debido a su algoritmo de compresión y al aprovechamiento de la DCT, en este trabajo demuestran que su método presenta robustez media contra ataques estadísticos y alta invisibilidad. Por otro lado, en las imágenes de tipo GIF presentan espacio aceptable para incrustar datos, emplean el método de compresión LZW la cual es aprovechada para comprimir datos que sean incrustados en la imagen, presentando una invisibilidad media y es susceptible a ataques estadísticos.

BBPVD trabaja con imágenes en escalas de gris y a color, se basa en la diferencia del valor de los píxeles, esta técnica la presentan en Patil et al. [35] en el 2013 mediante la extensión de bloques basándose en PVD de dos, cuatro y ocho píxeles, con ello se logra incrementar la capacidad de incrustar información, logrando que la diferencia entre la estego-imagen y la imagen portadora no presenten diferencias visuales. Cabe señalar que los trabajos de esteganografía emplean distintos métodos de generación de secuencias aleatorias como se muestra en Jyoti et al. [36] en el 2014.

Steffy Jenifer et al. [37] en 2014 proponen un método de esteganografía para video, incrustando imágenes en archivos encriptados para ocultar la información a través de la técnica LSB, combinándola con técnicas de transformación y filtrado de enmascaramiento.

Qazanfari y Safabakhsh 2014 [38] presentan la técnica LSB++ para mejorar el método LSB+ propuesto por Wu et al. [39], lograron conservar el histograma de la imagen en el dominio espacial, incorporando bits adicionales en las imágenes. Sin embargo, produce distorsiones estadísticas y perceptivas al prohibir que algunos píxeles cambien. En su trabajo mejoraron el método LSB+ al distinguir los píxeles sensibles a modificaciones y protegerlos de la incrustación de bits adicionales, lo que provoca una menor distorsión en las matrices de coocurrencia. La técnica LSB++ ayuda a preservar el histograma de coeficientes DCT de imágenes JPEG y generalizar el método para el caso en donde se utilizan más de un bit de los píxeles de la imagen portadora. Los resultados experimentales muestran que el método LSB++ mejorado, produce menos distorsiones en las matrices de concurrencia que el método LSB++. Con su propuesta, se probó que los ataques basados en histogramas no pueden detectar correctamente las estego-imágenes producidas con o sin incrustación de bits adicionales.

En el 2015 Muhammad et al. [40], proponen el empleo de las técnicas M-LSB y PBSA, esta última técnica permite convertir los datos secretos en representaciones de bits y los complementan con una estego-llave, ofreciendo que la extracción de los datos originales sea difícil para los atacantes. En sus resultados se obtiene un promedio de 44.58 dB de PSNR en las estego-imágenes, además proponen como métricas NCC y SSIM.

Otros trabajos encontrados en la literatura incluyen formas de segmentación de imágenes diferentes a las anteriores como en Puri y Deep. [41] que, en 2015, proponen una combinación de técnicas de incrustación de datos aplicando eliminación de ruido de la imagen, posteriormente se segmenta la imagen con la técnica Watershed [42] y se genera una búsqueda de valores en los píxeles, adicionando el cifrado RSA. Los valores de PSNR obtenidos en las estego-imágenes son superiores a 65 dB.

En Khandappalavar y Shrividya [43] en el 2015, trabajan con la transformada de Arnold [44] para poder incrustar datos empleando el método LSB, con la ventaja de que los datos alterados por LSB presenten alta resistencia contra los ataques de tipo estáticos. La aplicación de la transformada permite el encriptado de los datos incrustados.

Hernández et al. [45] en el 2015, toman como método de ocultamiento de datos TPVD, utilizando bloques de bits de 2x2 píxeles, en sus resultados se comparan con el algoritmo propuesto por Peng [46], quien utiliza la técnica Wavelet Haar, obteniendo resultados de PSNR mayor en comparación al trabajo de referencia.

Otra variante de LSB se puede observar en los estudios de Gulve et al. [47], quienes presentan una técnica en donde mediante pares de bloques de píxeles se oculta información, la base del trabajo está desarrollada en LSB, los bloques empleados son de 2x3 píxeles. Las diferencias en los histogramas de la imagen portadora y la estego-imagen son despreciables. El nivel de PSNR es superior a 32 dB. Un punto por destacar es que se comparan con los trabajos de Wu [48], Chang [49] y Liao et al. [50] con resultados muy similares o ligeramente superiores ya sea en calidad o en capacidad para incrustar datos.

Hussain et al. [51] en el 2016, proponen como mecanismo de ocultamiento el algoritmo LSB y criptografía, empleando

operaciones XOR y el método SHA de 256 bits para reforzar la seguridad. Adicionalmente, agregan *Pseudo Ramdom Number*, más la inclusión de técnicas Hash para ocultar información.

Mistry et al. [52] proponen un sistema de autenticación para acceso, empleando el ocultamiento de claves en imágenes a escala de gris mediante esteganografía en combinación de teléfonos inteligentes con la capacidad de manejar NFC.

En 2017 Kasara et al. [53], proponen la detección de patrones en códigos QR, emplean LSB y DWT en la etapa de incrustación de datos, y en la fase de recuperación de datos se aplica IDWT, mientras que Al-Farraji [54] propone una revisión sobre LSB y genera una división de las imágenes seleccionadas. Incrustan datos mediante la segmentación de objetos y al finalizar generan la codificación binaria sobre la información oculta.

Darabkh et al. [55] en el 2017, proponen una serie de algoritmos basándose en variantes de PVD denominadas Quinnary PVD y Octa-PVD ambas en combinación de MLSB, con la primera técnica utilizan una partición de bloques de 3x3 píxeles en 5 parejas para cada uno de ellos, los bloques de partición y las parejas representan los píxeles vecinos, los cuales serán seleccionados para poder realizar el ocultamiento de datos. Además, minimizan el MSE y la distorsión de la estego-imagen. La imagen de prueba que utilizan es de 512x512 píxeles y el valor del PSNR para la estego-imagen es de 38 dB.

Soleymani y Taherinia [56] en 2018, presentan un método para esteganografía de un documento de texto en la imagen del objeto portador, aprovechan la propiedad dispersa de los documentos escaneados. Los documentos escaneados pasan de nivel de gris a valores binarios por medio de medio tono, posteriormente las partes incluidas en la información se extrajeron utilizando *quadtree*, la cual es una técnica que pondera una región de una imagen en donde se da prioridad a un cierto nivel de intensidad, color o textura, en este caso son las áreas donde se encuentran las secciones donde existe texto e imágenes. Separan las áreas de interés para comprimir las partes extraídas, proponen un algoritmo basado en la lectura de los bits de cadena binarios, ignorando el cero detrás del siguiente digito y convirtiéndolos a valores decimales. La capacidad de incrustación es generalmente superior a 7 bits por pixel de la imagen portadora, para la mayoría de las estego-imágenes que presentan se superan los 37 dB.

Souza-Neto et al. [57] presentan un enfoque de esteganografía para imágenes en escala de gris mediante la sustitución de los bits menos significativos, aplicaron la varianza para los bits menos significativos de la imagen para modificar la imagen portadora, de esta forma se tienen los puntos de modificación por LSB y evitar deformaciones graves en la estego-imagen.

Martinez et al. [58], presentan un método de esteganografía que realiza el ocultamiento de información en una señal portadora, sin que se perciba su presencia mediante la aplicación de la transformada discreta de ondas Haar sobre la señal portadora, y el remplazando de los bits menos significativos de una de sus señales componentes con los bits del mensaje que se oculta. El método es capaz de incrustar la información en señales portadoras unidimensionales, así como en imágenes, una vez que estas han sido acondicionadas como señales unidimensionales. Los métodos de codificación y decodificación son apropiados para implementarse en sistemas basados en dispositivos CPLD y FPGA.

Pelcastre et al. [59], su método incrusta información mediante una red neuronal capaz de generar medios tonos inversos, basados en la función atómica y la red neuronal de múltiples capas de perceptrón. Con su método, se obtienen imágenes en escala de gris con PSNR mayores a 30 dB.

Brandao et al. [60] presenta una técnica para transmitir información de manera segura, ocultando mensajes confidenciales. Emplean el método LSB para incrustar imágenes en imágenes digitales o marcas de agua secretas. Las redes neuronales artificiales se utilizan en el proceso de retiro de información cifrada, que actúa como claves que determinan la existencia de información oculta. Aplican una red neuronal para verificar la relación que existe entre los bits disponibles para la modificación por LSB para evitar ataques vía estadísticos y por análisis de ceros.

Tavares y Madeiro [61] presentan el LSB Word-Hunt (LSB WH), se basa en el rompecabezas de la búsqueda de palabras, diseñado para reducir el ENMPP en comparación con otros métodos, sus resultados muestran que LSB WH tiene un ENMPP alrededor de 0.315, siendo esta métrica una estimación para verificar el número aproximado de modificaciones en una estego-imagen, para imágenes naturales con alta entropía en el segundo y el tercer bit menos significativo. Los resultados muestran que el método es robusto ante el ataque estadístico de chi cuadrada.

La Tabla II, presenta un resumen de los autores y las técnicas propuestas de esteganografía mostradas en esta investigación sobre imágenes a escala de gris. Los trabajos han sido seleccionados en función de los resultados reportados por los autores. Remarcamos que predominan las técnicas LSB y PVD que han sido modificadas para proponer un nuevo método.

IV. Esteganografía para imágenes a color

Chuang et al. [62] proponen el su método de esteganografía para imágenes comprimidas con BTC. En el esquema propuesto se usa programación dinámica para encontrar la solución óptima de la función de mapeo biyectivo para el reemplazo de LSB con tres bits, obteniendo una baja distorsión en la estego-imagen.

En el área de imágenes a color se tiene el trabajo de Nori y Al-Qassab [63] en el 2012, desarrollan el fractal Julia para incrustar datos en imágenes RGB a través de la modificación de bits en cada canal de la imagen. Los resultados mostrados por los autores son de una estego-imagen con un PSNR superior a 79 dB y un MSE reducido y un BER sin pérdida de datos.

Sun et al. [64] en el 2013, presentan una modificación en la codificación de bloque de momento absoluto denominado AMBTC, esta técnica permite dividir las imágenes originales en bloques y luego aplica un cuantizador para reducir el número de niveles de gris en cada bloque mientras mantiene la misma media y la desviación estándar. En este estudio, proponen un método de esteganografía en el que utilizan incrustaciones de matriz con código de Hamming para incrustar un mensaje secreto en el flujo de bits AMBTC comprimido, muestran resultados aceptables en la capacidad de incrustación, velocidad de bits y eficiencia de ocultación.

TABLA II
TRABAJOS DE ESTEGANOGRAFÍA PARA IMÁGENES EN ESCALA DE GRIS SEGÚN LOS DATOS OBTENIDOS DE LAS MÉTRICAS DE CALIDAD

Autores	Técnicas empleadas	Trabajo realizado
Al-Bahadili 2013	BPIS, LSB	Combinan LSB con la permutación de bloques para dificultar la ubicación de la secuencia generada por LSB en imágenes BMP. MSE=ND y PSNR=58.71 dB.
Qazanfari 2014	LSB++	Presentan la técnica LSB++ la cual le permite eludir pruebas estadísticas como chi cuadrada.
Muhammad et al. 2015	M-LSB y PBSA	Combinación de LSB con PBSA para generar una base de ocultamiento de patrones en la imagen portadora. MSE=ND y PSNR=44.58 dB.
Puri et al. 2015	Watershed	Proponen la eliminación de ruido en la imagen portadora y se buscan regiones de píxeles para incrustar datos. Utilizan RSA como segundo mecanismo de protección. MSE=0.008 y PSNR=68.74 dB.
Hernández et al. 2015	TPVD	Aplican TPVD mediante bloques de píxeles de 2x2, obteniendo mejores resultados que la técnica Wavelet Haar empleada por F. Pen. MSE=ND y PSNR=36.04 dB.
Gulve et al. 2015	LSB	Utilizan una variante de LSB con bloques de 2x3 píxeles y obtienen resultados aceptables en cuanto a la calidad de la estego-imagen. MSE= 5.153 y PSNR= 41 dB.
Darabkh et al. 2017	PVD con variante Quinnary y Octa MLSB	Modificación de PVD con bloques de píxeles de 3x3 en agrupaciones de 5 u 8 bloques, y emplean ORPSA para minimiza el MSE. MSE=ND y PSNR=40.03 dB.
Soleymani y Taherinia 2018	Quadtree	Detección de zonas, empleo de binarización. PSNR> 37 dB Bit rate superior a 7 bits por pixel.

*ND= No disponible

Eswari et al. [65] en el 2014, aplican el algoritmo de Zhang para incrustar información dentro de imágenes fractales además de combinar la técnica con RSA. Los resultados obtenidos del PSNR son superiores a 42 dB.

En el 2014 Bhattacharyya et al. [66], aplican PMM en combinación con los planos de bits para imágenes RGB. La innovación en esta técnica es que aprovechan los planos de bits de los canales de la imagen y obtienen resultados aceptables de PSNR. Para la imagen Lena de 512x512 píxeles obtienen un PSNR de 41.67 dB, un MSE de 4.42, SSIM de 0.9332, una correlación de 0.9968 y una máxima capacidad de incrustar datos superiores a 294,000 bytes.

Prabakaran et al. [67] en 2014, proponen el DWT para la incrustación de datos y la IDWT para obtención de los datos ocultos en la imagen, además de la incorporación de la técnica SVD. Las pruebas se hicieron en imágenes con formatos JPEG y TIFF en Matlab, utilizando matrices de 512x512 píxeles con el modelo RGB y bloques de 4 píxeles con operaciones XOR, obteniendo un total del 25% de capacidad de incrustación de datos.

Nehete y Bhide [68] en el 2014, aplican el análisis de segmentación de texturas y color, la base principal de la investigación es el aprovechamiento de las variantes de los tonos de piel en un conjunto de rostros humanos. La técnica de esteganografía aplicada es DWT sobre el modelo YCbCr. En Kumar et al. [69] en el 2014, emplearon modificaciones del LSB con bloques de 64x64 píxeles, utilizando un FPGA como hardware de procesamiento gráfico.

En el 2014 Meenakshi y Kuppusmay [70], proponen una modificación de LSB para espacios de color en YIQ en imágenes con formato JPEG, aplicando rotaciones sobre RGB, realizaron pruebas extensivas sobre modelos CMYK, XYZ, YCbCr y YIQ, obteniendo un PSNR apenas superior a 30 dB para el modelo CMYK, para el resto de los modelos el PSNR es inferior a 20 dB.

La teoría de fractal se puede llevar a cabo para aplicaciones de esteganografía, como lo aplica Desai et al. [71] en el 2014, utilizando criptografía y Watermarking, emplean el fractal de Mandelbrot aprovechándolo para la compresión de la imagen a incrustar. En este trabajo la imagen a ocultar se divide en varias secciones de acuerdo con la ecuación fractal propuesta y posteriormente se incrusta mediante DCT. Las pruebas fueron realizadas tanto para imágenes en escala de gris como para imágenes RGB analizando su eficiencia a través del histograma, donde es posible apreciar nulas diferencias entre ellos.

Shobana [72] en el 2015, explota las propiedades de las sombras de imágenes que estén diseñadas en el modelo CMYK, utilizan el método LSB de 4 bits para las modificaciones en píxeles. Los niveles de PSNR de la estego-imagen son superiores a 44 dB. Stoyanova y Tacheva [73] en el 2015, aplican una modificación sobre LSB, emplean una llave criptográfica, la cual permite el control de la incrustación de datos y recuperación de estos a través del sistema simétrico de Rijndael. El PSNR de las estego-imágenes es superior a 54 dB, tomando en cuenta que usan los tres primeros bits más significativos. Las métricas de comprobación de calidad de la imagen que aplican son MSE, PSNR y SSIM.

Rabie [74] en 2015, desarrollan un paradigma basado en la esteganografía para la compresión sin pérdida de calidad en imágenes a color de alta resolución adquiridas por cámaras de 3.9 megapíxeles. Su esquema combina operaciones de procesamiento de imágenes en el dominio del espacio y la frecuencia. En el dominio del espacio, se explota la separación de colores y brillos, y en el dominio de la frecuencia, se aprovechan las propiedades espectrales de la magnitud de Fourier y la fase de la imagen en color. Los resultados experimentales presentan que superan el estándar de compresión de JPEG.

Vaishali y Kajal [75] propusieron un método de esteganografía basado en la técnica de compresión LZW y en la segmentación de plano de bits (BPCS). El método propuesto integra las dos técnicas LZW y BPCS, donde las imágenes se comprimen antes de ser transmitidas por la red. Su propuesta mejora la capacidad de ocultación de datos de la imagen en comparación con los métodos de esteganografía de imagen existentes, al tiempo que se conserva la calidad de la imagen después de incrustar el mensaje secreto en ella. Presentan cargas de inyección superiores a 370,000 bytes, logrando que los niveles de PSRN estuvieran por encima de los 50 dB.

Kaur y Deep [76] en el 2015, utilizaron imágenes de color con baja resolución, aplicándoles el método de la curva elíptica y el mecanismo de cifrado. Obtienen niveles de PSNR superiores a 70 dB para la estego-imagen, pero no se muestra el tamaño de datos incrustados, ni el tamaño de las imágenes que se utilizaron como base. Su propuesta es una variante de LSB para imágenes RGB, los datos están codificados en ASCII. Al ocultar una imagen de 128x128 píxeles en otra de 512x512

píxeles se obtiene un PSNR de 55.9 dB y el tiempo de procesamiento es de 1.3 segundos.

Naoum et al. [77] en el 2015, emplearon la DWT y ERBP, seleccionan la estego-imagen a través de un proceso de redes neuronales artificiales. La primera red es del tipo SOM, este tipo de redes fueron propuestas por Kohonen en 1982 [78], [79]. Este modelo está compuesto por dos capas de neuronas, la capa de entrada (formada por N neuronas; una neurona por cada variable de entrada) recibe la entrada y transmite a la capa de salida la información procedente del exterior, mientras que la capa de salida (M neuronas) se encarga de procesar información y formar el mapa de rasgos de Palmer [80]. La primera red neuronal es no supervisada y la segunda utiliza la retro propagación resilente. Recurren a métodos de encriptación por llaves, se ocultan imágenes de 64x64 píxeles y de 128x128 píxeles en imágenes de 256x256 y 512x512 píxeles respectivamente. Los resultados del PSNR están por arriba de los 105 dB y un MSE inferior a $2.57e^5$.

Las modificaciones de una imagen portadora mediante LSB permiten que las distorsiones no sean visibles, como lo proponen en el trabajo de Ouyang et al. [81] en el 2016, combinan operaciones XOR obteniendo resultados sobresalientes en imágenes de 512x512 píxeles al incrustar imágenes del tamaño de un 25% en relación con la imagen portadora, arrojando niveles superiores de 55 dB de PSNR.

Swain [82] propone utilizar el método LSB como el PVD en un bloque. La imagen se divide en bloques de 2×2 píxeles, por cada bloque el pixel superior izquierdo está incrustado con k-bits de datos mediante la sustitución de LSB. Posteriormente, el nuevo valor de este pixel se usa para calcular tres diferencias de valor de pixel con los píxeles superior derecho, inferior izquierdo e inferior derecho del bloque. Los bits de datos se ocultan utilizando estos tres valores de diferencia en tres direcciones, se consideran tanto los bordes horizontales como verticales. Hay dos variantes propuestas utilizando dos tablas de cuantización denominadas como Tipo 1 y Tipo 2. En las pruebas que presentan utilizan imágenes de tipo RGB con una dimensión de 512x512 píxeles, tanto para la versión Tipo 1 como Tipo 2 se comparan con los resultados obtenidos por Khodaei y Faez's [83] y obtienen un bit rate superior a 3.10, y un PSNR superior a 42 dB cuando se genera el análisis en Lena.

Al-Mutairi [84] en el 2016, compara los diferentes métodos de ocultación de imágenes secreta, utilizando dos métodos comunes de ocultamiento de imágenes de esteganografía y criptografía visual, en donde la imagen secreta original se divide en diferentes partes, para corroborar sus resultados utilizaron parámetros de calidad de reconstrucción, tiempo de ejecución, fuerza y complejidad del método.

El desarrollo de Thamizhchelvy y Geetha [85] en el 2014, incorpora el concepto de PRNG en su versión hardware, generando una secuencia de números difíciles de predecir, por lo que se le considera altamente utilizable en la generación de llaves criptográficas. A través de la generación fractales se combina la teoría del caos y la aplicación de la secuencia Fibonacci, para posteriormente aprovecharlo como marca de agua en un archivo de imagen.

Roy y Changder [86] en el 2016, utilizan la transformada de Radon en donde generan un haz de luz paralelo para conseguir la reducción de datos incrustados en la imagen, aplicando un algoritmo pseudo-aleatorio que permite cifrar los datos incrustados, y con ello proponen una matriz de codificación de datos. El método de ocultamiento es LSB y el uso de llaves criptográficas con técnicas hash reportando niveles de PSNR superiores a 56 dB.

En el 2016 Umbarkar et al. [87], proponen un método basado en la incrustación de datos de forma aleatoria que, dependiendo del tamaño de los mensajes para cifrar, se seleccionan regiones de la imagen idóneas para realizar el proceso utilizando LSB. Los resultados del PSNR en las imágenes de 512x512 píxeles con 26,214 bits incrustados son mayores a 61 dB, cuando se triplica la cantidad de datos a incrustar se puede obtener un PSNR mayor a 56 dB y con 5 veces más datos se obtiene un PSNR mayor a 54 dB. Los formatos de las imágenes que se manipularon son BMP, PNG, TIFF y JPEG. Los resultados obtenidos contra otros autores con variantes de métodos espaciales como LSBM, LSMMR, PVD, IPVD, EA-LSB y HBC son superiores a los antes mencionados.

Hardikkumar et al. [88] en el 2016, realizan una investigación sobre ocultamiento de información basándose en la generación de un fractal de Mandelbrot para localizar los datos ocultos dentro de la imagen, en éste se muestra la incrustación de una imagen la cual contiene texto. El proceso de modificación se realiza sobre imágenes RGB y se manipulan los bits a alterar, obteniendo resultados satisfactorios en relación con otras técnicas, pero tiene el problema de que la imagen a incrustar es menor a la resultante cuando se genera el fractal.

El trabajo de Geetha et al. [89] en el 2016, aplican la teoría del caos y la teoría fractal. El análisis que presenta permite obtener una idea sobre los alcances que existen en el área de teoría fractal, sobre todo al emplear los métodos de compresión a través de fractales, y las técnicas de reconocimiento de patrones de elementos cíclicos para esteganografía, aunque se observa que se combinan con los métodos LSB, DCT, DWT, entre otros.

Kim [90] en el 2016, propone un sistema de autenticación utilizando el algoritmo simétrico de cifrado AES, y un código de detección de modificaciones. Tanto el código de cifrado como el de autenticación se envían de forma independiente. El método propuesto utiliza un teléfono inteligente con un lector y grabador de tarjetas NFC y una estego-imagen para acceder a los datos grabados en la tarjeta.

La Tabla III muestra un resumen de los autores y las técnicas propuestas de esteganografía más relevantes mostradas en esta investigación para imágenes a color, como se puede observar existe una fusión de técnicas basadas en el dominio del espacio y de las frecuencias. Se observa un claro predominio de LSB en la mayoría de los trabajos reportados.

V. Discusión

El aprovechamiento de los métodos espaciales generalmente se centra en zonas homogéneas de las imágenes, en donde las modificaciones que se efectúan sobre ellas no son significativas debido a que la alteración no es perceptible. Los métodos como PVD y LSB realizan una serie de modificaciones sobre los píxeles. El primero, presenta la sustitución de un pixel dependiendo de su valor y de los píxeles vecinos para poder incrustar la información.

TABLA III
TRABAJOS DE ESTEGANOGRAFÍA PARA IMÁGENES A COLOR EN BASE A LOS RESULTADOS OBTENIDOS DE LA MÉTRICAS DE CALIDAD

Autores	Técnicas empleadas	Trabajo realizado
Nori et al. 2012	Fractal Julia, LSB	Aprovechan las características de las imágenes resultantes de los fractales utilizando el conjunto de Julia e incrustar datos con LSB. MSE= 0.27 y PSNR= 79.96 dB.
Prabakaran et al. 2014	DWT	Ocultan datos en imágenes con formato JPEG a través de DWT combinado con SVD, la imagen se segmenta en bloques de píxeles de 4x4. MSE= 0.025 y PSNR= 64.24 dB.
Meenakshi et al. 2014	LSB	Aplican rotaciones en bloques de imágenes con modelo de color YIQ, los datos son ocultados con LSB. MSE= 58.86 y PSNR= 30.43 dB.
Desai et al. 2014	Fractal de Mandelbrot, DCT	Generan imágenes con fractales obtenidos del conjunto de Mandelbrot, además se aprovecha la compresión fractal. Los datos son ocultos mediante DCT. Valores no disponibles de MSE y PSNR.
Nehete et al. 2014	DWT	Proponen un conjunto de imágenes de rostros de personas con distintos tonos de piel para ocultar datos a través de DWT. MSE=ND y PSNR=68.73 dB.
Thamizhchelvy et al. 2014	PRNG, Fractal	Incrustan datos mediante números aleatorios para ocultar la secuencia de datos. En el fractal propuesto aprovechan la serie de Fibonacci para aplicar una marca de agua. MSE y PSNR no reportados.
Stoyanova y Tacheva 2015	LSB	Proponen una combinación de LSB con sistemas criptográficos, utilizando Rijndael para su recuperación. Explotan los tres bits menos significativos de los píxeles. MSE= 2.68e-5 y PSNR= 86.21 dB.
Naoum et al. 2015	DWT y ERBP	Combinan DWT y ERBP, proponen la elección de las imágenes de cubierta por redes neuronales. MSE= $2.57e^{-5}$ y PSNR= 105.68 dB.
Vaishali y Kajal 2015	BPCS y LZW	Aplicación de compresión de datos para obtener una alta carga de incrustación de datos mediante LZW aplicando planos de bits. PSNR >50 dB.
Swain 2016	PVD y LSB	Presentan la manipulación de PVD en bloques de 2x2. Obtienen cargas de inyección superiores a 3 bits por píxeles con un PSNR que generalmente supera los 40 dB
Ouyang et al. 2016	LSB y operaciones XOR	Combinan LSB con operaciones XOR, logran ocultar hasta un 25% de la capacidad total de la imagen. MSE= ND y PSNR= 55.88 dB.
Roy et al. 2016	Transformada de Radon, LSB	Utilizan la transformada de Radon para lograr compresión de datos junto con el LSB para incrustar los datos, es resistente a ataques estáticos. MSE= 0.01 y PSNR= 57.23 dB.
Umbarkar et al. 2016	LSB	Utilizan una incrustación aleatoria de datos mediante LSB, generan un análisis previo sobre las zonas idóneas de incrustación de datos. MSE= ND y PSNR= 55.03 dB.

*ND= No disponible

El segundo, modifica los bits menos significativos de los píxeles. Si bien es cierto que son métodos ampliamente estudiados, se proponen variantes de ellos, en cuanto a la distribución de las modificaciones por vía bloques, o utilizando mecanismos de permutación en los bloques, con la finalidad de eludir mecanismos de detección de patrones de incrustación de datos.

Se observa que entre los trabajos presentados de esteganografía existe un gran número de ellos que combinan sus métodos con la criptografía, a fin de aumentar la seguridad de los datos incrustados en la imagen portadora. Comúnmente, se aplican los mecanismos tales como: RSA, AES, sistemas con llave pública y privada, entre otros, esto es una práctica común que se ha extendido a lo largo del área. Sin embargo, aunque provee una protección adicional a los datos, no satisfacen los principios de imperceptibilidad, confidencialidad y alta carga de inyección.

De los trabajos analizados el 90 % de ellos emplean al menos el MSE o PSNR como métricas de calidad, éstas se presentan como un estándar cuando se desea analizar la estego-imagen, debido a que son las métricas que describen la calidad visual que el sistema de visión humana es capaz de detectar cuando existen modificaciones en imágenes. Generalmente, cuando la técnica de esteganografía es correctamente implementada, los cambios en la imagen son imperceptibles. Por otro lado, una cantidad más reducida de autores emplean SSIM, la cual es una técnica de análisis de imágenes más sofisticada que las anteriormente mencionadas, el SSIM presenta una mejor evaluación sobre la calidad de la imagen debido a que el análisis lo hace sobre un número finito de cuadros locales de la imagen original con respecto a la estego-imagen, y no sobre una función logarítmica. De los trabajos analizados, aproximadamente un 20% emplean técnicas de verificación sobre la distribución de los datos, como es el caso de técnicas como coeficientes de correlación, normalización cruzada, análisis por histograma, entre otros. Las técnicas de estegoanálisis son minoritariamente empleadas en los trabajos de esteganografía debido a que su aplicación requiere de la generación de métodos más robustos que permitan evadir este tipo de análisis, además de que no existe una técnica de estegoanálisis que sea empleada como analizador universal que permita detectar todas las técnicas de esteganografía existentes.

Los métodos de esteganografía pueden surgir prácticamente de cualquier modelo matemático, que si se aplica de forma correcta e ingeniosa pueden dar resultados sobresalientes, es el caso de los trabajos encontrados sobre teoría del caos y fractales. Dichos trabajos han combinado de forma distinta modelos caóticos para describir secuencias de datos que pueden ser incrustadas en imágenes, a través de ecuaciones complejas que dan como resultados sistemas no determinísticos.

Los fractales analizados desde la perspectiva de representación de estructuras son aplicados para determinar elementos recursivos dentro de una imagen y llevar a cabo la compresión fractal, además, permite determinar zonas propicias para incrustar datos, o para fungir como guía para identificar en dónde se ha incrustado la información. En los trabajos reportados que utilizan fractales, observamos que éstos son

altamente redituables para incrustar información dentro de ellos, debido principalmente a su topología permitiendo alojar datos. Los fractales pasan desapercibidos cuando son enviados por un canal de comunicación, pues su uso estriba generalmente en lo académico.

Con base en el análisis efectuado en la revisión literaria presentada, en este artículo se introduce una posible propuesta de un nuevo método de esteganografía basado en el estudio de la teoría fractal, el cual se ilustra en la Fig. 6.

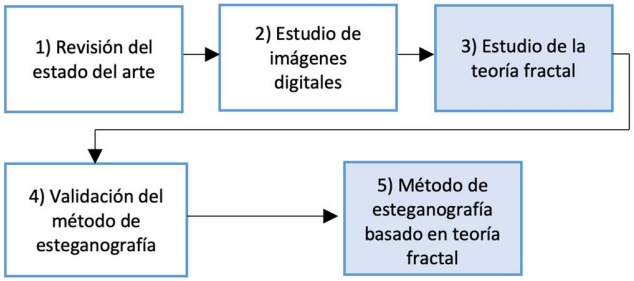

Fig. 6. Diagrama general del método propuesto de esteganografía.

Como se muestra en la Fig. 6, el método propuesto de esteganografía está basado en la teoría fractal, este es un diseño de forma general un mecanismo de incrustación de datos mediante la manipulación de los bits menos significativos para obtener una carga de datos elevada en la imagen de portada, para posteriormente generar una incrustación de los datos de forma aleatoria mediante técnicas en la frecuencia, con la finalidad de romper con la secuencia de ocultamiento del mensaje como mecanismo de confusión. En este método se propone utilizar la dimensión de Minkowski-Bouligand para calcular la dimensión fraccionaria de los fractales a utilizar. La explotación del cálculo de la dimensión fraccionaria nos permitirá la obtención de símbolos distintos a los que contaba originalmente el mensaje a incrustar de una forma dinámica y estable.

Los mecanismos de evaluación del método de esteganografía con base a la teoría fractal se proponen que sean al menos el PSNR, MSE, SSIM, coeficientes de correlación (CC), chi-cuadrada y entropía.

VI. Conclusiones

En la reciente década se ha incrementado de forma notable el interés de emplear imágenes a color para la esteganografía y aprovechar los canales adicionales con los que cuentan para incrementar la cantidad de información a incrustar. No obstante, la mayoría de los trabajos reportados utilizan como recurso de resguardo adicional de la información técnicas criptográficas, además se ha explotado la combinación de los enfoques espacial y del dominio de la frecuencia para incrustar información en las imágenes portadoras. Es notable que, los métodos LSB, PVD, DWT y DCT, y la combinación entre ellos, son ampliamente utilizados en esteganografía, obteniendo resultados ampliamente aceptables.

Existe notablemente un incremento en el interés del empleo de fractales para esteganografía, ya sea como la generación de figuras portadoras de mensaje ocultos o como base para lograr incrustar información, inquiriendo mejorar el desempeño que hasta ahora se ha reportado.

Los métodos modernos de esteganografía buscan un balance entre la cantidad de datos incrustados y el nivel de seguridad con el que se protegen los datos incrustados, buscando superar las métricas de calidad y técnicas de estegoanálisis existentes. A pesar de los avances significativos alcanzados, existen áreas de oportunidad en el apartado de superar los 8 bits por pixel de incrustación y de la misma forma sin alterar significativamente los parámetros arrojados por las métricas de calidad, técnicas de estegoanálisis y técnicas de distorsión de datos.

Agradecimientos

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

Referencias

[1] S. Katzenbeisser, F. A. Peticolas, “Information hiding techniques for steganography and digital watermarking”, London, England, Artech House, 2000, pp. 17-20.

[2] R. Roy. and S. Changder, “Steganography with projection aided payload dimension reduction and reconstruction for military cover communication”. *International Journal of Computer Applications*, vol. 139, no 3, pp. 32–37, 2016.

[3] G. Simmons, “The prisoners problem and the subliminal channel in proceedings of crypto”. Plenum Press, 1984.

[4] Herodotus, “The Histories*”*. J. M. Dent & Sons, 1992.

[5] L. M. Vargas, “Marcas de agua múltiples para autentificación y detección de adulteraciones en imágenes digitales médicas”, Cordoba, 2015.

[6] R. C. Gonzalez and R. E. Woods, “Digital image processing”. Jersey, USA. Upper Saddle River: Pearson Education, 2008, pp. 123-125.

[7] A. G. Sofloo and M. Aguayi, “Steganography in least significant bit”. *Journal of Innovative Research in Engineering Sciences*, vol. 3, pp. 8–14, 2017.

[8] S. Das, S. Das, D. Bandyopadhyay and S. Sanyal, “Steganography and steganalysis: different approaches”. *Journal of Innovative Research in Engineering Sciences*, pp. 120-125, 2010.

[9] T. Dhruw and D. N. Tiwari, “Different method used in pixel value differencing algorithm”. *IOSR Journal of Computer Engineering*, pp. 102–109, 2016.

[10] K. H. Jung and L. Young, “Three directional data hiding method for digital images. research gate”, vol. 38, no. 2, pp. 178–191, 2012.

[11] S. Bhattacharyya, A. Nandi, A. Khan, S. Roy and G. Sanyal, “Pixel Mapping Method (PMM) Based Bit Plane Complexity Segmentation (BPCS) steganography”. *World Congress on In Information and Communication Technologies*, pp. 207–214, 2001.

[12] S. Bhattacharyyya, L. Kumar, L and S. Gautam, S, “A novel Approach of Data Hiding Using Pixelmapping Method (PMM)”. *International Journal of Computer Science and Information Security*, vol. 8, pp. 207–214, 2010.

[13] X. Zhang and W. Shuozhong, “Efficient steganography embedding by exploiting modification direction”. IEEE Communications Letters, vol. 10, no. 11, pp. 1431-1437, 2006.

[14] D. D. Patil, “Text information hiding in image by BBPVD steganography techniques”. *International Journal of Advanced Information Science and Technology*, vol. 14, pp. 56–61, 6, 2013.

[15] S. S. Khaire and S. L. Nalbalwar, “Review: Steganography Bit Plane Complexity Segmentation (BPCS) technique”. *International Journal of Engineering Science and Technology,* vol. 2, no. 9, pp. 4860–4868, 2010.

[16] X. Zhang and W. Shuozhong, “efficient steganographic embedding by exploiting modification direction”. *IEEE Communications Letters.* vol. 10, no. 11, pp. 1431–1437, 2006.

[17] C. C. Chang and H. W. Tseng, “A steganographic method for digital images using side match”. *Pattern Recognition Letters.* vol. 10, no. 25, pp. 1431–1437, 2004.

[18] S. Atawneh and P. Sumari, “An overview of frequency based digital image steganography”. *International Journal of Cryptology Research*, vol. 5: pp. 15–27, 2015.

[19] J. D. Hamilton, “Time series analysis”. Princeton University Press, 1994.

[20] C. L. Velasco, J. C. López, M. Nakano and H. Pérez, “Esteganografía en una imagen digital en el dominio DCT*”*. Científica, vol. 11, pp. 169–176, 2007.

[21] P. Symes, "Video compression demystified". McGraw-Hill, 2001.
[22] F. Djebba, B. Ayad, K. A. Meraim and H. Hamam "Comparative study of digital audio steganography techniques". *EURASIP Journal on Audio, Speech, and Music Processing*, pp. 1–16, 1 2012.
[23] D. Salomon and G. Motta, "Handbook of Data Compression". Springer, USA, 5 th ed. pp. 2010, 479-480.
[24] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli E. P, "Image quality assessment: from error visibility to structural similarity". IEEE Transactions on Image Processing, vol. 13, pp. 1–13, 2014.
[25] R. M. Haralick and L. G. Shapiro, "*Computer and robot vision"*, Addison-Wesley, vol 2 pp. 316-317, 1992.
[26] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems". *Proceedings of the Third International Workshop on Information Hiding*, vol. 1, pp. 60–70, 2000.
[27] D. Huffman. "A method for the construction of minimum-redundancy codes" Proc, vol 40, 1952.
[28] R. C. Gonzalez, R.E. Woods and S.L. Eddins, "Digital image processing using MATLAB", New Jersey, Prentice Hall, 2003, Chapter 11.
[29] J. Fridrich and G. Miroslav, "Practical steganalysis of digital images - state of the art". In proceedings of spied. Springer-Verlag, pp. 1–13, 2002.
[30] N. I. Wu, K. C. Wu, and C. M. Wang, "Exploring pixel value differencing and base decomposition for low distortion data embedding". *Applied Soft Computing*, vol. 10, pp. 942–960, 2011.
[31] Y. P. Lee, J. C. Lee, W. K. Chen, K. C. Chang and I. J. Su, "High-payload image hiding with quality recovery using tri-way pixel-value differencing". *information sciences*, pp. 214–225, 1, 2012.
[32] A. P. Gajendra and L. M. Seth, "Data security using cryptosteganography in web application". *Computer Engineering and Intelligent Systems*, vol. 3, pp. 74-80, 2012.
[33] H. Al-Bahadili, "A secure block permutation image steganography algorithm". *International Journal on Cryptography and Information Security*, vol. 3, pp. 11–22, 2013.
[34] E. E. A. Elgabar and F. A. Mohammed, "JPEG versus GIF images in forms of LSB steganography". *Inter- national Journal of Computer Science and Network*, vol. 2, no. 8, pp. 86–93, 2013.
[35] D. D. Patil, "Text information hiding in image by BBPDVD steganography techniques". *International Journal of Advanced Information Science and Technology*, vol. 14, no. 6, pp. 56-61, 2013
[36] A. Jyoti, S. Banerjee and G. Gupta, "" High capacity image steganography using block randomization. International Journal of Computer Science and Network, vol 3. no. 4, pp. 559-562, 2014.
[37] K. Steffy Jenifer, G. Yogaraj and K. Rajalakshmi, "LSB approach for video steganography to embed images". *International Journal of Computer Science and Information Technologies*, vol. 5, no. 1, pp. 319-322, 2014.
[38] K. Qazanfari and R. Safabakhsh, "A new steganography method which preserves histogram: generalization of LSB++". Information Sciences, Elsevier, pp. 90-101, 2014.
[39] H. T. Wu, J. L. Dugelay and Y. M. Cheung, "A data mapping method for steganography and its application to images" 10th International Workshop on Information Hiding, vol. 5284, pp. 236-250, USA, May 2008.
[40] K. Muhammad, J. Ahmad, H. Farman and Z. Jan, "A new image steganographic technique using pattern based bits shuffling and magic LSB for grayscale images". *Sindh University Research Journal*, vol. 47, pp. 723–728, 2015.
[41] Y. Puri and G. Deep, "Image seeded steganography: steganography using seed values". *International Journal of Scientific Research And Education*, vol. 3, pp. 4004–4012, 2015.
[42] N. La Serna, S. C. Luzmila, L. Kumar and S. Gautam, "Watershed: un algoritmo eficiente y flexible para segmentación de imágenes de 2 geles". *Revista de Investigación de Sistemas e Informática*. vol. 7, no. 2, pp. 35-41, 2010.
[43] G. Khandappalavar and G. Shrividya, "Encryption of an image using least significant bit substitution method and Arnold transformation". *International Journal of Combined Research and Development*, vol. 4, pp. 534–538, 2015.
[44] Y. Wang and T. Li, "Study on image encryption algorithm based on Arnold transformation and chaotic system", I*ntelligent System Design and Engineering Application (ISDEA*), 2010 International Conference, vo1. 2, pp. 449-451, Oct. 2010.
[45] J. A. Hernández, J. R. Marcial, V. Muñoz and H. A. Montes, "A modification of the TPVD algorithm for data embedding". *Pattern Recognition*, vol. 6, pp. 74–83, 2015.
[46] F. Peng, X. Li and B. Yang, "Adaptive reversible data hiding scheme based on integer transform". *Signal Process*, vol. 92, no. 2, pp. 54–62, 2012.
[47] A. K. Gulve and M. S. Joshi, "A high capacity secured image steganography method with five-pixel pair differencing and LSB Substitution". *I.J. Image, Graphics and Signal Processing*, vol. 5, pp. 66–74, 2015.
[48] H. C. Wu, N. I. Wu, C. Wu, S. Tsai and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods". IEEE *Proceedings on Vision, Image and Signal Processing*, vol. 5, pp. 611– 615, 2005.
[49] K. Chang, H. Tu and C. P. Chang, "Adaptive image steganographic scheme based on tri-way pixel-value differencing". IEEE *International conference on Systems, Man and Cybernetics*, pp. 1165– 1170, 2007.
[50] X. Liao, Q. Wen and J. A. Zhang, "steganographic method for digital images with four-pixel differencing and modified LSB substitution". *Journal of Visual Communication and Image Representation*, vol. 22, no. 1, pp. 54–62, 2011.
[51] M. L. Hussain and K. F. Rafat, "Secure steganography for digital images". *International Journal of Advanced Computer Science and Applications*, pp. 15-21, 2016.
[52] C. Mistry, S. Muke, S. Shinde and P. Jawalkar, "NFC hardware device based access control system using information hiding". *International Journal of Innovative Research in electrical, electronics, Instrumentation and Control Engineering,* vol. 5, no. 1, pp. 69–72, 2017.
[53] N. Kasara, R. Kakade, S. Kulkarni, S. Kumbalpuri and S. Patil, "Image steganography and data hiding in QR code". *International Research Journal of Engineering and Technology*, vol. 4, pp. 2926–2928, 2017.
[54] O. I. I. Al-Farraji, "New technique of steganography based on locations of LSB." *International Journal of Information Research and Review*, pp. 3549–3353, 2017.
[55] K. A. Darabkh, A. K. Al-Dhamari and I. F. Jafar, "A new steganographic algorithm based on multi directional PVD and modified LSB". *Information Technology and Control*, pp. 16–36, 2017.
[56]. H. Soleymania and A. H. Taherinia, "High capacity image data hiding of scanned text documents using improved quadtree". Elsevier, vol. 1, no. 1 pp. 1-12, 2018.
[57] Souza-Neto, W. Dantas-Almeida and F. J. Alves-Aquino, "Esteganografia de imagens em escala de cinza pela técnica de substituição LSB" "XXXIV Simpósio Brasileiro de Telecomunicacões–SBrT2016", IEEE Transactions Latin America, pp. 769-770, 2016.
[58] A. Martínez, I. Compeeán, R. E. Fosado and R. Ávila, "Codificación esteganográfica usando la Transformada de Onditas Haar Discreta Multi-resolución". *Información Tecnológica.* , vol 4, no. 29, pp. 317-328, 2018.
[59] F. Pelcastre, M. N. Miyatake, Member, IEEE, K. Toscano, Member, IEEE, G. Sanchez, Member, IEEE and H. Perez, Senior Member, IEEE, "An inverse halftoning algorithms based on neural networks and atomic functions", pp. 1-8, 2014.
[60] A. S. Brandao and D. C. Jorge, "Artificial neural networks applied to steganography". IEEE Latin America Transactions, vol. 14, no. 3, pp. 1361-1366, 2016.
[61] R. Tavares and F. Madeiro, "Word-Hunt: An LSB steganography method with low expected number of modifications per pixel", IEEE LATIN AMERICA TRANSACTIONS, vol. 14, no. 2, pp. 1058-1064, 2016.
[62] J. C. Chuang and C. C. Chang, "Using a simple and fast image compression algorithm to hide secret information". Int. J. Computer Appl. vol. 28, no. 4, pp. 329–333, 2006.
[63] A. S. Nori and A. M. Al-Qassab, "Steganographic technique using fractal image". *International Journal of Information Technology and Business Management*, vol. 8, pp. 52-59, 2012.
[64] W. Sun, Z. Lu, Y. Wen, F. Yu and R. Shen, "High performance reversible data hiding for block truncation coding compressed images". Springer-Verlag. vol. 1, no. 1, pp. 1–10, 2013.
[65] G. S. Eswari, N. Leelavathy and U. S. Rani, "Fractal image steganography using non-linear model". *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 1, pp. 2644–2649, 2014.
[66] S. Bhattacharyya, K. Aparajita, B. Indradip and G. A. Sanyal, "Robust image steganography method using PMM in bit plane domain". *International Journal of Computer and Information Engineering*, vol. 8, no. 9, pp. 35–41, 2014.

[67] G. Prabakaran, R. Bhavani and S. Sankaran, "Dual transform color image steganography method". *International Journal of Innovative Research in Science, Engineering and Technology*, pp. 129–135, 2014.
[68] D. Nehete, and A. Bhide, "Skin tone based secret data hiding in images". *International Journal of Current Engineering and Technology,* pp. 18–24 2014.
[69] G. R. Kumar, M. M. Reddy and T. L. Kumar, "An implementation of LSB steganography using DWT technique". *International Journal of Engineering Research and General Science*, vol. 2, pp. 398–403, 2014.
[70] R. Meenakshi and K. Kuppusmay, "The use of least significant bit technique at various color spaces for secure steganography with performance evaluation". *IJARCSSE*, vol. 1, no. 5, pp. 1047–1051, 6, 2014.
[71] H. V. Desai and A. V. Desai, "Image steganography using Mandelbrot fractal". *Trans Stellar*, vol. 4, pp. 71–79, 2014.
[72] M. Shobana, "An efficient image steganographic algorithm using CMYK color model". *International Journal of Research and Innovations in Science and Technology*, pp. 25–31, 2015.
[73] V. Stoyanova and Z. Tacheva, "Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images." *Technics Technologies Education Safety*, pp. 1–4, 2015.
[74] T. Rabie, "Lossless quality steganographic color image compression". *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 6, no. 4, pp. 114-123, 2015.
[75] A. Vaishali and A. Kajal, "Increasing data hiding capacity of BPCS steganography using LZW compression technique". *International Journal of Advanced Computational Engineering and Networking*, vol. 3, no. 7, pp. 55-60, 2015.
[76] G. Kaur and E. G. Deep, "HSI color space conversion steganography using elliptic curve". *International Journal of Innovations and Advancement in Computer Science*, vol. 4, pp. 63–67, 2015.
[77] R. Naoum, A. Shihab and S. Al-Hamouz, "Enhanced image steganography system based on discrete wavelet transformation and resilient back-propagation". *International Journal of Computer Science and Network*, vol. 15, no. 1, pp. 6–18, 2015.
[78] T. Kohonen, "Self-organized formation of topologically correct feature maps". *Biological Cybernetics*, vol. 43, pp. 59–69, 1982.
[79] A. M. Gómez, "Redes Neuronales Artificiales: The Self-organizing Maps (SOM) para el reconocimiento de patrones". Universidad los Libertadores, vol. 1, no. 1, pp. 1–12, 2013.
[80] A. Palmer, "Metodología de las ciencias del comportamiento". *Universitat de les Illes Belears*, pp. 43-50, 2002.
[81] L. Ouyang, J. H. Park, and H. Kau, "Performance of efficient steganographic methods for image and text", vol. 7, no. 1, pp. 29–33, 2016.
[82] G. A. Swain, "Steganographic method combining LSB substitution and PVD in a block". *Procedia Computer Science,* Elsevier, pp. 39–44, 2016.
[83] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing". IET Image processing, vol. 6, no. 1, pp. 677-689, 2012.
[84] A. Al-mutairi, "A comparison of secret image hide methods of steganography and visual cryptography". International Conference on Engineering and Technology Systems , vol. 13, no. 2, pp. 116-120, 2016.
[85] K. Thamizhchelvy and G. Geetha, "Data hiding technique with fractal image generation method using chaos theory and watermarking". *Indian Journal of Science and Technology*, vol. 7. no. 9, pp. 1271–1278, 2014.
[86] R. Roy. and S. Changder, "steganography with projection aided payload dimension reduction and reconstruction for military covert communication". *International Journal of Computer Applications*, v. 139, no 3, pp. 32–37, 2016.
[87] A. Umbarkar, P. R. Kamble and A. V. Thakre, "Comparative study of edge based LSB matching steganography for color images". *ICTACT Journal on Image and Video Processing*, vol. 6, no. 3, pp. 1185–1191, 2016.
[88] V. D. Hardikkumar and A. D. Apurva, "Steganography of messages using Mandelbrot fractal". VNSGU *Journal of Science and Technology*, vol. 5, no. 1, pp. 13-20, 2016.
[89] G. Geetha and K. Thamizhchelvyb, "Application of chaos and fractals in Image steganography a review". *International Journal of Control Theory and Applications*, vol. 9, no. 45, pp. 95–106, 2016.
[90] H. Kim, "A Study on the cryptographic algorithm for NFC". *Indian Journal of Science and Technology*, vol. 9, no. 1, pp. 1–5, 2016.

Héctor Caballero-Hernández was born on May 15, 1988, in Tapaxco, State of Mexico, Mexico. He received the Engineering degree in Computing from Universidad del Estado de México, México in 2011, and he is a PhD student in Engineering Science. His research themes are steganography and science computing based on natural language.

Vianney Muñoz-Jiménez is researcher professor in Image Processing and Computational Vision at the Autonomous University of the State of Mexico. In 2009. She received her PhD from Paris 13 University, France. Her research work is about computational vision, image processing, video compressing, etc.

Marco A. Ramos is researcher professor in Artificial Intelligence and Virtual Reality at the Autonomous University of the State of Mexico. He got his PhD from Toulouse University on 2007, France. His research themes are: Artificial Life, animation techniques, distributed systems, Intelligent agents, etc.

Alicia Morales-Reyes is a titular researcher in the Computer Science department at the National Institute for Astrophysics, Optics and Electronics (INAOE) in Tonantzintla, Mexico. She received her PhD degree from the University of Edinburgh in 2011. In 2006, she received the MSc degree in Computer Science from the INAOE.

Marcelo Romero-Huertas is researcher professor in computer science at the Autonomous University of the State of Mexico. He obtained his doctorate from the University of York in 2010, United Kingdom. His research topics are anthropometric points, image processing, pattern recognition, etc.