

A comparative study of steganography using watermarking and modifications pixels versus least significant bit

Hector Caballero, Vianney Muñoz, Marco A. Ramos-Corchado

Department of Computer Science, Faculty of Engineering, State of Mexico University, Toluca, Mexico

Article Info

Article history:

Received Feb 9, 2023

Revised May 24, 2023

Accepted Jun 4, 2023

Keywords:

Compression

Security

Singular value decomposition

Steganography

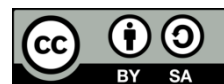
Watermarking

Wavelets

ABSTRACT

This article presents a steganography proposal based on embedding data expressed in base 10 by directly replacing the pixel values from images red, green blue (RGB) with a novel compression technique based on watermarks. The method considers a manipulation of the object to be embedded through a data compression triple process via LZ77 and base 64, watermark from low-quality images, embedded via discrete wavelet transformation-singular value decomposition (DWT-SVD), message embedded by watermark is recovered with data loss calculated, the watermark image and lost data is compressed again using LZ77 and base 64 to generate the final message. The final message is embedded in portable network graphic (PNG) images taken from the Microsoft common objects in context (COCO), ImageNet and uncompressed color image database (UCID) datasets, through a filtering process pixel of the images, where the selected pixels expressed in base 10, and the final message data is embedded by replacing units' position of each pixel. In experimentation results an average of 40 dB in peak signal noise to ratio (PSNR) and 0.98 in the similarity structural index metric (SSIM) evaluation were obtained, and evasion steganalysis rates of up to 93% for stego-images, the data embedded average is 3.2 bpp.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Hector Caballero

Department of Computer Science, Faculty of Engineering, State of Mexico University

Toluca de Lerdo 50000, Mexico

Email: hcaballero045@alumno.uaemex.mx

1. INTRODUCTION

Nowadays are different branches of computer science in charge of protecting information so that it remains preserved from malicious attacks, such branches include cryptography [1], watermarking and steganography [2]. Cryptography is widely used to protect information that requires high privacy but has the particularity that encrypted data is recognized as sensitive information by attackers, which means an effort by attackers to obtain the original message [3]. There are other areas such as watermarking and steganography to protect information.

Steganography is the science and art of information concealment, it is generally used to transport hidden information in digital objects such as video, image, audio, and other objects that are used by computers, although the objects have the greatest use are digital images because authors allow embedding high rates of information [4]. In steganography, there are spatial methods such as least significant bit (LSB) [5], pixel value differentiation (PVD) [6], tri-way pixel value differentiation (TPVD) [7], bit plane caps segmentation (BPCS) [8], which represents spatial information manipulation, and the methods that use discrete wavelet transformation (DWT), discrete cosine transformation (DCT) and discrete Fourier transformation (DFT) are responsible for embedding information through frequency-based transformations [9]. Generally, spatial methods in steganography are optimal for embedding large amounts of information

without loss, while methods based on the frequency domain are suitable for securing information against attacks such as clipping and compression or noise applications such as Gaussian or Brownian, although the information may suffer data loss, and on some occasions the embedding rates are lower than what was achieved in the spatial [10].

One of the main characteristics is in the case of stego-images must look as like the cover images, in addition to the fact that stego-images must be considered to approve steganalysis techniques such as chi-square, RS and PVo, among others [11]–[14]. A steganography system is a quintuple $\delta = C, M, K, D_k, E_k$, where C is the set of all cover images, M is the messages to hide, K is the set of secret keys, $E_k : C \times M \times K \rightarrow C$, and $D_k : C \times K \rightarrow M$ [15] are two functions, the first is the embedding and the second is the extraction function, such that $D_k(E_k(c, m, k)) = m$ [16]. On the other hand, watermark is a digital signature used to identify the data integrity of the cover object, as well as confirm the authenticity of the object [17]. Objects that contain a watermark, when are video or images, it is possible to visually verify if contain a distinctive element of this type of method, on the other hand, watermarks do not necessarily require that be visible, said characteristic it can be shared with that of steganography, although the purpose is not the same [18]. Watermarks must be designed to withstand attacks such as rotation, scaling, joint photographic experts group (JPEG) compression, Gaussian noise, brightness shifting, cropping, or deletion [19].

There are many mathematical techniques to implement watermarks, one of the most used is singular value decomposition (SVD), which is a factorization of a real or complex matrix. An image can be represented in the form of a matrix of scalar values [20]. SVD decomposes an image represented by a matrix A of size $M \times N$ into a product of three matrices $A = USV^T$ where U and V^T are orthogonal matrices $M \times M$ and $N \times N$, respectively. S is a diagonal matrix $N \times N$. The elements of S are only nonzero on the diagonal and are called singular values of A . Equation (1) represents the general form of SVD.

$$I = USV^t \quad (1)$$

I is an image and this indicates that I belongs to $RM \times N$ where R represents a real number. Where $U \in RN \times M$ and $V \in RN \times N$ are unitary matrices and $S \in RN \times N$ is a diagonal matrix with diagonal integers if it satisfies $s_1 \geq s_2 \geq s_3 \geq s_N \geq 0$ and the superscript denotes the transpose matrix. U and V are left and right singular vectors and S is a singular value of the transpose matrix.

Vector U and vector V are right and left, and S is a singular value of the matrix. The main property of SVD in image processing is that the singular value of the image has a high stability and is known with a small perturbation, this means that the image of the singular value does not present significant changes [21]. The singular vectors of an image specify the geometry of the image, while the singular values specify the luminance (energy) of the image. Slight variations in singular values do not affect the visual perception of image quality. The psychovisual effect-based property allows embedding of the watermark bits into the original image by minor modification to singular values of the original image [22].

DWT can be applied in watermarking and steganography; this represents the small waves of variable frequency and limited duration are wavelets. It is widely used due to its ability to compact space and frequency energy compaction. At each level, DWT decomposes an image into four sub bands, a lower resolution approximation (LL) component and three other spatial direction components corresponding to the horizontal (HL), vertical (LH) and diagonal (HH) components. High-resolution sub bands help locate edge and texture patterns in any image [23]. In the next subsection, a detailed mention will be made about the interesting proposals of existing steganography and watermarking.

Different research has been carried out aimed at hiding information aimed at replacing information by means of secret digits, as in the research by Nagaraj *et al.* [24] using the pixel value modification (PVM) by module function, Shashikiran *et al.* [25] used a data encryption process to hide information in digital images, using knight movements with 5×5 blocks. A proposal for the combination of parity bit pixel value difference (PBPVD) and improved rightmost digit replacement (IRMDR) is in [26], the method divides the cover image into two non-overlapping blocks of pixels, the value of the difference between the pixels in each block is used to determine the selection of PBPVD and IRMDR for RS analysis evasion. Other investigations that use combination with steganography and cryptography is the work of Al-Mamun *et al.* [27], proposes that the image pixels are randomly selected using the Stern-Brocot sequence, while the keying is achieved with multiple LSBs of color components (RGB). On the other hand, Hossen *et al.* [28] applies a cryptosystem with advanced encryption standard (AES) and Rivest cipher 5 (RC5). Kordov and Zhelezov [29] propose an approach to hide secret text messages in color images, combining steganography and cryptography. The location and order of the image pixels chosen for embedding are randomly selected by a chaotic pseudorandom generator.

Some studies that use a combination of steganography with watermarking can be seen in Gutub and Al-Shaarani [30], by combining LSB and DWT to hide digital images in cover images. An application of

LSB sees the work of Zakaria *et al.* [31], use data mapping to reduce the amount of bit modification per pixel, in such a way that four secret data bits are mapped to the four most significant bits of a coverage pixel, the only two bits of a pixel are modified to indicate the mapping strategy for evasion of analysis by histogram and RS. Sahu and Swain [32] propose replacement of n right-oriented bits to hide the secret data in an image, where 1 is less than n and less than 4 , to avoid the fall of boundary problem (FOBP), as well as resist attacks by noise of salt, pepper, and RS.

Fractal images allow embedding large amounts of data as Durafe and Patidar [33] use SVD and DWT to hide the information content within the cover image. The method proposed by the authors employs a cover image using fractals, to reconstruct when have exact parameters in the fractal imaging equations. These parameter values become part of the secret key. The authors also apply the hybrid IWT-SVD technique to monitor the differences in performance with respect to the DWT-SVD scheme.

Abdallah *et al.* [34] propose an embedding that relies on the use of SVD orthogonal matrices as a container for embedding information rather than embedding in the singular values of the images. Subhedar and Mankar [35] developed an image steganography scheme based on the framelet transformation that hides a secret image in the cover image, using bidiagonal singular value decomposition, because the secret information is embedded in singular values of framelet coefficients. Rodriguez-Mendez *et al.* [36] present a steganographic model that hides a digital voice signal in a color image, shows embedding capabilities, robustness, and imperceptibility of the secret message, as well as superior visual quality of the stego-image and audio quality of the signal of recovered voice compared to the state-of-the-art (SoTA) schemes. The model proposed by the authors obtained average values of 32 dB and 0.92 in peak signal to noise ratio (PSNR) and similarity structural index metric (SSIM).

Transforms such as the sharp frequency localized contourlet transform (SFLCT) are combined with SVD to build a secure watermarking pseudocode, as observed by Najafi and Loukhaoukha [37]. A formal generic model for digital image watermarking is seen in research [38] for the initial construction of a basic watermark model was developed to incorporate the use of keys. Rupa [39] uses several levels of security with steganography and watermarks, first level is with Gyration encryption pseudocode, in the second level it uses PLSB to hide encrypted information and in the third level the watermark image is embedded in the original image. Rahman *et al.* [40] has authored the novel least significant bit technique (NLSBT) using the magic matrix and multi-level encryption algorithm (MLEA) and expels the repetition of the most normal letters. In this procedure by inserting a secret message into a file, one can then prove ownership and/or guarantee the reliability of the item. Vu *et al.* [41] propose the multi-bit marking layer (MBML) method, which consists of reusing results from the previous embedding time (layer) as input data to continue embedding them in audio signals, the method demonstrates adequate performance in the error and signal to noise ratio (SNR) embedding rate surpassing methods such as LSB, large sample embedding (ELS), bit marking (BM) and BM/SW method (sliding window) which consist of a single layer.

In the reviewed information is possible observed that the regular ways of applying steganography and watermarks allow us to manipulate information contained in the images that underwent the watermarking process, although the loss of data is contemplated, which is not highly important, because the survival of the signature that identifies the authenticity of the carrier object is widely considered. Loss handling Information that may exist in a watermarking process can be leveraged to represent information without data loss. The following section presents a steganography method that takes advantage of watermarks for information compression, in addition to providing an encapsulation of information which cannot be retrieved directly.

2. METHOD

The proposal of this work is focused on combining watermarks to achieve information compression through an ingenious method that encompasses the DWT-SVD process with lossless compression techniques based on run length encoding (RLE) and base 64, to later embed this information in digital images with RGB color model without data loss due to compression, portable network graphic (PNG) format. The data embedding process is carried out by replacing the units with the lowest weight of each pixel when these are represented in base 10. Figure 1 shows the methodology to follow for the steganography process with watermarking as a compression mechanism of data, also named steganography method based in watermarking and replacing pixels (SMWRP). As can be seen in Figure 1 are three essential stages in SMWRP, the first stage being the conversion of a message into an RGB image, stage two is the application conversion process where I_{b10} is embedded in I_{lq} (image of low quality), to obtain M_f , which is the sum of I_w and M_{RE} , finally there is stage 3 that represents the embedding of M_f in the cover image, called I_p by replacing the base 10 units of each pixel of cover image. Below is a more detailed description of each stage.

Conversion of the message into an image. The input message is called M_i , this message is compressed by LZ77, then the number of symbols generated by LZ77 is reduced by base 64 encoding, in such a way that all symbols are represented by 8 bits, finally, each symbol it is represented by its position in the base 64 alphabet (represented in base 10), and the message M_{b10} is generated. M_{b10} is inserted into a new RGB image, whose initial values in all its pixels is 0, this image is I_0 , the data embedding process must be carried out through a cycle, prioritizing the data input to the R channel. In this stage are the following phases to complete the transformation of the message.

- Watermarking process. A low quality RGB image is generated, where the smallest possible image size is obtained, to later start the engraving process with SVD and DWT. The SVD process consists of multiplying the channels of the cover image with a constant, in the same way with DWT the multiplication process. By forming the stego-image by the watermarking process, to initialize the message recovery. This stage presents the following phases.
- Recovery of the watermarking message. A recovered message is subjected to verification to calculate the loss and recover it based on the recovered message and the original message expressed as an image, in which a third image is formed to respect positions that have been lost.
- Sum of messages. The stego-image formed with watermarking and the image that represents the loss are compressed by RLE and encoded in base 64, to be later concatenated. The message that is obtained from the concatenation is a final message to be embedded in a cover image.
- Concatenated message conversion. The message that represents an image with the watermarking process and the image that recovered data represented are converted to base 10, from this phase the M_f message is formed (the I_{b10} image).

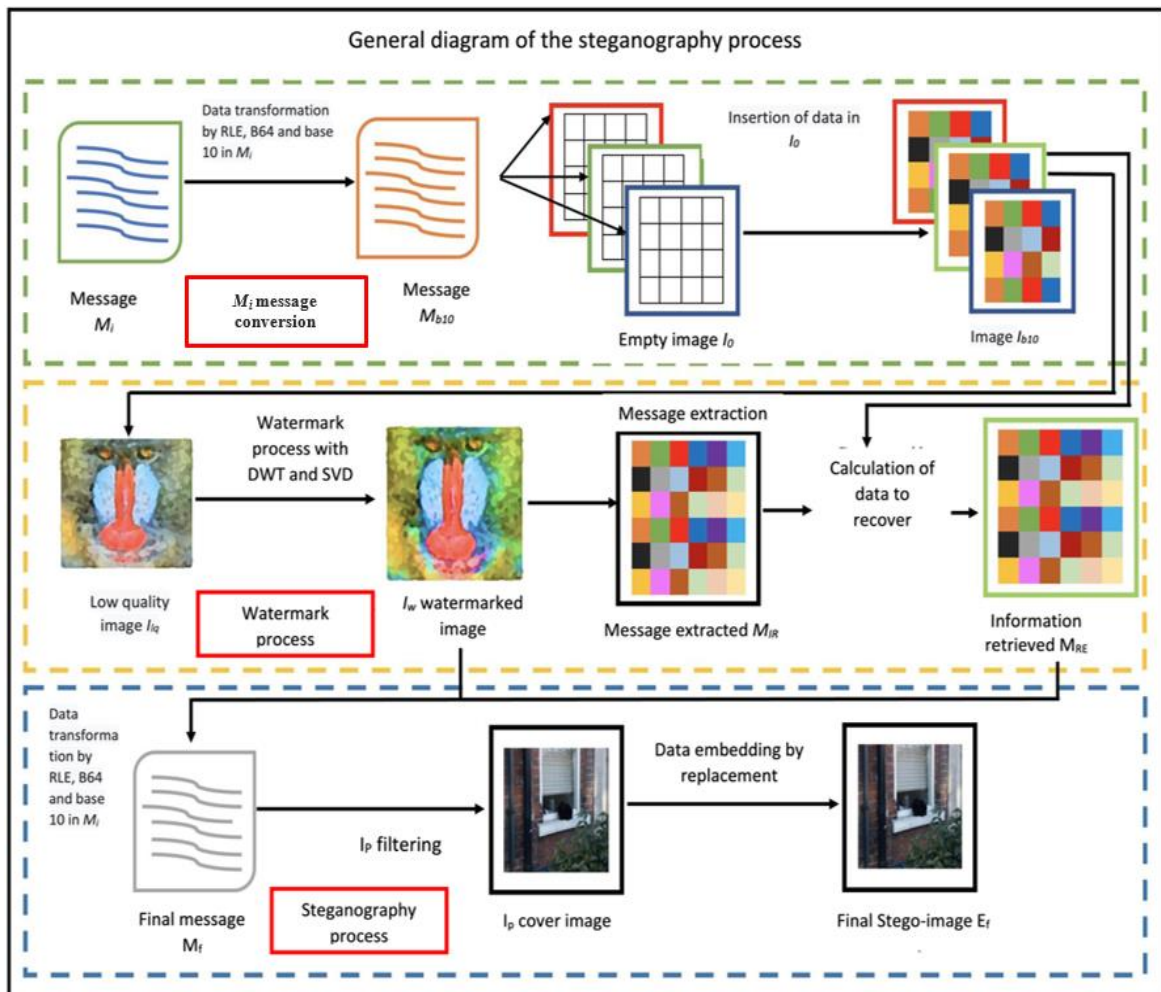


Figure 1. General diagram of the steganography process

Data replacement M_f message is sliced to form a digit-based data stream to replace the cover image pixel data. The process begins with filtering the image. The data replacement is applied to the cover image I_p , where a filter is applied to determine pixels in which the unit replacement process will be applied for each modified pixel, giving rise to the stego-image E_f . On the other hand, data recovery is focused on reconstructing the message in its entirety, without affecting the message that was originally embedded. The following steps are the process of recovering the embedded message.

- Step 1: In E_f , the range of pixels where the values close to color 255 are represented is chosen. Later, the chain of digits that represents the M_f is converted into a vector to replace the units of the pixels with that of the data.
- Step 2: The digits are concatenated to generate a series of pairs that are going to make up the base 64 symbols in the vector M'_f . The message that has been base 64 encoded is again encoded to separate the image corresponding to the image representing I_w and the image representing M_{RE} .
- Step 3: I_w is generated again, as well as M_{RE} . Once I_w has been extracted, the reverse watermarking process is applied to obtain M_{IR} and compare with M_{MR} .
- Step 4: Both M_{RE} and M_{IR} are compared in its positions to verify missing data sections, all data representing changes are stored in its corresponding coordinate in M_{RE} , to recover I_{b10} .
- Step 5: The I_{b10} pixels are read from the R channel to the B channel, stop being decoded in base 64, decompressed with LZ77 and finally M_i is recovered.

Algorithm 1 presents the general mechanism for embedding I_{b10} in an I_{lq} image. Algorithm 2 represents recovery of loss data, because the watermarking process generates data loss. The purpose of these two algorithms is to preserve the integrity of the message to be embedded.

Algorithm 1. Process to embed M_i in I_{lq}

```

1: Start
2:  $M_i$  //Message
3:  $M_{b10}=B_{10}(B64(LZ77(M_i)))$  //Codification to  $M_i$ 
4: Read ( $I_{b10}$ ) //  $M_i$  converted in image
5: Read ( $I_{lq}$ ) //Image to degraded in quality
6:  $I_{lq}=\text{Low-quality}(:I_{lq})$  //Low quality image
7:  $M_{IR}$  //image to recover
8:  $I_w=\text{DWT}(I_{lq})*\text{SVD}(I_{b10})*c_i$  //Merging process to  $I_w$ 
9:  $M_{IR}=I_w*\text{IDWT}*\text{ISVD}$  //Embedded inverse
10: End

```

Algorithm 2. Recovery loss data

```

1: Start
2: Read ( $M_{IR}$ ) //Image that represented loss data from  $I_w$ 
3: Read ( $I_{b10}$ ) //Image with ASCII code in base 10
4:  $M_{RE}=\text{Generated\_imageRGB}()$  //Imagen RGB empty
5:  $i=0, e=0, \text{channel}=0, \text{TypeD}=\text{"Segment data"}$ 
6: while  $\text{channel} \leq 3$  do
7:  $[M,N]=: I_{b10}$  //dimensions
8:   for  $i \leq M$  do
9:     for  $e \leq N$  do
10:      if  $I_{b10}[i][e] \neq M_{IR}[i][e]$  then
11:         $M_{RE}[i][e] = I_{b10}[i][e]$ 
12:      end if
13:    end for
14:  end for
15:   $\text{channel}++$  //Increase channel
16: end while
17: Write ( $M_{RE}$ ) //Data recovery converted in image
18:  $M_f=B64(LZ77(:M_{RE} + \text{"separator"} + B64(LZ77(:I_w))))$  //Message to embedded into final cover image
19: End

```

When M_{RE} has been generated, this image is converted to a string by using the functions LZ77 and B64, after this, I_w is converted to a string and both results are concatenated, in such a way that the result is added to a new chain named as M_f . This can be visualized in a general way in (2). The data embedding process consists of filtering the I_p cover image, selecting which pixels are candidates to be modified in its unit position by M_f values that are expressed in base 10, going through all the I_p channels, at the end the stego-image E_f is generated. Algorithm 3 shows the data embedding process.

$$M_f = B64(LZW(MRE + B64(LZW(I_w)))) \quad (2)$$

Algorithm 3. Data embedded process

```

1: Start
2: Read ( $I_p$ ) //Cover image
3:  $E_f =: I_p$  //Read stego-image
4:  $Counter=0$ ,  $CounterC$ 
5:  $chan=Channel(I_p)$  //Image channels
6:  $M_t = B64(LZW(M_f))$ 
7: for  $3 \leq channel$  do
8:     for  $x \leq term$  do
9:         for  $y \leq term$  do
10: if  $I[x][y] \leq filter$  and  $Counter < Length(M_t)$  then
11:  $E_f[x][y].first\_digit = M_t[Counter]$ 
12:     end if
13:     end for
14: end for
15:      $CounterC ++$ 
16: end for
17: Display ( $E_f$ )
18: End

```

To recover the information, several algorithms are used for the reverse process. The data recovery algorithm 4 indicates that the stego-image is read, a filter indicates the pixels that make up a range of values where it is possible to find the substituted data in its numerical value of the first digit of the selected pixels of the stego-image. The digits are concatenated in the concatenate variable.

The concatenate variable contains a message that encompasses I_w and M_{RE} . The digits stored in the concatenate variable are converted into numbers corresponding to base 64 to later be decompressed, as can be seen in algorithm 4. In algorithm 5, the process of generating the image to which the code was applied begins. The watermarking process, represented by I_w , and the M_{RE} image which contains the information that represents data loss by the DWT-SVD application process.

Algorithm 4. Counted chain deployment

```

1: Start
2: Read ( $E_f$ )
3: Filter_pixels ( $E_f$ )
4:  $channel = Channel(E_f)$  //Extraction channels
5: for  $3 \leq channel$  do
6:     for  $i \leq end$  do
7:         for  $e \leq end$  do
8: if  $E[x][y] \leq filter$  then
9:      $concatenate += E[x][y].fists\_digit$ 
10:    end if
11:    end for
12:    end for
13: end for
14: Display ( $concatenate$ )
15: End

```

Algorithm 5. Main image extraction

```

1: Start
2: Read ( $N_{cad64}$ )
3:  $breaker = "x"$ 
4: for  $i \leq cad64$  do
5:  $I_{cw}$  //Representation of values from  $I_w$ 
6:     if  $N_{cad64}(i) \neq "breaker"$  then
7:          $I_{cw} += N_{cad64}(i)$ 
8:     Else
9:         Print ('First image')
10:         $flag=1$ 
11:    end if
12:    if  $N_{cad64}(i) \neq breaker$  and  $flag == 1$  then
13:         $M_{CRE} += N_{cad64}(i)$ 
14:    end if
15: end for
16: End

```

Algorithm 6 expresses the conversion of the M_{CRE} and I_{CW} chain to give way to the generation of the I_w and M_{RE} images again, reconstructing its R, G, and B channels, through the conversion of the converted data in base 64, to recover values in base 10. When recovering the image that received the treatment by watermarking using DWT-SVD, the process of breaking it down using DWT to obtain the R, G, and B channels, then SVD process is applied to recover in ew the image that presents the stored message and contains the original message. In algorithm 7, when the M_{IR} image is recovered, a comparison is made with the M_{IR} image that represents the loss of data when applying DWT-SVD, in such a way that it is compared with the M_{RE} image, in a series of cycles where the values that are the same in M_{RE} are replaced in I_{b10} by the values of M_{IR} , because these represent the values that were not lost in the watermark generation process, whereas, if the values do not match, these are passes the M_{RE} values to I_{b10} . At the end of the I_{b10} values, these are decoded from ASCII to B64 and later decompressed to give rise to the originally embedded message.

Algorithm 6. Image transformation process

```

1: Start
2: resol = x, resol = y image resolution
3: for x ≤ resol = x do
4:   for x ≤ resol = y do
5:      $M_{RE}.R = M_{CRE}(i).Decb64$  // Numerical conversion from pixels
6:      $I_w.R = I_{cw}(i).Decb64$ 
7:   end for
8: end for
9: for x ≤ resol = x do
10:  for x ≤ resol = y do
11:     $M_{RE}.G = M_{CRE}(i).Decb64$ 
12:     $I_w.G = I_{cw}(i).Decb64$ 
13:  end for
14: end for
15: for x ≤ resol = x do
16:  for x ≤ resol = y do
17:     $M_{RE}.B = M_{CRE}(i).Decb64$ 
18:     $I_w.B = I_{cw}(i).Decb64$ 
19:  end for
20: end for
21: End

```

Algorithm 7. Message extraction with DWT-SVD

```

1: Start
2: Read( $I_w$ )
3: Read( $I_{b10}$ ) // Message in base 10
5:  $wm_{LL}, wm_{LH}, wm_{HL}, wm_{HH} = \text{DWT } I_w, \text{ haar}$ 
6:  $Im_w = wm_{LL}$  //  $Im$  represent the image
7:  $R = w, B = w, G = w$ 
8:  $U_{imr}, S_{imr}, V_{imr} = \text{svd}(red)$ 
9:  $U_{img}, S_{img}, V_{img} = \text{svd}(green)$ 
10:  $U_{imb}, S_{imb}, V_{imb} = \text{svd}(blue)$ 
11:  $S_{ewr} = (Simr - Simgr1)/0.10$  // ew process watermarking
12:  $S_{ewg} = (Simg - Simg1)/0.10$ 
13:  $S_{ewb} = (Simb - Simb1)/0.10$ 
14:  $ewr = U_{imr2} * S_{ew} * V_{imr2}$ 
15:  $ewg = U_{img2} * S_{ew} * V_{img2}$ 
16:  $ewb = U_{imb2} * S_{ew} * V_{imb2}$ 
17:  $M_{IR} = \text{Concatenate matrix}(3, ewr, ewg, ewb)$ 
18: while channel ≤ 3 do
19:  $[M, N] = I_{b10}$  // dimension extracted
20:   for i ≤ M do
21:     for e ≤ N do
22:       if  $M_{IR}[i][e] \neq M_{RE}[i][e]$  then
23:          $I_{b10}[i][e] = M_{RE}[i][e]$ 
24:       end if
25:       if  $M_{IR}[i][e] == 'equal'$  then
26:          $I_{b10}[i][e] = M_{IR}[i][e]$ 
27:       end if
28:     end for
29:   end for
30:   channel ++ // increase channel
31: end while
32:  $M_{b10} = \text{DecodeB10}(M_{RE})$  //  $M_{RE}$  transformed in base 10
33: Print( $dLWZ(d64(M_{b10}))$ ) // Decodification  $M_{b10}$ 
34: End

```

When carrying out the analysis of the big O [42], [43] for the previous pseudocodes, the following complexities have been observed: in algorithm 1 it is observed that the variables present an assignment of values, but from this assignment process functions that demand great computational power are used, because it corresponds to algorithms 3 to 7, which will be discussed later. In algorithms 2 to 4 a nesting of 3 cycles is observed, this complexity would correspond to $O(n^3)$. In algorithm 5 a complexity $O(n)$ is observed, algorithm 6 has a complexity of $O(n^2)$ because the code segments with the greatest weight are those that have two nested cycles. While in algorithm 7 the highest complexity observed is $O(n^3)$, on the other hand, the message decoding functions, as well as the watermarking process present levels of $O(n^2)$ for the process matrix multiplication. The stages with the highest computational cost occur in the watermarking process, the embedding of the final message and the recovery of the message process.

3. RESULTS AND DISCUSSION

This section presents the evaluation of SMWRP. Cover images have been randomly selected from uncompressed color image database (UCID) [44], Microsoft common objects in context (COCO) [45] and ImageNet [46], three sets of images named A, B and C was conformed from these datasets, each set contains 500 digital images with RGB color model and in PNG, with a resolution of 512×512 pixels. For each cover image a 320,000 bytes message was embedded, both image sets A, B, C, and the message was used to perform a comparison with LSB. In Figure 2 shows the evaluation process to SMWRP.

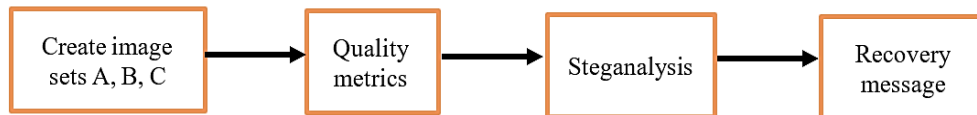


Figure 2. Experimental process for SMWRP

The stego-images generated in the evaluation process will be subjected to an analysis to calculate the relationship of modifications are present against the cover images, the metrics CC, MSE, PSNR, SNR and SSIM have been considered, for the steganalysis it has been used the StegExpose tool [47]. The implementation of SMWRP has been developed in MATLAB 2015b development environment, on a Mac Book Pro computer with a 2.3 GHz Core i5 processor and 8 GB of RAM. One of the metrics developed to check the structural integrity of an image is the mean squared error (MSE), which is defined as a mean square error, where $f(x,y)$ is a carrier signal (cover image), $\hat{f}(x,y)$ is a processed signal (stego-image), $M \times N$ is the size of the signal in 2D [48], equation (3) represents the calculation of the MSE.

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - \hat{f}(x,y)]^2 \quad (3)$$

The existing relationship between the signal and the noise known as SNR is established between the proportion that exists between the signal of the power that is transmitted and the power of the noise signal that breaks it down by [49]. This ratio is measured in decibels and is defined by (4). The PSNR is defined as a limit, where the relationship with the error receptor is approximated through the human vision system. The PSNR is dimensionless since the units of both the numerator and denominator are pixel values [50] in (5).

$$SNR = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \hat{f}(x,y)^2}{MSE} \quad (4)$$

$$PSNR(dB) = 10 \log_{10} L^2 / MSE \quad (5)$$

The SSIM is a method used to determine the similarity between two images, this metric allows to measure or predict the quality of the image, based on an initial image that is not compressed or without distortion (cover image) [51]. Generally, the mean SSIM (MSSIM) index is used to assess the overall quality of an image, $f(x,y)$ represents the ported image and $\hat{f}(x,y)$ represents the distorted image, f_j and \hat{f}_j are the content of the j th local window, and W is the number of local windows in the image, equation (6) represents MSSIM [52]. Correlation coefficient (CC) of two random variables is a quantity of linear dependence [53]. If each variable has n scalar observations, the Pearson correlation coefficient is defined as in (7). Where A

represents the first variable and B the second variable, being m and n the sections to be evaluated between the random variables.

$$MSSIM(f(x, y), \hat{f}(x, y)) = \frac{1}{W} \sum_{j=1}^W (f_j, \hat{f}_j) \quad (6)$$

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

3.1. Results and discussion

In Table 1 important aspects can be observed during experimentation process, first, it can be noted that the quality of the stego-images with SMWRP demonstrated when analysis was applied present a PSNR with greater than 42 dB for sets A, B and C, which indicates that visually there are no great differences with respect to cover images, the SNR registers 36 dB, although a striking increase is observed in the MSE of more than 4 points, it is important to clarify that the SSIM registers for the three sets a score higher than 0.980, which validates that visually there are no significant deformations that are appreciable by the human vision system, while the CC is entered at 0.999 points. When analyzing the results of the stego-images with the LSB implementation, it can be observed that the results presented by the quality metrics in PSNR and in SNR show less 9 dB than SMWRP, as well as an MSE of 27 points and SSIM with scores of 0.926 points, which indicates that the stego-images present more degradation in visual quality with respect to SMWRP. One of the most important advantages to SMWRP is its effectiveness in avoiding the steganalysis that was applied through StegExpose, where an evasion of more than 90% is obtained, while with LSB it presents an evasion of 1%, which indicates that it is a steganography method not recommendable when statistical analysis is applied.

Table 1. Comparison of results between the proposed method and the LSB, when applying StegExpose in the stego-images

Dataset	Resolution	Stego-images detected	PSNR	SNR	MSE	SSIM	CC
UCID SMWRP	512×512	50	42.532	36.742	4.291	0.985	0.999
COCO SMWRP	512×512	35	42.857	36.728	4.049	0.983	0.999
ImageNet SMWRP	512×512	30	43.008	36.954	3.813	0.987	0.999
UCID LSB	512×512	496	33.706	27.330	27.235	0.926	0.992
COCO LSB	512×512	495	33.779	27.607	27.263	0.928	0.994
ImageNet LSB	512×512	491	33.653	27.743	28.112	0.926	0.995

One of the reasons why SMWRP is highly effective in evading steganalysis is that it does not break the block pattern in the same way that LSB does, where a random pattern is created, which is detected by analysis such as chi square, RS, among others. Figure 3 shows graphically the results of the PSNR and SNR evaluation of LSB and SMWRP, for the COCO dataset, where it is possible to verify that the results of the metrics indicate that visually the alterations are more appreciable in the traditional LSB method. The previously described is also observed in the results obtained from the UCID dataset, Figures 4 and 5 ImageNet dataset. When analyzing the results of the evaluation of SSIM and CC of LSB and SMWRP, it can be seen in Figures 6 to 8 it is possible to see that the SMWRP generates alterations to a lesser extent than the LSB method. The LSB method does not maintain a good performance from the visual aspect of a stego-image, and it is widely deficient when performing a statistical analysis, as it was demonstrated when the analysis was applied with the StegExpose tool.

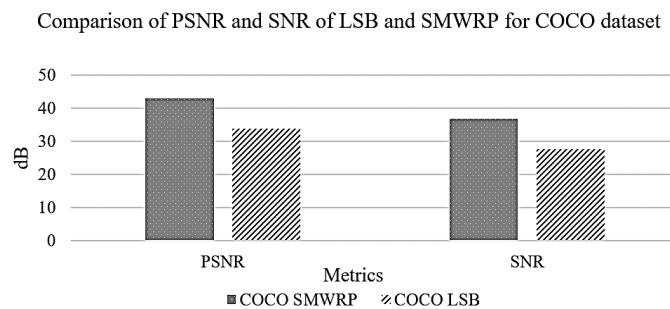


Figure 3. Results obtained from the evaluation of the COCO dataset when evaluating PSNR and SNR

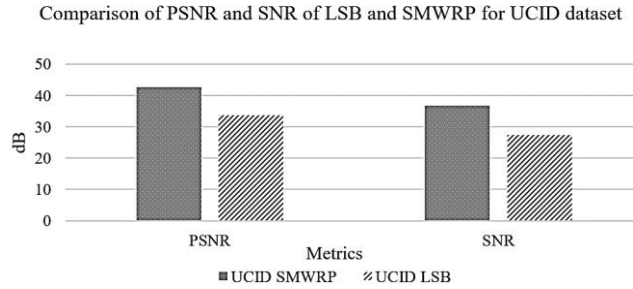


Figure 4. Results obtained from the evaluation of the UCID dataset with PSNR and SNR

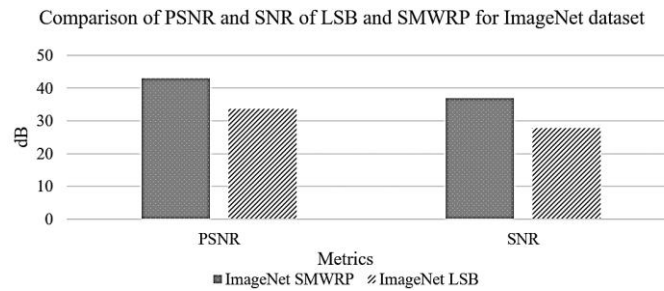


Figure 5. Results obtained from the evaluation of the ImageNet dataset with PSNR and SNR

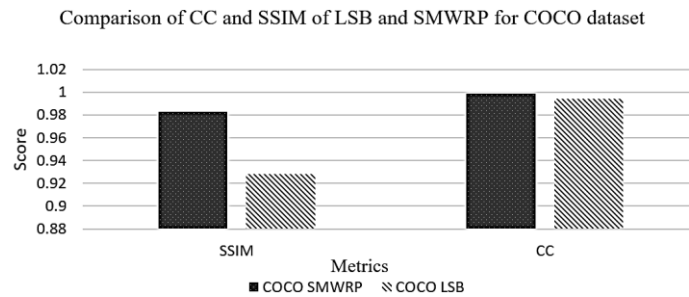


Figure 6. Results obtained from the evaluation of the COCO dataset with SSIM and CC

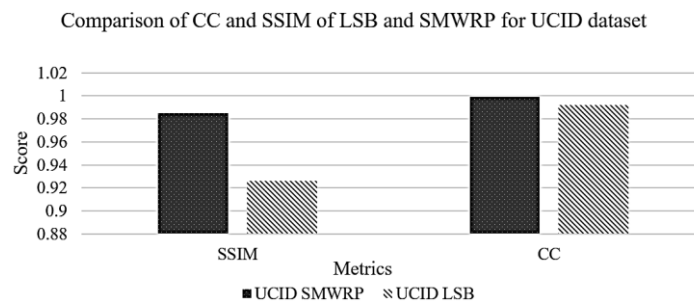


Figure 7. Results obtained from the evaluation of the UCID dataset with SSIM and CC

The combination of compression without loss data embedded in digital images with watermarks using DWT-SVD, has allowed to obtain outstanding results according to what can be observed at the end of tests, a series of important aspects can be observed in the experimentation process, such as the representation that SVD makes on the first stego-image, allow to reduce its size so that, in the end, it is possible to increase data compression. SMWRP allows to distribute the information in such a way that it does not affect the relationship between the pixels of the final cover image, and thus avoid detection by means of statistical

techniques. It can be observed that the results obtained in PSNR are higher than 40 dB, as well as the measurements recorded in the SNR remain above 37 dB and a SSIM superior to 0.980 in all sets, which indicates that visual stability is preserved in the stego-images, in comparison with the traditional replacement with LSB, a lower degradation in LSB would be expected because the affected bits per pixel are maximum 3, compared to SMWRP that presents 4 altered bits per pixel, but due to the compression that is applied the visual alterations are compensated. The data embedding process involves a double stage, because the original message is compressed and encoded to be embedded as an image using DWT-SVD and after this, it requires that the data loss that has originated be recovered, on the one hand, this allows the original message to not be obtained directly, on the other hand it is a longer process to prepare the message to be embedded, in the second stage, the replacement of units of the pixels expressed in base 10 allows avoiding the change of the pixels consecutively, and in this way avoid to the greatest extent possible evading the statistical analysis.

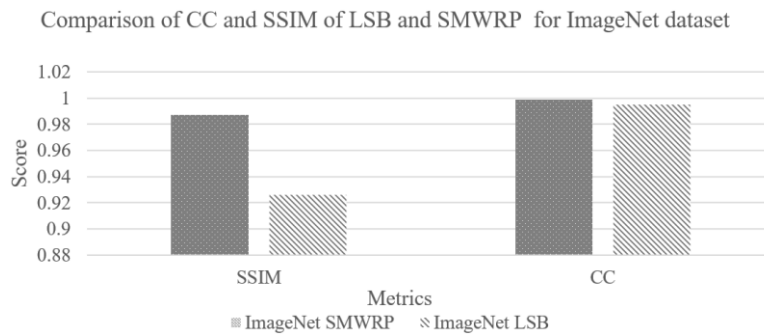


Figure 8. Results obtained from the evaluation of the ImageNet dataset with SSIM and CC

In Figure 9, 18 images are presented, contained in six groups of images that are compared with cover images, stego-images from SMWRP and the stego-images resulting from LSB method. The most notorious changes on the effects of embedding the message can be observed in the images of Figures 9(a) to 9(c), while the images contained in subsections are minus notable Figures 9(d) to 9(f), this trend with more impact can be observed between the group images of Figures 9(g) to 9(i) and those of the fourth group Figures 9(j) to 9(l), as well as in the fifth group as shown in Figures 9(m) to 9(o) and sixth group as shown in Figures 9(p) to 9(r) where LSB stego-images are evidently modified by the embedding process. As can be seen, the stego-images produced by LSB, present some stripes that visibly affect quality, while in the stego-images from SMWRP remain more near like the cover images. These visual results are reflected in the data obtained in the application of the PSNR, SNR, SSIM, CC and MSE metrics. The distribution of the data that was embedded by LSB, being homogeneous and in large numbers, tends to noticeably alter visual perception, because more than 3 bits per pixel are modified, making it visually appreciable, on the other hand, in SMWRP it focuses in locating pixels where large-scale changes are not perceptible, based selectively on the data being changed.

Figure 10 presents in first place 3 extracts of the images presented in presented in Figures 9(a) to 9(c), it is possible to visualize the changes that occur when applying the two methods, comparing Figure 10(a) against Figure 10(b) SMWRP it can be noted that the differences are not visible, because the modifications in these areas are minor, while comparing Figure 10(a) with Figure 10(c) large changes can be observed due to that a large amount of data has been entered with LSB. On the other hand, when comparing the images of Figure 10(d) with Figure 10(e) SMWRP the changes are observed in the central part, but due to the tonalities found in these areas, there is no impact on the appreciation of digital images. In the red boxes found in Figures 10(d) to 10(f) can see the differences that exist between the pixels of the stego-images, where the largest differences stand out in LSB, noting a greater randomness in the tonalities of the pixels. Finally in Figures 10(g) to 10(i) are extract from ImageNet, in these images is possible see the aggressive effect from LSB as shown in Figure 9(i) and the modification distribution from SMWRP as shown in Figure 10(h). During the execution of the tests, the compression process carried out by Lempel–Ziv–Welch (LZW) and later with DWT-DWT, as well as the recovery of the data recovered from the watermarking process, generates a time consumption which triples the insertion time with respect to the LSB method, but SMWRP has the advantage of not visually compromising the result of the steganography process, as well as avoiding stego-analysis. The results shown in the SSIM and CC metrics for LSB indicate that the images do not present structural deformations, although visually it is possible to notice the changes in the pixels. While SMWRP, the scores obtained in both metrics remain above 0.985 points for SSIM and 0.99 for CC.

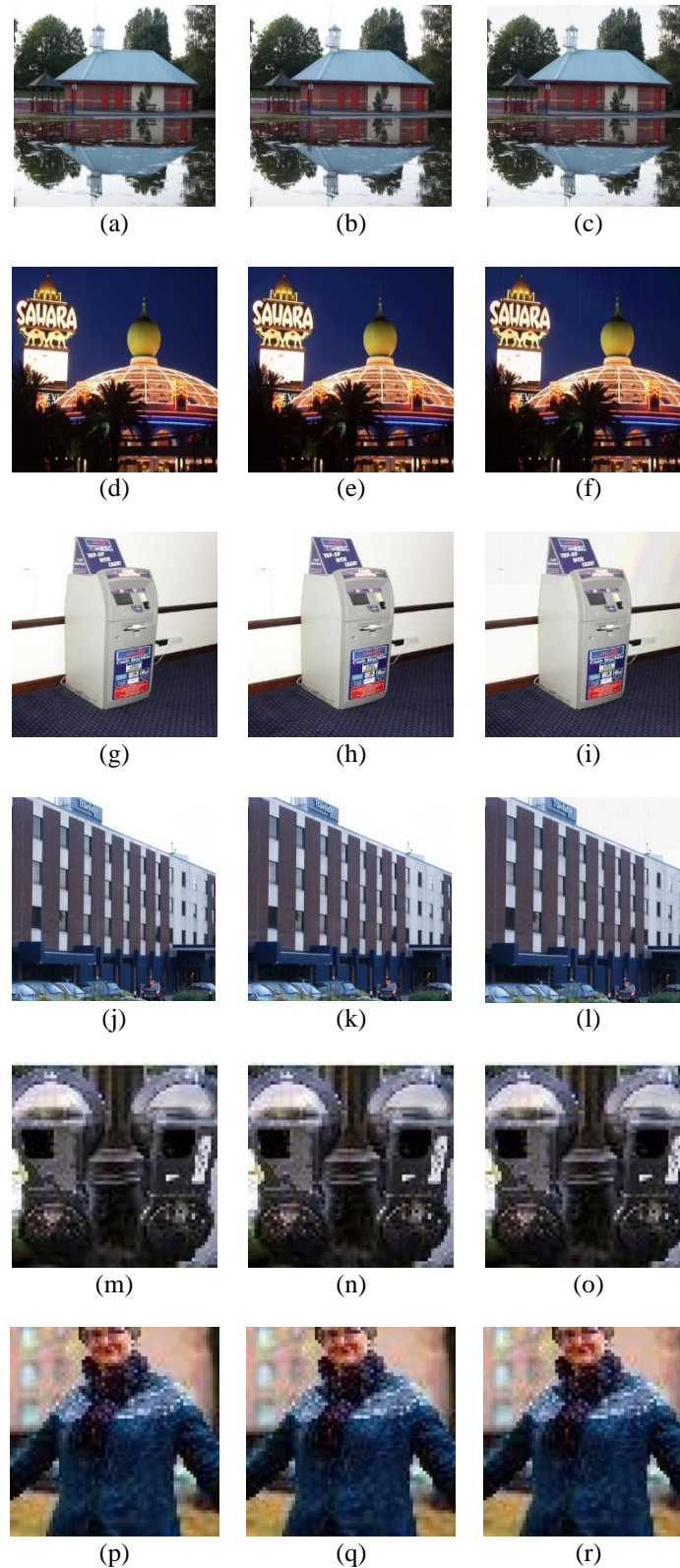


Figure 9. Visual quality comparison between cover images and stego-image ordered in six groups (a) cover image, (b) against stego-image SMWRP, and (c) stego-image LSB, (d) cover image, (e) against stego-image SMWRP, and (f) stego-image LSB, (g) cover image, (h) against stego-image SMWRP, and (i) stego-image LSB, (j) cover image, (k) against stego-image SMWRP, and (l) stego-image LSB, (m) cover image, (n) against stego-image SMWRP, and (o) stego-image LSB, and (p) cover image, (q) against stego-image SMWRP, and (r) stego-image LSB

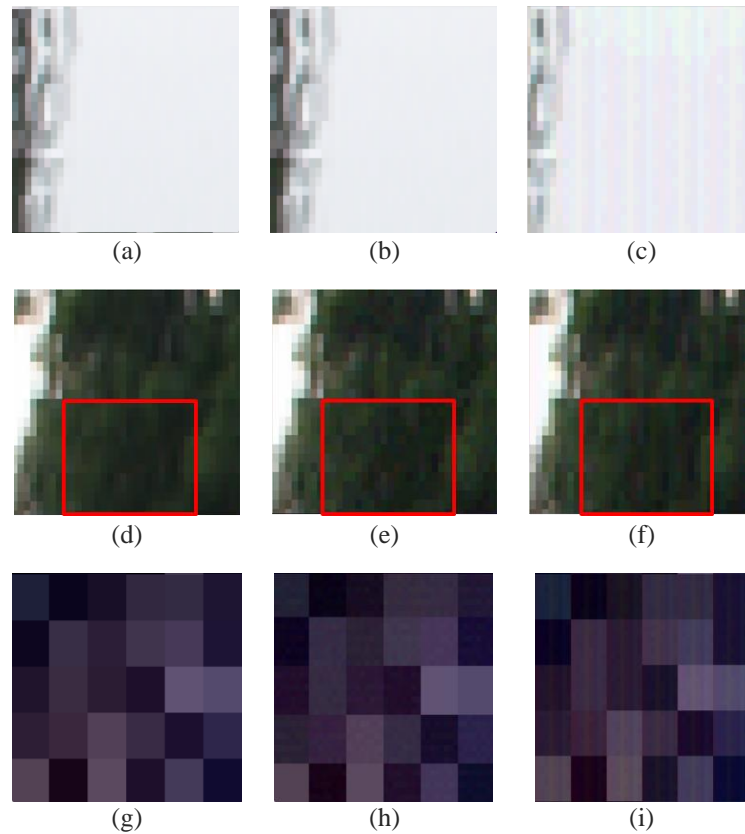


Figure 10. Visual modification difference comparison between images extracts, (a) cover image extract, (b) against SMWRP stego-imagen extract, and (c) LSB stego-imagen extract, (d) cover image extract, (e) against SMWRP stego-imagen extract, and (f) LSB stego-imagen extract, and (g) cover image extract, (h) against SMWRP stego-imagen extract, and (i) LSB stego-imagen extract

The method SMWRP presents an adequate balance with respect to proposals such as [31], as well as the ability to operate on images with RGB color models, on the other hand, compared to [40], it has the advantage of embedding a greater amount of data, having a high capacity to evade steganalysis. The advantage of SVD is in the reduction of the data size and a variable distribution over the image segments according to the pixel filtering function. Throughout the data analysis, quality check was executed with advanced metrics such as SSIM, CC to accurately validate the results with respect to the human vision system.

4. CONCLUSION

Watermarks provide many advantages for protection of digital information, since watermarks are robust against modifications made to the cover images. The characteristics also allow the information represented by the watermark to be manipulated, since the techniques used for implementation allow the size of the objects that are embedded to be reduced, particularly in this case digital images. It was observed during the development of the experiments that the information recovered by means of DWT-SVD had a loss of approximately 30% with respect to the message that was embedded, but the advantage of the proposal resides in the fact that when using an RGB image with reduced significant of its original quality as first cover object, it is possible to compensate the amount of information lost with respect to the final size of the new image that represents the loss, allowing both objects to be added in order to be embedded in a final stego-image by steganography.

The initial compression process using LZ77 and B64 is originally capable of reducing up to 50% of the original size of the message, while by means of the watermark and compression procedure by LZ77 and B64, it is possible to obtain the reduction of the message converted into an image (first stage of compression) in a size of 30% with respect to the original. Data embedding mechanism through units' replacement of numbers expressed in base 10, corresponding to the pixel values, with respect to LSB allows to significantly increase the evasion capacity of the classic steganalysis methods that are applied for the mechanisms of bit substitution embedding. In the tests carried out, the SSIM and CC results for the proposed method always

obtained scores higher than 0.98, indicating that the modifications made were not significant in the stego-images. This has been observed that the evasion capacity grows significantly, being up to 93% effective in evading the analysis executed by StegExpose tool, due to the reduction in randomness that traditionally occurs when LSB is used. One of the limitations that have been observed with the replacement of units corresponding to the values of the pixels, is a smaller amount of data that can be embedded, since not being able to use all the pixels of the cover image to preserve quality otherwise, stego-images drastically reduce quality, although it is possible to maintain the approval of the steganalysis test.

ACKNOWLEDGEMENTS

We thank CONACYT for the financial support granted to carry out this research project.




REFERENCES

- [1] M. Kaushal, "Cryptography: A brief review," *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, no. 2, pp. 763–767, Feb. 2022, doi: 10.22214/ijraset.2022.40401.
- [2] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: a review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.
- [3] V. Rishab, S. Sachin, S. Yadrami, S. N. Singh, and P. S. Pati, "A study on cryptography," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 325–328, Mar. 2022, doi: 10.48175/IJARSCT-2852.
- [4] D. Megías, W. Mazurczyk, and M. Kuribayashi, "Data hiding and its applications: digital watermarking and steganography," *Applied Sciences*, vol. 11, no. 22, Nov. 2021, doi: 10.3390/app112210928.
- [5] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proceedings of the 2001 workshop on Multimedia and security new challenges-MM&Sec '01*, 2001, doi: 10.1145/1232454.1232466.
- [6] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626, Jun. 2003, doi: 10.1016/S0167-8655(02)00402-6.
- [7] K.-C. Chang, P. S. Huang, T.-M. Tu, and C.-P. Chang, "Image steganographic scheme using tri-way pixel-value differencing and adaptive rules," in *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, Nov. 2007, pp. 449–452, doi: 10.1109/IIHMSP.2007.4457745.
- [8] E. Kawaguchi and R. O. Eason, "Principles and applications of BPCS steganography," in *Multimedia systems and applications*, 1999, pp. 464–473.
- [9] F. Şahin, T. Çevik, and M. Takaoğlu, "Review of the literature on the steganography concept," *International Journal of Computer Applications*, vol. 183, no. 2, pp. 38–46, 2021, doi: 10.5120/ijca2021921298.
- [10] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," *Mathematics*, vol. 9, no. 21, Nov. 2021, doi: 10.3390/math9212829.
- [11] S. Huang, M. Zhang, Y. Ke, X. Bi, and Y. Kong, "Image steganalysis based on attention augmented convolution," *Multimedia Tools and Applications*, vol. 81, no. 14, pp. 19471–19490, Jun. 2022, doi: 10.1007/s11042-021-11862-4.
- [12] N. Bunzel, M. Steinebach, and H. Liu, "Cover-aware steganalysis," *Journal of Cyber Security and Mobility*, Mar. 2021, doi: 10.13052/jcsm2245-1439.1011.
- [13] Y. L. Grachev and V. G. Sidorenko, "Steganalysis of the methods of concealing information in graphic containers," *Dependability*, vol. 21, no. 3, pp. 39–46, Sep. 2021, doi: 10.21683/1729-2646-2021-21-3-39-46.
- [14] S. Chhikara and R. Kumar, "Image steganalysis with entropy hybridized with chaotic grasshopper optimizer," *Multimedia Tools and Applications*, vol. 80, no. 21–23, pp. 31865–31885, Sep. 2021, doi: 10.1007/s11042-021-11118-1.
- [15] C. Cachin, "An information-theoretic model for steganography," in *Information Hiding*, Springer Berlin Heidelberg, 1998, pp. 306–318, doi: 10.1007/3-540-49380-8_21.
- [16] D. Dumitrescu, I.-M. Stan, and E. Simion, "Steganography techniques," *Cryptology ePrint Archive*, pp. 1–20, 2017.
- [17] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: a review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, Feb. 2014, doi: 10.1016/S1665-6423(14)71612-8.
- [18] W. Wan, J. Wang, Y. Zhang, J. Li, H. Yu, and J. Sun, "A comprehensive survey on robust image watermarking," *Neurocomputing*, vol. 488, pp. 226–247, Jun. 2022, doi: 10.1016/j.neucom.2022.02.083.
- [19] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*. Morgan Kaufmann, 2007.
- [20] G. H. Golub and F. T. Luk, "Singular value decomposition: applications and computations," in *Transactions of the Twenty-Second Conference of Army Mathematicians*, 1977, pp. 577–605.
- [21] P. Pandey, S. Kumar, and S. K. Singh, "Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 723–748, Sep. 2014, doi: 10.1007/s11042-013-1375-2.
- [22] G. Bhatnagar, Q. M. J. Wu, and P. K. Atrey, "Secure randomized image watermarking based on singular value decomposition," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 10, no. 1, pp. 1–21, 2013, doi: 10.1145/2542205.2542207.
- [23] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," *Procedia Computer Science*, vol. 46, pp. 612–618, 2015, doi: 10.1016/j.procs.2015.02.105.
- [24] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color image steganography based on pixel value modification method using modulus function," *IERI Procedia*, vol. 4, pp. 17–24, 2013, doi: 10.1016/j.ieri.2013.11.004.
- [25] B. S. Shashikiran, K. Shaila, and K. R. Venugopal, "Minimal block knight's tour and edge with LSB pixel replacement based encrypted image steganography," *SN Computer Science*, vol. 2, no. 3, 2021, doi: 10.1007/s42979-021-00542-7.
- [26] M. Hussain, A. W. A. Wahab, A. T. S. Ho, N. Javed, and K.-H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Processing: Image Communication*, vol. 50, pp. 44–57, Feb. 2017, doi: 10.1016/j.image.2016.10.005.
- [27] M. A. Al Mamun, S. M. M. Alam, M. S. Hossain, and M. Samiruzzaman, "A novel image steganography using multiple LSB substitution and pixel randomization using stern-brocot sequence," in *Advances in Intelligent Systems and Computing*, Springer International Publishing, 2020, pp. 756–773, doi: 10.1007/978-3-030-39445-5_55.




- [28] M. S. Hossen, M. A. Islam, T. Khatun, S. Hossain, and M. M. Rahman, "A new approach to hiding data in the images using steganography techniques based on AES and RC5 algorithm cryptosystem," in *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, Sep. 2020, pp. 676–681, doi: 10.1109/ICOSEC49089.2020.9215442.
- [29] K. Kordov and S. Zhelezov, "Steganography in color images with random order of pixel selection and encrypted text message embedding," *PeerJ Computer Science*, vol. 7, Jan. 2021, doi: 10.7717/peerj-cs.380.
- [30] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2631–2644, Apr. 2020, doi: 10.1007/s13369-020-04413-w.
- [31] A. Zakaria, M. Hussain, A. Wahab, M. Idris, N. Abdullah, and K.-H. Jung, "High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution," *Applied Sciences*, vol. 8, no. 11, Nov. 2018, doi: 10.3390/app8112199.
- [32] A. K. Sahu and G. Swain, "A novel n-rightmost bit replacement image steganography technique," *3D Research*, vol. 10, no. 1, Mar. 2019, doi: 10.1007/s13319-018-0211-x.
- [33] A. Durafe and V. Patidar, "Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4483–4498, Jul. 2022, doi: 10.1016/j.jksuci.2020.10.008.
- [34] H. A. Abdallah, M. Amoon, M. M. Hadhoud, A. A. Shaalan, S. A. Alshebeili, and F. E. Abd El-Samie, "An embedding approach using orthogonal matrices of the singular value decomposition for image steganography," *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 7175–7191, Mar. 2020, doi: 10.1007/s11042-019-7657-6.
- [35] M. S. Subhedar and V. H. Mankar, "Secure image steganography using framelet transform and bidiagonal SVD," *Multimedia Tools and Applications*, vol. 79, no. 3–4, pp. 1865–1886, Jan. 2020, doi: 10.1007/s11042-019-08221-9.
- [36] A. R. Mendez, C. C. Ramos, R. R. Reyes, and V. Ponomaryov, "Digital image steganography scheme for speech signals in the discrete wavelet transform domain," *Computación y Sistemas*, vol. 24, no. 3, Sep. 2020, doi: 10.13053/cys-24-3-3479.
- [37] E. Najafi and K. Loukhaoukha, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," *Journal of Information Security and Applications*, vol. 44, pp. 144–156, Feb. 2019, doi: 10.1016/j.jisa.2018.12.002.
- [38] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: its formal model, fundamental properties and possible attacks," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, 2014, doi: 10.1186/1687-6180-2014-135.
- [39] C. Rupa, "A novel approach in security using gyration slab with watermarking technique," *Journal of The Institution of Engineers (India): Series B*, vol. 97, no. 3, pp. 273–279, Sep. 2016, doi: 10.1007/s40031-015-0195-3.
- [40] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A novel steganography technique for digital images using the least significant bit substitution method," *IEEE Access*, vol. 10, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.
- [41] V. T. Vu, D.-T. Tran, and T. H. Phan, "Data embedding in audio signal using multiple bit marking layers method," *Multimedia Tools and Applications*, vol. 76, no. 9, pp. 11391–11406, 2017, doi: 10.1007/s11042-016-3851-y.
- [42] M. B. P. Cygan, J. Łącki, and P. Sankowski, "Algorithmic complexity of power law networks," in *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, Jan. 2016, pp. 1306–1325, doi: 10.1137/1.9781611974331.ch91.
- [43] J. A. Mañas, "Algorithm analysis-complexity (in Spanish Análisis de Algoritmos-Complejidad)." ADSW, 1997. [Online], Available: <https://www.dit.upm.es/~pepe/doc/adsw/tema1/Complejidad.pdf>
- [44] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," in *Storage and Retrieval Methods and Applications for Multimedia 2004*, 2003, pp. 472–480, doi: 10.1117/12.525375.
- [45] T.-Y. Lin *et al.*, "Microsoft COCO: Common objects in context," in *ECCV 2014: Computer Vision – ECCV 2014*, 2014, pp. 740–755, doi: 10.1007/978-3-319-10602-1_48.
- [46] O. Russakovsky *et al.*, "ImageNet large scale visual recognition challenge," *International Journal of Computer Vision*, vol. 115, no. 3, pp. 211–252, Dec. 2015, doi: 10.1007/s11263-015-0816-y.
- [47] B. Boehm, "StegExpose-A tool for detecting LSB steganography," *arXiv preprint arXiv: 1410.6656*, 2014.
- [48] D. Salomon and G. Motta, *Handbook of data compression*. London: Springer London, 2010, doi: 10.1007/978-1-84882-903-9.
- [49] M. J. Tapiovaara and R. F. Wagner, "SNR and noise measurements for medical imaging: I. A practical approach based on statistical decision theory," *Physics in Medicine and Biology*, vol. 38, no. 1, pp. 71–92, Jan. 1993, doi: 10.1088/0031-9155/38/1/006.
- [50] T. Dumas, A. Roumy, and C. Guillemot, "Image compression with stochastic winner-take-all auto-encoder," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 1512–1516, doi: 10.1109/ICASSP.2017.7952409.
- [51] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multiscale structural similarity for image quality assessment," in *Proceedings of the 37th IEEE Asilomar Conference on Signals, Systems and Computers*, 2003, pp. 9–12.
- [52] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, Apr. 2004, doi: 10.1109/TIP.2003.819861.
- [53] M. Spiegel, "Ch14 in theory and problems of probability and statistics 'Correlation theory' 2nd edn New York." McGraw-Hill, 1992.

BIOGRAPHIES OF AUTHORS






Hector Caballero    was born on May 15, 1988, in Tapaxco, State of Mexico, Mexico. He received the Ph.D. in Engineering Science degree from Universidad del Estado de México, México in 2020. His research themes are steganography, biometric systems and science computing based on natural language. He can be contacted at email: hcaballero045@alumno.uaemex.mx.



Vianney Muñoz    is researcher professor in Image Processing and Computational Vision at the Autonomous University of the State of Mexico. In 2009 she received her Ph.D. from Paris 13 University, France. Her research work is about computational vision, image processing, and video compressing. She can be contacted at email: vmunozj@uaemex.mx.



Marco A. Ramos-Corchado    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 in 2007, France. His research themes are artificial life, animation techniques, distributed systems, and intelligent agents. He can be contacted at email: maramosc@uaemex.mx.