DOI: http://dx.doi.org/10.26483/ijarcs.v11i3.6615

ISSN No. 0976-5697

Volume 11, No. 3, May-June 2020

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SPATIAL AND FREQUENCY DOMAIN COMBINATION BASED IN SCHEMES TOSTEGANOGRAPHY IN RGB DIGITAL IMAGES USING CANTOR SET

Hector Caballero-Hernandez
Department Engineering Science
University Autonomous of State of Mexico, UAEMex
Toluca de Lerdo, Mexico

Vianney Muñoz-Jimenez
Department Engineering Science
University Autonomous of State of Mexico, UAEMex
Toluca de Lerdo, Mexico

Marco A. Ramos-Corchado
Department Engineering Science
University Autonomous of State of Mexico, UAEMex
Toluca de Lerdo, Mexico

*Abstract:*This paper describes a proposal based on the combination of based methods on the spatial domain and the frequency for the hiding of data in RGB digital images, by substituting bits in pixels less important and modifying coefficients DWT to increase data security. The main idea of this research is to take advantage of the selection logic of the Cantor set in defined sections of the cover images, where the pixels are regrouped, and in these sections the pixels that will be used to hide data are selected. This proposal has the advantage that the application of the logic of the Cantor set allows selecting at different levels a variable number of pixels to be modified and increasing the security of the steganography system. The results obtained are high loads of data embedding, as well as the approval of quality metrics for digital images how PSNR, MSE, SSIM and others. The dataset image used in the experiments is UCIDdue to the large number of images available for embedding messages in images.

Keywords:DWT; spatial domain; bit substitution; steganography, Cantor set

I. Introduction

Steganography is the science of hiding information in digital objects. A cover object representing the entity in which the message to be hidden and a stego-objects afusion of the hidden message with acoverobject [1], [2].

The most widely used steganography methods are those in which the least significant bits of the bearer object are replaced by the data of the message to be hidden, and the methods that use techniques in the frequency domain. These methods are widely used for the robustness and offer against statistical attacks.

Among the best-known techniques in steganography is Least Significant Bit (LSB) method, also known as the least significant bit, consisting of modifying only the least significant bit of an information byte in the carrier object. Substituting the least significant bit does not distort the carrier object, from the point of human perception, it can be detected under spectral or statistical analysis [3].Pixel Value Differencing (PVD), which consists of obtaining a difference between two continuous pixels of the carrier image, and replacing that difference by hidden data, so that the difference is similar or equal to the initial to avoid being discovered. This method is generally used for grayscale images [4]. In the PVD process, you can select the pixel to obtain the difference and replace it with data from the message to be hidden using the PVD method.

Bit Plane Complexity Segmentation Steganography (BPCS) method is a method proposed by Eiji Kawaguchi and Richard Eason in 1998 at the Kyushu Institute of Technology, University of Maine. It appears as an alternative to steganography methods that have an embedding capacity of less than 10%, the BPCS method approaches 50% embedding. This method allows data to be hidden in a random way, making use of a compression function to increase the difficulty of being located by steganalysis tools [5].

The techniques most frequently used in the frequency domain such asDiscrete Fourier Transformation (DFT), Discrete CosineTransformation (DCT) [7] and Discrete Wavelet Transformation (DWT) [6] allow us to work modifying coefficients its obtain to modify the values and allow to implement a system of data representation. One advantage of these techniques over spatial domain techniques is that the information is less exposed to compression, cropping and image processing [9], [10], [18].

One of the techniques that has been exploited in steganography is the use of fractals, whose term was proposed by Benoit Mandelbrot, because these figures whose metric dimension is represented by a fractional number. Fractals can be represented as mathematical sets whose patterns are similar to each other. Fractals can be exactly the same at all scales. These objects have a fractal dimension that generally exceeds its topological dimension and is between integers and fractional numbers [11]. Fractal dimension can be calculated through Equation(1).

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

Where
D= Euclidean dimension
MB= Minkowski-Bouligand dimension
l= dimension number

N= number of auto similar objects
ε= linear side.

In fractal theory, there is an interesting set, the Cantor set, allows us to establish an analysis of how data segments can be divided, and then iteratively repeat the same pattern, generally this process comes from taking two thirds of a segment of one unit, and the pattern repeats in two-thirds of three segments, as seen in Fig. 1.

Figure 1. Cantor set division.

A relationship between the Cantor set and a channel of an RGB image is defined by:

Let $\{K_\alpha\}_{\alpha\in A}$ be a non-empty family of subset of adjacent pixels in a metric space X, if the intersection of any finite sub-collection of $\{K_\alpha\}_{\alpha\in A}$ is not empty $\bigcup_{\alpha\in A} K_\alpha$.

Let C_n be an interval [0,1] divisible into three segments and separated by three segments $\left(\frac{1}{3}\middle|\frac{2}{3}\right)$.

Let $C_1 = \left[0,\frac{1}{3}\right] \cup \left[\frac{2}{3},1\right]$ divide both intervals, each into three parts and separate the central thirds.

Let $C_2 = \left[0,\frac{1}{9}\right] \cup \left[\frac{2}{9},\frac{3}{9}\right] \cup \left[\frac{6}{9},\frac{7}{9}\right] \cup \left[\frac{8}{9},1\right]$

The sequence of compact set of pixels C_n is obtained, such that,

1.- $C_1 \supset C_2 \supset C_3 \supset \cdots$
2.- $C_n$is the union of 2^n intervals, each of length 3^{-n}pixel segments, Equation (2):

$$C = \bigcup_{n=1}^{\infty} C_n \qquad (2)$$

$C$is a closed compact set and a subset of a compact and non-empty set, without, any segment of the form, Equation (3).

$$\left(\frac{3k+1}{3^m},\frac{3k+2}{3^m}\right) \qquad (3)$$

Where k and m are positive integers.

As every pixel segment (α, β) contains a segment with the previous form, if it is fulfilled, Equation (4):

$$3^{-m} < \frac{\beta-\alpha}{6} \qquad (4)$$

As it has been expressed in the previous paragraphs, Cantor set allows groups to be formed through the selection of subsets from thirds, thus, following the same logic, it can be used as a pattern of pixel selection in images at different scales.

To assess the quality of digital images that have undergone a transformation process, metrics are available to measure the level of image distortion. Among the most used metrics is Mean Square Error (MSE) [12] represented by Equation (5).

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left[f(x,y)-\hat{f}(x,y)\right]^2 \qquad (5)$$

Where
$f(x,y)$=the cover image
$\hat{f}(x,y)$= the stego-image
MN= represents the 2D image size.

Another of the metrics to validate is Peak Signal Noise to Radio (PSNR), which is defined as a limit where the relationship with the error receiver is approached by the human vision system [12]. PSNR is defined by Equation (6).

$$PSNR(dB) = 10log_{10}L^2/MSE \qquad (6)$$

where

L = number of intensities.

SSIM metric determines the similarity between two images [13]. Generally, the MSSIM index is used, which assesses the quality of an image $f(x,y)$ represents cover image and $\hat{f}(x,y)$ the stego-image, f_j and $\hat{f}_j$is the contents of local window j_{th}, and W is the number of local windows of the image. MSSIM is obtained through Equation (7).

$$MSSIM\left(f(x,y),\hat{f}(x,y)\right) = \frac{1}{W}\sum_{j=1}^{W} SSIM\,(f_j,\hat{f}_j) \qquad (7)$$

II. Literature Survey

In steganography area there are a diverse number of applications and techniques for information concealment. This section shows relevant works in the area of steganography.

In Ouyang et al. [14] in 2016combine XOR operations obtaining outstanding results in images of 512x512 pixels by embedding images of the size of 25% in relation to the carrier image, yielding higher levels of 55 dB of PSNR.

In this work Swain [15] proposes to use LSB method as PVD in a block. The image is divided into 2 × 2 pixel blocks, for each block the upper left pixel is embedded with k-bits of data by substituting LSB. Subsequently, the new value of this pixel is used to calculate three pixel value differences with the upper right, lower left and lower right pixels of the block. Data bits are hidden using these three difference values in three directions, both horizontal and vertical edges are considered. There are two proposed variants using two quantization tables called Type 1 and Type 2. In the tests they present and use RGB-type images with a dimension of 512x512 pixels and are compared with the results obtained by Khodaei and Faez's [16], obtaining a bit rate greater than 3.10, and a PSNR greater than 42 dB when the analysis is generated on the Lena image.

Al-Mutairi [17] in 2016, compares the different secret image concealment methods, using two common steganography image concealment methods and visual cryptography, where the original secret image is divided into different parts, to corroborate their results. They used parameters of reconstruction quality, execution time, strength and complexity of the method.

In Thamizhchelvy and Geetha [18] in 2014, incorporates the concept of PRNG in its hardware version, generating a sequence of numbers that are difficult to predict, which is why it is considered highly usable in the generation of cryptographic keys. Through fractal generation, chaos theory and the application of the Fibonacci sequence are combined, to later use it as a watermark in an image file.

Roy and Changder [19] in 2016, use the Radon transform where generate a parallel light beam to achieve the reduction of embedded data in the image, applying a pseudo-random algorithm that allows encrypting the embedded data, and with it they propose a data coding matrix. Hiding method is LSB and the use of cryptographic keys with hashing techniques reporting PSNR levels higher than 56 dB.

In 2016 Umbarkar et al. [20]propose a method based on the embedding of data in a random way that, depending on the size of the messages to encrypt, suitable image regions are selected to carry out the process using LSB. The results about PSNR in the images of 512x512 pixels with 26,214 embedded bits are greater than 61 dB, when the amount of data to be embedded is tripled, a PSNR greater than 56 dB can be obtained and with 5 times more data a PSNR greater than 54 dB. Results obtained against other authors with variants of spatial methods such as Least Significant Bit Matching (LSBM), PVD, IPVD, EA-LSB and Hiding Begin Corner (HBC) are superior to those mentioned above.

Hardikkumar et al. [21] in 2016carried out an investigation on hiding based on the generation of a Mandelbrot fractal to locate the hidden data within the image, in which the embedding of an image which contains text is shown. Modification process is performed on RGB images and the bits to be altered are manipulated, obtaining satisfactory results in relation to other techniques, but it has the problem that the image to embed is less than one resulting when the fractal is generated.

The combination of security techniques such as RSA allow the message to have an extra layer of security as in the work of Ambika et al. They apply DWT to embed encrypted messages in color images with dimensions of 512 x 512 pixels, the hidden message is grayscale images. They get 31.792 dB and 0.86612 MSE points.

Geetha et al. [22] in 2016 apply chaos theory and fractal theory. The analysis presented presents an idea about the scope that exists in the area of fractal theory, especially when using compression methods through fractals, and the techniques of pattern recognition of cyclic elements for steganography, although it is observed that itis combined with the LSB, DCT, DWT methods, among others.

A combination of security techniques such as RSA allow the message has an extra layer of security as in Ambika et al. [23]apply DWT to embed encrypted messages in color images with dimensions of 512x512 pixels, hidden message is grayscale images. They get 31.792 dB and 0.86612 MSE points.

In Monika and Singh 2016 [25] they propose in their research to hide the text of a message in the pixels of the image in such a way that the human visual system cannot differentiate between the original image and the stego-image. They calculate the PSNR of the images as a quality metric. They take advantage of the modification of the bits coming from blue pixels, because it is less susceptible to modifications both visually and statistically based on Hecht's studies [26].

In the work of Shashi Kiran et al. [24] propose an ingenious technique using DWT to decompose the cover images in their R, G and B channels and later obtain LL, LH, HL and HH sub bands from cover image, the images to be hidden are decomposed in their R, G and B channels to later be embedded by LSB in the MSB. In this paper they embed one image for each channel of the cover image and obtain average PSNR scores greater than 35 dB for the stego-images, while the images recovered from their average in PSNR have an average of 29 dB.

In Zenati et al. 2019 [27] propose a system to embed gray scale images, in documents converted to gray scale images by means of a modeling called Beta Elliptic, with the purpose of hiding the Beta Elliptic signature as secret data in the image of the host document. The system has two main phases, the first is the embedding of data using steganography, they use a nominee key point detector Binary Robust Invariant Scalable Key points (BRISK) to identify the embedding positions in the image of the host document. The Beta Elliptic signature becomes a sequence of secret bits through the pre-possession of the signature. The second part consists of using a system made up of Binary Transformation and Huffman Compression. The obtained sequence is added in the first least significant bit (LSB) of the embed positions in the image of the host document. The SSDIS-BEM system allows you to hide the Beta elliptical signature at specific points, extracted by the BRISK detector in various types of images of the document in gray scale. The authors' proposal allows to directly embed the Beta elliptic signature based on the domain of space using LSB. The authors propose as performance metrics PSNR, SSIM, HVS and Bit Error Ratio (BER), obtaining outstanding results in PSNR with higher scores that range between 80 dB and 92 dB in the three datasets that are used, on the other hand, the averages of the SSIM scores are greater than 0.993 points. Analyzing the works presented, we can see that most of these works present development in space techniques such as LSB, PVD, on the other hand, one of the novel contributions is the use of fractals for data embedding. In the following section we present method that includes techniques in the domain of space and frequency domain to embedding data in a digital image. On the other hand, it has been analyzed to take advantage of spatial techniques and frequency domain to offer a method with the ability to embed high data rates in addition to not being lost when applying information retrieval.

III. METHOD PROPOSED

In this method we propose the embedding of data through LSB, the message to be embedded presents a conversion of its characters through ASCII which will be distributed through channels R, G and B, where they are subsequently subjected to manipulation by means of DWT to generate a layer that protects the data in such a way that the original inlay patterns are altered and in this way they are not directly recovered.

Proposal method for steganography consists in four stages as shown in Fig. 2.

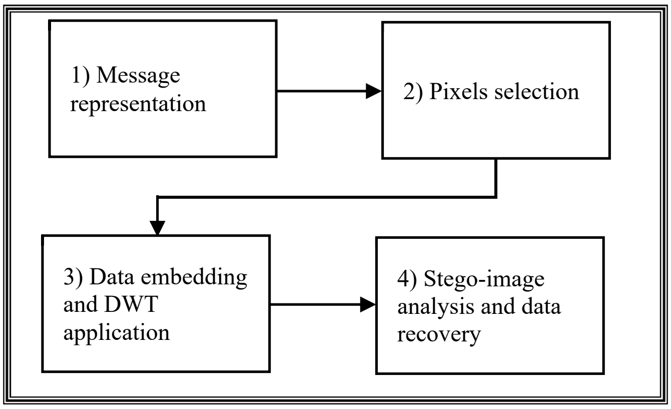

1) Message representation
2) Pixels selection
3) Data embedding and DWT application
4) Stego-image analysis and data recovery

Figure 2. General diagram of the proposed method

1.- Message representation.All alphabet symbols are extracted from the message andafter are converted in ASCII. The embed message is represented by M_e, a cover image is named as I_p, M_t is a product of transforming M_e into ASCII by ASCII function (M_e), this is converted to UTF-8 binary code by function M_{utf-8} = UTF8(M_t) this final string is binary and will be the final string to insert. Stage 1 is represented by Algorithm 1.

Algorithm 1. Message representation

```
Begin
Read message $M_e$
Convert $M_e$ : $ASCII(e)$store in$M_t$

Binarize $M_t$: $M_{utf-8} = UTF8(M_t)$,
Store $M_{utf-8}$ in $binaryfileUTF - 8$
End
```

2.- Pixels selection. In this stage we manipulate a cover image to separate its three channels and select the pixels of these channels using the logic of the Cantor set, choosing two out of three pixels. I_p image requires that the embedding logic be modified in an apparent way so that the data is not exposed in the first instance, for this it is proposed that the pixels of I_p be distributed in sets where two elements of three are taken, using I_p as cover image, the data embedding function is applied to this image. During separation process an increment of one unit is applied randomly using the random function which varies from 0 to 1. Algorithm 2 shows the separation of the channels from cover image.

Algorithm 2.Channel separation

```
Begin
$I_p$ = Extraction (Dir-imagecover)
Create $PR$, $PG$, P$B$ channels with $id$, $x$, $y$, value fields
Initialize $value$, $value1$, $value2$, i, $e$ = 0;
Matrix from $I_p$= Mat [i, e, channel]
Mat [i, e, 0] = R, Mat [i, e, 1] = G, Mat [i, e, 2] = B

Begin cycle $i<M$
Begin cycle $e<N$
$value$=int(Mat[i,e,0]) + random()
$value1$=int(Mat[i,e, 1]) + random()
$value2$=int(Mat[i,e,2]) + random()

Insert values ($PR$, $counter$, $i$ , $e$, $value$)
Insert values ($PG$,$counter$, $i$ , $e$, $value1$)
      Insert values ($PR$ , $counter$, $i$ , $e$, $value2$)
   counter = counter + 1

   End cycle
   End cycle

   $I_r$ = $Pr + Pg + Pb$

   End
```

Cantor set allows determining the selection of a space that is seen as a subset, from which a binary set represented as [0,1] is taken, in this case a section of pixels has been taken which represent a set 1, which must be divided into three thirds. The central third will be eliminated, the two lateral thirds must be preserved (two pixels preserved, and one discarded for embedding), this process is repeated until finished with pixels available to generate a division. Pixels not discarded are those selected to perform the data embedding process, as shown in Algorithm 3.

Algorithm 3. Pixel selection

```
Begin

$R, G, B = I_r$
                              $[\mathrm{M}, \mathrm{N}] = I_r$
$Cir_{xy} = R, Cig_{xy} = G, Cib_{xy} = B$

   Begin cycle
$\left(\frac{1}{3} \middle| \frac{3}{3}\right) = M_1, N_2$
$C_{ixy} = \left(\frac{3k+1}{3^m}, \frac{3k+2}{3^m}\right)$
   End cycle

$C_n = Cir_{xy}, Cig_{xy}, Cib_{xy}$

End
```

In Algorithm 3 I_r is divided intothree channels and subsequently it is placed in their values in the matrices Ci_{xy}, from each of these matrices 2 out of three pixels are selected in one cycle and finally the set C_n is formed, which contains the selected pixels.

3.- Data embedding and DWT application. This stage consists in replacing the least significant bits in the image. When pixels selected in C_n matrix are completely stored andfinal message is encoded, proceed to embed M_{UTF-8}, using the embedding function that modifies the bits of lesser weight based on the bits of the message. The embedding process is shown in Algorithm 4.

Algorithm 4. Data embedding

```
Begin
constant
$[R_{xy}, G_{xy}, B_{xy}] = I_r$

$[Cir_{xy}, Cig_{xy}, Cib_{xy}] = C_n$
Initialize variables $r$ = 0 Binarytemporal = ''

Begin cycle $index$
   Begin cycle $x < M_1$
   Begin cycle $y < N_1$

   If $(temporal < M_1 * N_1)$
$Binarytemp =$
$Binary\ (Cir_{xy})$.posicion[bimindex]+ $M_{utf8}[index]$
         $Cir_{xy} = Decimal(Binarytemp)$
temporal= temporal+1
         index= index+1
End If

         $If (temp < M * N * 2\ and\ temp > M_1 * N_1)$
$Binarytemp = Binary\ (Cig_{xy})$. allocation[bit
guide]+ $M_{utf8}[index]$
```

```
$Cig_{xy} = Decimal(Binarytemp)$
        temp= temp+1
        index= index+1
        End If
    If (temp <$M * N * 3$ and temp>$M_1 * N_1 * 2$)
      $If (temp < M * N * 3 \text{ and } temp > M_1 * N_1 * 2)$
        $Binarytemp = Binary\ (Cib_{xy})$.allocation
                [bit index]+ $M_{utf8}[index]$
              $Cib_{xy} = Decimal(Binarytemp)$
        Temp= Temp+1
        index= index+1

                End if
        End cycle
    End cycle
    End cycle
$E_n = Cir_{xy} + (R_{xy} - Cir_{xy}), Cig_{xy}$
                $+ +(G_{xy} - Cig_{xy}), Cig_{xy} + (B_{xy} - Cib_{xy})$
    Begin cycle
        [LL, LH, HL, HH] = DWT($E_n$)
        $[LL, LH, HL, HH] + constant$
End cycle
$E_n$= IDWT($LL, LH, HL, HH$)
End
```

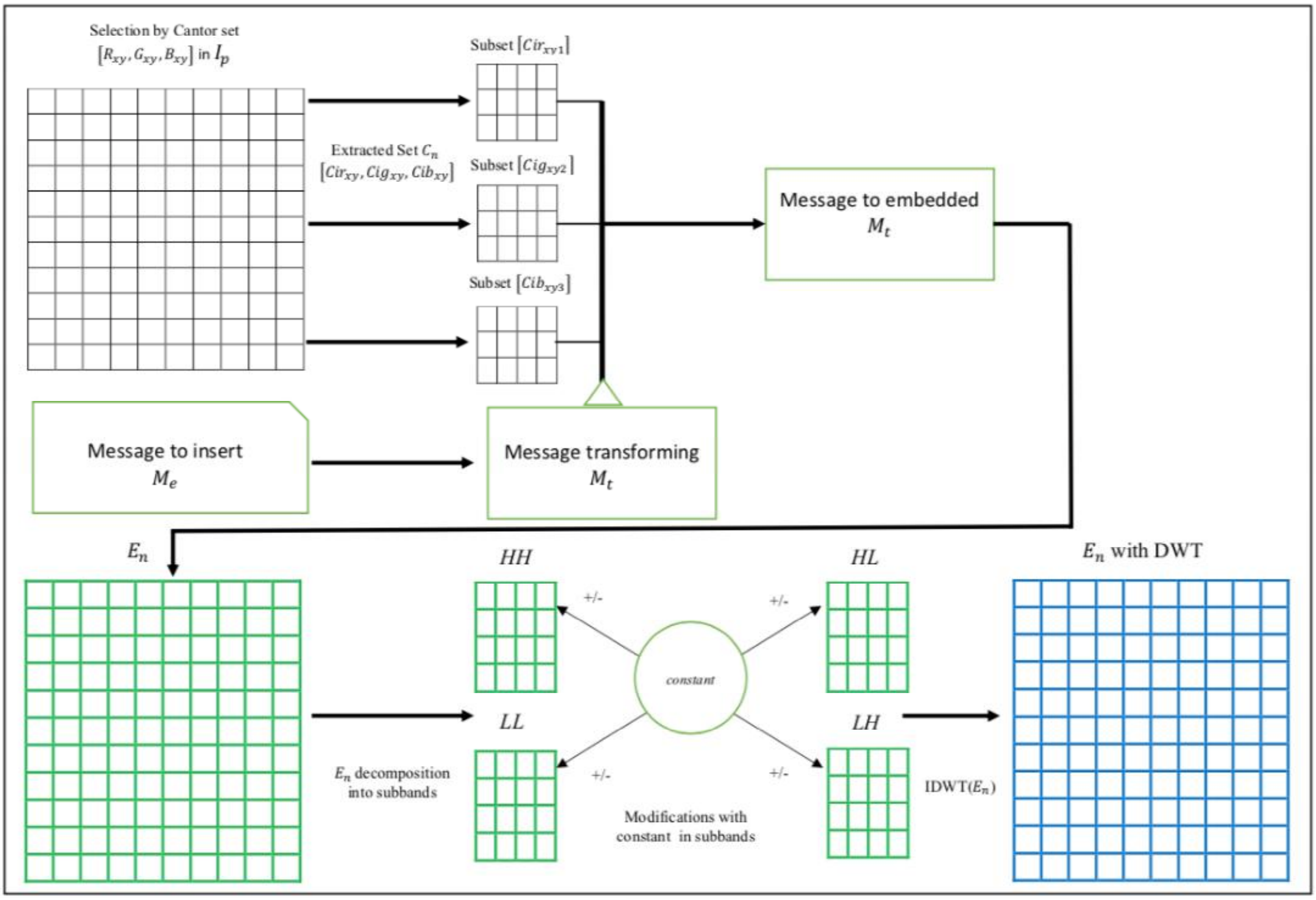


Figure 3. Process to hide M_e in I_p

In Algorithm 4, the pixels belonging to the 3 channels that made up C_n are obtained to embed the data of the binarized M$_{\text{utf-8}}$ message. Final stego-image will be named E_n and contains the embedded message. E_n is reconstructed by the sum of the positions of the selected sets of C_{xy} and of the unselected channels of the R, G and B channels of the image I_p, later the sum of coefficients is applied by means of the DWT and finally the inverse function is applied of the DWT named as IDWT to rebuild E_n.

Graphically, Fig. 3 shows the data embedding process, as specified in the previous 4 algorithms, where the cover image $I_p$is divided into matrices that represent the sets extracted by theoperation of the Cantor set. Subsequently, the data on the selected matrices are embedded, either those corresponding to the first and third third or the second third, later the message is converted into ASCII Code and a binary message with UTF-8 to be embedded. When the message has been embedded, stego-image E_n is generated. In this image, the operation by DWT is applied to generate the data hiding modification.

4.- Stego-images analysis and data recovery. In this stage we modified pixels using DWT by adding a constant in its respective sub-bands. The message is also retrieved, and stego-image is evaluated, using the PNSR, MSE, SNR and SSIM.

At the end of the process, amount of data correctly recovered is established,executing the process of selecting the pixels chosen by Cantor function, as indicated in Algorithm 5.Fig.4 represents data recovery, where E_n is divided into the 4 DWT subbands (HH, HL, LH and LL). In this process, the added value for all pixels is eliminated so that it is continuous and constant for eliminate the effect of concealment on the original values of the message that was embedded in the stego-image. After removing the values provided by the DWT, the Cantor function is again used to extract the set of matrices in which the message is embedded and start with the reverse process of data extraction. When acquiring the subset data, this data goes from UTF-8 binary to ASCII and finally get M_e.

Algorithm 5: Data recovery

```
Begin
$constant\ = c$
Begin cycle
  [LL, LH, HL, HH] = DWT($E_n$)

$[LL, LH, HL, HH]$ - $constant$
End cycle

$E_n$= IDWT($LL, LH, HL, HH$)

$E_n$ cycle begins
$\left(\frac{1}{3}\middle|\frac{3}{3}\right) = M_1, N_2$
        $C_n = \left(\frac{3k+1}{3^m}, \frac{3k+2}{3^m}\right)$
End cycle

    to:
$[M, N] = E_n$
$Cir_{xy}, Cig_{xy}, Cib_{xy} = Descomposed(C_n)$
channels = ($nochannels(E_n)$

    i = 0, e = 0, change_channel = 0
    concatenator = ‘’
    Begin cycle change_channel <channels
    Begin cycle $i$<$M$
    Begin cycle $e$<$N$
        If (search.concatenator.check)!= 1)
concatenator + $Bitselection(E_n[M, N, change\_channel])$
      [M, N, change_channel])
    End If
    End cycle
    End cycle

    File = DecoderUTF-8(concatenator)
    File = DecoderASCII(File)

    If (File.search (verification string) == 0))
                        $File = E_n$
    Else If
                        $File = E_n$
    Go to a:
    End if
    End
```

In Algorithm 5 coefficients added by DWT are eliminated, E_n pixels are selected using Cantor selection logic, to later extract the least significant bits and generate the inverse process of encoding with UTF-8 with function ASCII and

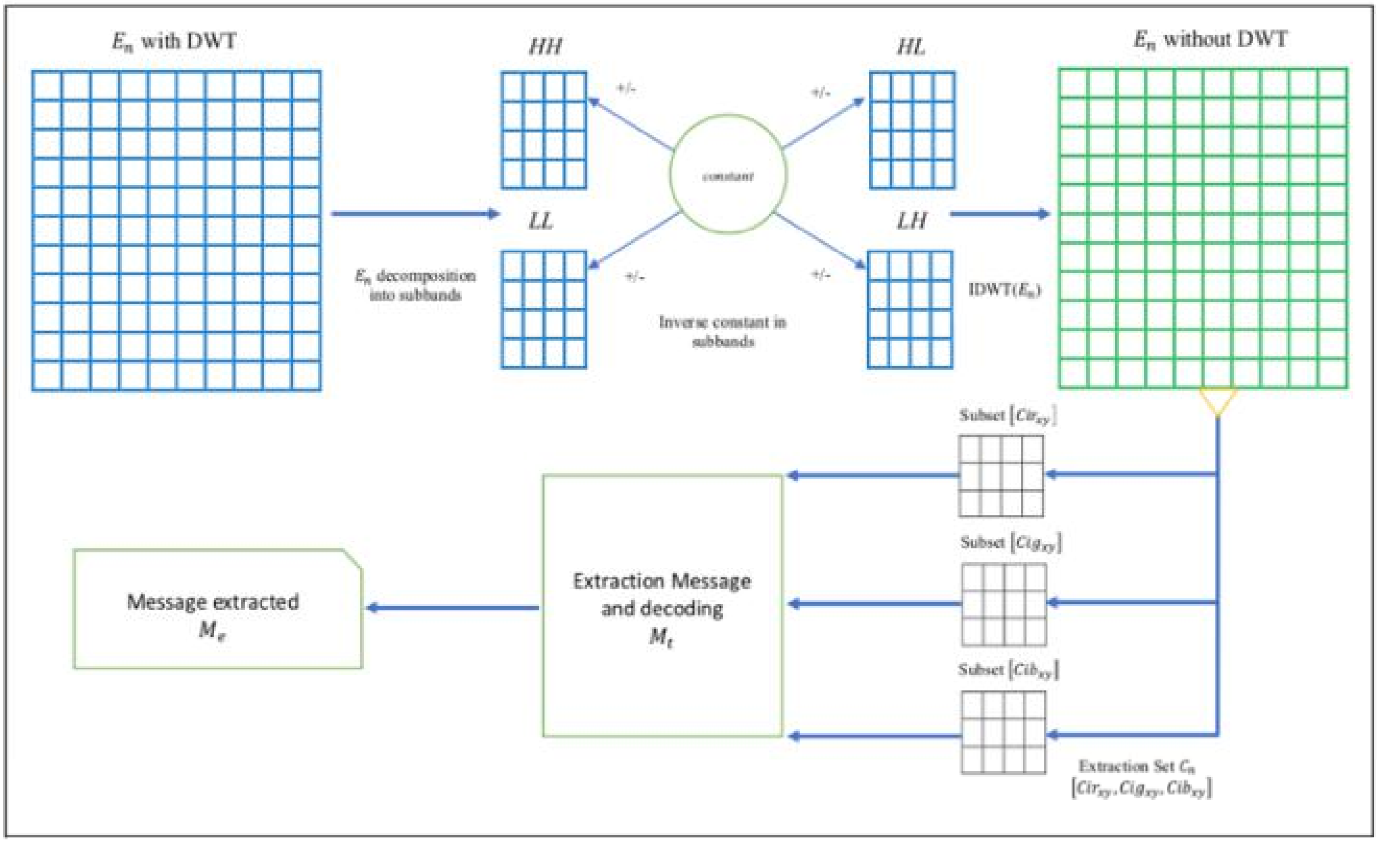
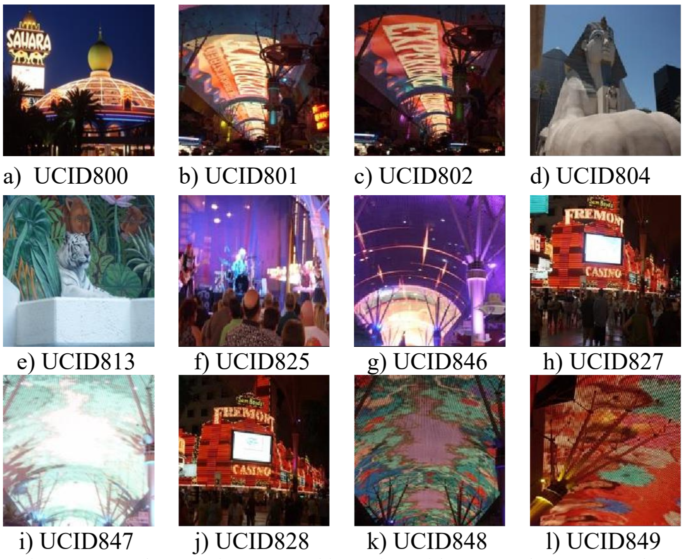

E_n with DWT
HH
HL
E_n without DWT
+/-
+/-
constant
LL
LH
E_n decomposition into subbands
+/-
+/-
Inverse constant in subbands
IDWT(E_n)
Subset $[Cir_{xy}]$
Subset $[Cig_{xy}]$
Subset $[Cib_{xy}]$
Extraction Set C_n $[Cir_{xy}, Cig_{xy}, Cib_{xy}]$
Extraction Message and decoding M_t
Message extracted M_e

Figure 4. Process to recoverM_e in E_n

IV. Experimentation

The proposed steganography method was verifiedusing a set of 50 digital RGB images with PNG format and dimensions of 512x512 pixels of each image, which are from UCDI dataset [25]. The message to embed is plain text with an approximate size of 200,000 bytes and metrics used that confirm the quality of the stego-images are PSNR, SNR, SSIM, MSE. Fig.5 and Fig.6 show a sample of the cover images as well as stego-images obtained.



a) UCID800 b) UCID801 c) UCID802 d) UCID804

e) UCID813 f) UCID825 g) UCID846 h) UCID827

i) UCID847 j) UCID828 k) UCID848 l) UCID849

Figure5. Sample cover images used in testing with proposed steganography method

a) UCID800 b) UCID801 c) UCID802 d) UCID804

e) UCID813 f) UCID825 g) UCID846 h) UCID827

i) UCID847 j) UCID828 k) UCID848 l) UCID849

Figure6. Sample of stego-images obtained in tests with proposed steganography method

Table 1 presents results obtained in stego-images with respect to the quality metrics.

Table 1. Results obtained by embedding the text message in stego-images

Estego-imagen	***Payload bpp***	***PSNR in dB***	***SNR in dB***	***SSIM***	***MSE***
UCID800	2.034	46.554	38.394	0.995	1.437
UCID801	2.034	46.553	38.941	0.996	1.437
UCID802	2.034	46.577	37.361	0.995	1.430
UCID803	2.034	46.544	39.728	0.995	1.440
UCID804	2.034	46.544	41.504	0.995	1.441
UCID805	2.034	46.563	40.505	0.995	1.434
UCID806	2.034	46.543	39.737	0.993	1.441
UCID807	2.034	46.542	40.797	0.996	1.441
UCID808	2.034	46.544	40.731	0.995	1.440
UCID809	2.034	46.554	41.365	0.994	1.437
UCID810	2.034	46.545	41.122	0.994	1.440
UCID811	2.034	46.554	40.037	0.993	1.437
UCID812	2.034	46.568	42.466	0.997	1.432
UCID813	2.034	46.562	41.658	0.997	1.434
UCID814	2.034	46.589	41.677	0.998	1.426
UCID815	2.034	46.550	41.376	0.997	1.438
UCID816	2.034	46.556	41.418	0.995	1.436
UCID817	2.034	46.556	40.783	0.994	1.436
UCID818	2.034	46.529	41.865	0.995	1.445
UCID819	2.034	46.558	41.970	0.996	1.436
UCID820	2.034	46.547	41.894	0.994	1.439
UCID821	2.034	46.515	42.334	0.998	1.450
UCID822	2.034	46.538	38.972	0.997	1.442
UCID823	2.034	46.542	39.744	0.997	1.441
UCID824	2.034	46.528	40.303	0.996	1.446
UCID825	2.034	46.554	40.963	0.998	1.437
UCID826	2.034	46.541	40.511	0.998	1.441
UCID827	2.034	46.521	38.150	0.994	1.448
UCID828	2.034	46.589	37.361	0.994	1.426
UCID829	2.034	46.540	38.075	0.995	1.442
UCID830	2.034	46.559	40.056	0.997	1.436
UCID831	2.034	46.547	38.985	0.996	1.439
UCID832	2.034	46.539	39.077	0.996	1.442
UCID833	2.034	46.514	39.314	0.996	1.450
UCID834	2.034	46.536	39.893	0.996	1.443
UCID835	2.034	46.557	40.890	0.994	1.436
UCID836	2.034	46.550	40.592	0.997	1.439
UCID837	2.034	46.552	40.017	0.994	1.438
UCID838	2.034	46.497	40.907	0.995	1.456
UCID839	2.034	46.537	39.851	0.996	1.443
UCID840	2.034	46.552	39.874	0.997	1.438
UCID841	2.034	46.553	38.698	0.996	1.437
UCID842	2.034	46.528	42.296	0.998	1.446
UCID843	2.034	46.570	35.249	0.998	1.432
UCID844	2.034	46.599	38.548	0.999	1.422
UCID845	2.034	46.594	38.331	0.998	1.424
UCID846	2.034	46.530	40.789	0.998	1.445
UCID847	2.034	46.360	44.983	0.994	1.503
UCID848	2.034	46.583	38.316	0.998	1.427
UCID849	2.034	46.622	38.506	0.999	1.415
Average	**2.034**	**46.548**	**40.138**	**0.996**	**1.439**

Analyzing the data presented in Table 1, it can be corroborated that a payload was obtained in all the stego-images greater than 2 bits per pixel, on the other hand, it is possible to observe that the PSNR scores exceed 46.5 dB in all the tests, while SNR remained above 40 dB, which indicates that despite the high fouling load, there are no notable visual alterations in the 50 stego-images analyzed. This is corroborated when analyzing the results presented by the SSIM metric, which is a specialized metric in the human vision system and allows establishing a relationship between contrast, luminosity and the structure of the object being analyzed. In this case, all stego-images present a score of 0.996, demonstrating that all modifications are technically imperceptible and therefore their quality is not perceptibly altered with respect to the cover images. As can be seen in the MSE column, an average score of 1.439 was obtained, which indicates that the first and second least significant bits were used to embed the message.

As observed in tests carried out, stego-images visually do not contain visually detectable areas as modifications, because, on the one hand, only the first two bits of the three channels of each cover image per pixel have been modified, by a selection modification sequence of 2 out of every three pixels.DWT application has allowed altering the value of originally modified data to generate a smoothing effect, which allows reducing error between the pixel areas, reducing effect that exists in an embedding pattern.

Regarding the works presented in the state of the art, we can include the work of Ouyang et al. [14], their work shows how a maximum of 32,768 bytes were embedded in a 512x512 image, with a PSNR of 73 dB (in this work an average of 200,000 bytes per image was applied), this value being higher than that is reported in the aforementioned work, in this work the authors take as reference the PNSR metric for evaluating the quality of stego-images, in addition the set of test images is quite small, in this research we have used a set of images of 50 objects, and in general the result between each stego-image keeps a general trend between the PSNR, SSIM and MSE metrics, in addition to the fact that the hidden data load is higher. In Swain's work [15] perform a combination of LSB with PVD, although their reported payload is 3 bits per pixel on average, and that reported in these tests is 2.034 on average, we must take into account note that more than a third of the pixels available for injection have been discriminated, in addition to the fact that only the first two bits of each pixel have been used for data embedding, on the other hand, in their proposal, their method validation is generally supported by PNSR validations, being that the SSIM metric allows more concise tests on the alterations that appear in images as demonstrated in [13],because it contemplates luminosity, contrast and structural similarity.

V. Conclusion

In general, we concluded that a combination of spatial techniques such as the substitution of less significant bits in pixels, which allows embedding high rates of information, combined with a technique based on frequency domain, allows, in the first instance, to reduce alterations generated on the stego-images, in addition to providing a scheme where modifications made are not noticeable because injection pattern is modified by DWT with the addition or reduction of constant values in the efficient of its sub-bands, despite the embedding pattern based on the modification two out of every three pixels, in addition to the results presented by the quality metrics, we can corroborate that the alterations do not compromise the contrast or luminosity of the stego-images, as well as its structural appearance.

VI. Future Work

We proposed to continue exploring variations in embedding scheme, which allows increasing the capacity of embedding data without compromising quality stego-images, as well as variants in the modification of pixels via modification of the coefficients of the images using DWT, applying variations by regions in RGB channels.

VII. Acknowledgment

We thank CONACYT for assigning the scholarship with registration number 445998 for postgraduate studies.

VIII. References

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

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

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

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

[5] S. S. Khaire and S. L. Nalbalwar, “Review: Steganography Bit Plane Complexity Segmentation (BPCS) technique”. International Journal of Engineering Science and Technology, vol. 2, 2010, pp. 4860–4868.

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

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

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

[9] P. Symes, “Video compression demystified”. McGraw-Hill, 2001.

[10] 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, 2012, pp. 1–16.

[11] Tawfiq Abdulkhaleq Abbas and Hassanein Karim Hamza. Steganography using fractal images technique. Steganography Using Fractal Images Technique, vol. 4, 2014, pp. 52–61.

[12] D. Salomon and G. Motta, “Handbook of Data Compression”. Springer, USA, 5 th ed.,2010, pp. 479-480.

[13] 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, 2014, pp. 1–13.

[14] L. Ouyang, J. H. Park, and H. Kau, “Performance of efficient steganographic methods for image and text”, vol. 7, 2016, pp. 29–33.

[15] G. A. Swain, “Steganographic method combining LSB substitution and PVD in a block”. Procedia Computer Science, Elsevier, 2016, pp. 39–44.

[16] M. Khodaei and K. Faez, “new adaptive steganographic method using least-significant-bit substitution and pixel-value differencing”. IET Image processing, vol. 6, 2012, pp. 677-689.

[17] A. Al-Mutairi, “A comparison of secret image hide methods of steganography and visual cryptography”. International Conference on Engineering and Technology Systems, vol. 13, 2016, pp. 116-120.

[18] 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, 2014, pp. 1271–1278.

[19] R. Roy. and S. Changder, “Steganography with projection aided payload dimension reduction and reconstruction for military covert communication”. International Journal of Computer Applications, vol. 139, 2016, pp. 32–37.

[20] 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, 2016, pp. 1185–1191.

[21] V. D. Hardikkumar and A. D. Apurva, “Steganography of messages using Mandelbrot fractal”. VNSGU Journal of Science and Technology, vol. 5, 2016, pp. 13-20.

[22] G. Geetha and K. Thamizhchelvyb, “Application of chaos and fractals in Image steganography a review”. International Journal of Control Theory and Applications, vol. 9, 2016, pp. 95–106.

[23]Ambika, R. L. Biradar and V. Burkpalli, “Efficient Approach for Steganography Using DWT and RSA Algorithm”.International Journal of Engineering and Advanced Technology (IJEAT), vol 8, 2019, pp. 1435-1443.

[24]B. S. Shashikiran, K. Shaila and K. R. Venigopal, “Hybrid Domain Steganography for Multiple Images using DWT-LSB Method”, vol. 9, 2019, pp. 1326-1334.

[25]Monika and M. Singh, “To Develop an Image Based Steganography Framework to Enhance Quality of Payload Object”. International Journal of Advanced Computing Research, vol 2, 2016, pp. 13-17.

[26]E. Hecht, “Optics”, 2nd Edition, Addison Wesley, 1987.

[27]A. Zenati, W. Ouarda and A. M. Alimi, “ SSDIS-BEM: A New Signature Steganography Document Image System based ob Beta Elliptic Modeling”. Enginnering Science and Technology Intertational Journal, vol 23, 2019, pp. 470-482, https://doi.org/10.1016/j.jestch.2019.09.002. (Article in a journal)

[28]G. Schaefer and S. Michal. UCID, “An uncompressed color image database”. Storage and Retrieval Methods and Applications for Multimedia, vol. 5307, 2004, pp. 472-480.