Research Article

Steganography Algorithm Based on the Nonlocal Maximum Likelihood Noise Estimation for Mobile Applications

Blanca Esther Carvajal-Gómez ^{1,2} and **Manuel Alejandro Diaz-Casco** ¹

¹*Instituto Politécnico Nacional, Sección de Estudios de Posgrado e Investigación-Escuela Superior de Cómputo, Ciudad de México 07320, Mexico*

²*Instituto Politécnico Nacional, Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas, Ciudad de México 07340, Mexico*

Correspondence should be addressed to Blanca Esther Carvajal-Gómez; becarvajalg@gmail.com

Received 19 March 2018; Revised 20 May 2018; Accepted 2 July 2018; Published 26 July 2018

Academic Editor: Leandros Maglaras

Copyright © 2018 Blanca Esther Carvajal-Gómez and Manuel Alejandro Diaz-Casco. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, thanks to the use of Internet services, daily activities used to imply movement became more accessible to any user. As a result of such interconnection, now millions of people from different countries are able to communicate among themselves through the Internet, generating a great flow of data and classified information. The information on the Internet can be stolen, intercepted, anonymized, or even destroyed, resulting in cases of infringement of intellectual property rights, and the loss or damage of data. In such a globalized and interconnected world, solid security measures have become increasingly important to ensure data privacy protection and its confidentiality during transit. Nowadays, there is a variety of security mechanisms such as the steganography, an information hiding technique, which protects intellectual property by allowing the transmission of hidden data without drawing any suspicion. In order to achieve these criteria, an adaptation of the nonlocal maximum likelihood filter is proposed; in this class of filters, in general, they are used in images that require a high level of irregular pattern detection, based on the statistical dependence of the underlying pixels of the image analysis area, when using it in the wavelet domain as edge detector and/or discontinuities in images in order to have a greater selectivity when inserting information in the image. It strengthens the detection of the areas with the highest probability of having noise presenting results which are suitable areas to insert the information and that it is imperceptible in a quantitative and qualitative manner as presented in the Results and Discussion.

1. Introduction

Steganography is the science of hiding information by means of a cover medium in such a way that even the presence of the message is invisible to any eavesdropper. The object, apparently harmless, is known as the “host” and the contained information as the “payload”. The variety of host objects can range from text files to images, audio, and/or video. The most common example is the use of images; they are used as hosts due to their omnipresence in our day-to-day activities, as well as their high level of redundancy in their representation. The image steganography techniques are classified according to their domain; the most frequently used are the spatial and the frequency domain ones. However, there are now some techniques that combine both domains, with the advantage of being adaptable to the nature of the image [1].

The spatial domain techniques are used by directly manipulating the pixels of the image to hide the information. They are also characterized by having the simplest schemes, a short implementation time [1], a reduced hardware requirement, and a low time complexity.

In the spatial domain, a steganographic algorithm modifies the data in the host image in the special domain; the most representative algorithm in this domain is the substitution of the least significant bit (LSB); although this method is simple, it has a greater impact in comparison with other methods.

In general, the insertion mechanism is carried out in the LSB up to the 4th LSB. It can be assumed that inserting in the 4th LSB generates greater visual distortion to the host image since the hidden information is seen as “unnatural”. Similarly, the distortion occurs at the time of recovery of the inserted image.

This algorithm has been perfected in order to decrease these distortions presented both in the host image and in the recovered image; one of the most widely used methods is the LSB-OPAP [2], which makes an adaptation to the insertion of the information following the considerations of the LSB algorithm. This consists of the following set of steps: the insertion of the information is done using the LSB method to obtain the stego-image pi' ; in parallel the steganographic algorithm is performed using the technique in [2] obtaining the stego-image pi'' . Then consider $pi(i)$, $pi'(i)$, and $pi''(i)$, the pixel values corresponding to the i -th pixel in the host image C , the stego-image C' obtained by the simple LSB substitution method, and the refined stego-image obtained after the OPAP. With $\delta i = pi' - pi$, the insertion error is between pi and pi' . According to the process of incorporation of the simple LSB substitution method described above, pi' is obtained by directly replacing the least significant bits of pi with k message bits, with the following condition: $-2^k < \delta_1 \leq 2^k$. As a result, it shows a slight improvement against the traditional LSB.

Recently, to improve visual quality and security against histogram attacks, an approach based on LSB with the capacity of 1 bpp was proposed, reducing the probability of changing pixels as a modification of 1/3 of pixels. Due to the smaller modification of the stego-image pixels, it improves the visual imperceptibility and also has resistance against detection attacks based on LSB, that is, the HCF-COM steganalysis [3].

Yuan et al. [4] proposed a method based on multilayer adaptive steganography. The insertion of the secret image adapts to the regions with different texture in the host image. The insertion of the information is done using the LSB algorithm, and this can be extracted using the XOR-based operation. This method resists modern attacks with steganalyzers such as SPAM and AUS. One of the main problems in methods based on the LSB algorithm is that although they are simple to understand and apply and even flexible to integrate with other methods, its main vulnerability is that having a direct relationship between the ability to insert with the visual quality of the stego-image, the latter is affected as the insertion in the maximum level of the LSB in a pixel is made.

The frequency domain or the transform domain is another technique used, which consists of diverse transformations used to retrieve information in the frequency domain or time-frequency.

To avoid the problems presented in the spatial domain, the processing in the frequency domain has been an adequate tool for signal filtering, pattern recognition, and image compression. A complicated problem to solve in the spatial domain becomes easy to deal with in the frequency domain, because the sharp edges and transitions in an image contribute significantly to the content of the high frequency of its transformation.

These techniques applied in the frequency domain insert the information through transforms in which the frequency components of the image are extracted, where the places or zones in which the image in the image will not be affected

can be identified in a more precise way, "visual quality" of the image. These compression techniques are often used because they extract characteristics of the host image that represent the high and low frequencies of the image, where the latter represent the edges or contours of the host image, thus allowing an exchange of values in the host image, values of the image to hide. Therefore, to search for the right pixels to hide data, transformations-based schemes are a reasonable approach. In these schemes, the host image is transformed due to its approach oriented to the extraction of the main characteristics in frequency.

Among these, there is the Discrete Cosine Transformation (DCT) technique and the Discrete Wavelet Transformation (DWT) technique [5, 6].

Some popular steganographic algorithms on the Internet that apply DCT are the following.

The Jsteg/JPHide algorithm has the following characteristics for the insertion of information [7].

Jsteg has (1) steganographic tool based on the insertion of LSB; (2) the insertion is done replacing the nonzero LSB values by nonzero DCT quantized coefficients by the secret message bits. (1) In JPHide, these quantized coefficients are randomly selected with the help of any pseudo-random number generator that can be controlled with a key, (2) the second LSB can also be modified in JPHide, and (3) the Jsteg capability is equal to the number of DCT coefficients whose values are not equal to 0, 1, and -1 (this condition is selected to avoid ambiguity in the extraction of secret bits).

Another known algorithm is YASS (another steganographic scheme), which is explained below [8]:

- (1) The input image in the spatial domain is divided into blocks of fixed size known as large blocks (block B). Within each large block, the 8×8 subblock called host block (block H) is randomly selected.
- (2) The bits of the secret message are integrated into the DCT coefficients of the H block by the quantum modulation index (QIM).
- (3) With the help of Inverse Discrete Cosine Transform (IDCT) of block H, a JPEG image can be obtained.
- (4) The advantages include the survival of the message bits in the active guardian scenario; it works well against the autocalibration tool called autoanalysis.

For example, DWT, in Subhedar et al. (2014) [1], obtains in its best result a value of PSNR = 54.819dB with a secret image of 256x256. The authors propose a steganographic algorithm using an adaptation of the DWT called redundant wavelet transform (RDWT) and QR factorization.

For the implementation of the DWT, Abdulaziz and Pang [1] use the vector quantification called Linde-Buzo-Gray (LBG) together with the block codes known as BCH code and the discrete wavelet decomposition Haar at a decomposition level. The result presented by them argues that their algorithm presents a good quality with few perceptual defects.

Nowadays, there are also techniques adaptable to the nature of the image; spatial and frequency domain techniques are combined in these techniques [5, 6].

Adaptive steganography is a special case of the two previous methods. It is also known as “insertion based on statistics”, “masking”, or “based on models”. This method takes global statistical characteristics of the image before attempting to interact with LSB/DCT/DWT coefficients.

The statistical values obtained from the images will define where to make the changes. It is characterized by a random adaptive selection of pixels according to the host image and the selection of pixels in a block with a large local standard deviation. The latter is intended to avoid areas of uniform color (smooth areas). This behavior causes adaptive steganography to search for images with noise or existing or deliberately added images that demonstrate the complexity of the color.

Wayner [5] named in his book “life in noise”, pointing out the usefulness of the insertion of data in noise. It is proven that this method is robust with respect to compression, trimming, and image processing [5].

Chin-Chen et al. [9] proposed an adaptive technique applied to the LSB substitution method. His idea is to exploit the correlation between neighboring pixels to estimate the degree of statistical belonging. They discuss the options of having 2-4 crossing lines. The payload (embedding capacity) obtained is 355588 bits.

Hioki et al. [10] present an adaptive method called “data insertion based on block complexity” (ABCDE). The insertion is done by replacing the data in the selected pixels of blocks with high noise content in the image and is replaced with another noisy block obtained with the inserted data. This suitability is identified by two measures of complexity to adequately discriminate complex simple blocks, which are irregular in length and with edges considered noise. The hidden message is part of the noise of the image.

Regardless of their field of application, all of the image steganography techniques should focus on the following three main points: where to hide the information inside the image, the security level when embedding the information into the image, and the security level of the play load in case of intrusion. There are many steganography algorithms and each one is differently addressed.

In order to use steganography in images, it is necessary to select the specific regions to embed the image; these regions will be mentioned as Possible Embedding Regions (PEB). The PEB can be in any section or object inside the image that is able to produce the minimum possible distortion. The appropriate PEB can be recognized by abrupt changes in values of surrounding pixels, which are interpreted as the edges of the objects inside the image. The edges are considered to be appropriate sections for hiding information due to the fact that human sight is less sensitive to shape or color distortions inside the peripheral areas of an object, in combination with the fact that it randomly locates pixel values. The random pixel distribution allows the dispersion of payload in the stego-image, reducing its detection. This paper presents an adaptive steganography mechanism that employs three security levels for the retrieval of the embedded information. This embedding mechanism uses the spatial as well as the frequency domain to detect the edges of the PEB. The three levels will request to have a primary

key for each embedded data, additionally verifying whether the data is correct or not. In case of not complying with the three security levels, the retrieval of the information could be blocked, which provides an advantage. Finally, the quantitative results of its performance will be shown. In this work, the cover images have 2 different dimensions: 1024 x 768 and 256 x 256 pixels, while the images to be hidden have 4 different dimensions: 712 x 534, 1024 x 768, 576 x 768, and 256 x 256 pixels.

2. Theory

In this section, the proposed mechanism for using steganography in images will be described in detail. The proposed mechanism is adaptive, which means that it analyses the spatial and the frequency domains of the PEB edges for the possible embedding of information.

2.1. Discrete Wavelet Transformation (DWT). The DWT is used to analyze an image regarding its spatial and frequency domain. It provides a time-frequency representation of the image. The DWT is created by repeatedly filtering the image in each row and in each column in order to obtain the different DWT coefficients. The DWT is useful because it analyses the information at high and at low frequencies in each pixel. The cover image goes through a filter bank, where each filter is expected to be sampled by two (wavelet transform), which has a finite impulse response.

The image processed with the low-pass filter provides a soft wavelet coefficient of the input image and, with the filter, it results in a version of the edges of the image [11].

We have used the DWT Haar to deconstruct the cover image and, in the case of the stego-image, a Haar deconstruction and a DB4 deconstruction are used [12].

2.2. Fourth Moment Wavelet. During the wavelet transform of the image, four subimages are obtained in different frequency bands. The submatrixes obtained are considered as random variables. The fourth moment wavelet (FMW) is used in the submatrixes obtained, considering the following [6, 7]:

$$x(k, l) = s(k, l) + n(k, l) \quad (1)$$

where $x(k, l)$ is the image with additive noise, $s(k, l)$ is the original image, $n(k, l)$ represents the white Gaussian noise, and k, l is the current position of the pixel. From (1), it can be understood that $n(k, l)$ is a 2D random vector with N consecutive samples of a real process using a Gaussian distribution, with a mean equal to zero. From this consideration, the FMW is obtained as follows:

$$\begin{aligned} M_x^{(4)}[0, 0, 0, 0] &= E \{ (s(k, l) + n(k, l))^4 \} \\ &= E \{ s^4[k, l] \} + 4E \{ s^3[k, l] n[k, l] \} \\ &\quad + 6E \{ s^2[k, l] n^2[k, l] \} \end{aligned}$$

$$\begin{aligned}
& + 4E \{s[k, l] n^3[k, l]\} + E \{n^4[k, l]\} \\
& \geq 3\sigma_n^4
\end{aligned} \tag{2}$$

From (3), the mean and the FMW standard deviation are obtained with the following consideration $p = M_z^{(4)}$; then, the mean of p is obtained from the normal distribution [18, 19]:

$$E\{p\} = \frac{1}{N} \sum_{i=0}^{N-1} E\{x_i^4\} = 3\sigma_{LL}^4 \tag{3}$$

where E represents the submatrix expected value and p represents the probability of its occurrence in the sample. For the proposed method, the variability of the probability distributions is considered, and a selection threshold is finally chosen, based on the traditional considerations for hard and soft thresholding. The FMW, obtained from the coefficients of the decomposition of details, will have a value higher than $3\sigma_{nj}^2$, where $\sigma_{nj}^2 = (1/N) \sum_{k=0}^{N-1} (x(k)^2 - \sigma_{IC}^2)$. This is due to the conditions of variability occurrence of the components of the image [6, 7].

2.3. Noise-Level Estimation Mechanism. The noise-level estimation in images requires improved accuracy in the filters in order to be able to distinguish the edges and borders of the image and, thus, be able to separate it from the noise and the edge. Quality in image manipulation allows accurate insertion in the possible embedding regions, detected as edges and noise [20]. In this research, the nonlocal filter is used to detect noise in the images, which consists of the progressively selection of images, through each layer of their spatial composition. This type of filter is a multispectral extension of the nonlocal maximum likelihood filter

(NLML). It is possible to represent to detect noise in an image through filters used for the multispectral extension of the images; this filter is known as NLML [21].

Besides, given that the standard deviation of noise (SD) is an important reference for all the no local filters, an adaptation to the Maximum Likelihood Estimation (MLE) of noise levels is presented, and it is compared with MLE local and nonlocal methods.

The SD is an important parameter for the filtering of Nonlocal Media (NLM) and the NLML [22]. According to this, several noise estimation methods have been developed through the intensity of underlying pixels in the image that is being detected. However, this might sometimes not be enough to guarantee an accurate identification of the edge of the image. Because of this, the method [22] is used, with the pertinent adaptations for the edges estimation. In respect thereof, a Linearized Maximum Likelihood (LML) method has been proposed as edge detector in images [23].

2.4. Estimation of Noise Standard Deviation. The precise estimation of σ is essential for the filtering quality, as well as for other image processing tasks such as the segmentation and the estimation of parameters to detect edges [24]. The LML approach has been proposed when the image information does not provide the information needed to detect edges and to determine the precise value of σ [25–27].

For this paper, we propose the use of a modified Noise Estimation Filter using local maximum likelihood (NE-LML) to detect thresholds, employing the FMW as a selection process. During the edge detection, the adaptation of the NE-LML was employed. The estimation of σ is made for each layer of the image, which we denominate as k , which is maximized due to the use of the Rician distribution regarding the unknown values of $\hat{\sigma}$ and $\hat{A}_k$ range through the following equation [28]:

$$(\hat{\sigma}, \hat{A}_k) = \underset{\sigma, A_k}{\operatorname{argmax}} \left\{ \sum_{r=0}^R \sum_{c=0}^C \log \frac{S_k(r, c)}{\sigma^2} - \sum_{r=0}^R \sum_{c=0}^C \frac{S_k^2(r, c) + A_k^2}{2\sigma^2} + \sum_{r=0}^R \sum_{c=0}^C \log I_0 \left(\frac{S_k(r, c) A_k}{\sigma^2} \right) \right\} \tag{4}$$

where I_0 is the modified Bessel function of the first kind. For an optimal estimation, S_k represents the intensity of the image, k represents the decomposed layer, and A_k represents the range of the image in layer k . The combination of the FMW and the NE-LML filter allows the detection of appropriate areas to embed information in order to obtain the stego-image.

3. Methods and Materials

3.1. Wavelet Decomposition. Suppose digital image I is composed of a set of layers k , where $k = \{1, 2, 3\}$; with a set of samples $I_{k(1,1)}, I_{k(1,2)}, I_{k(1,3)}, \dots, I_{k(m,n)}$, that take values between $0 \dots 2j+1$ (typically $J=27$). In order to improve the steganography performance in mobile devices, we carried out the wavelet decomposition through the Haar Discrete Wavelet

Transformation Technique (HDWT) and the Daubechies Discrete Wavelet Transformation Technique (DDWT). The HDWT is frequently used for detecting edges, compressing images, coding, etc. Because the HDTW requires few computational requirements, it has been principally used for image processing and pattern recognition; this low computational demand provides advantages by implementing complex algorithms in limited technologies such as the mobile devices. The base operation of the HDWT when applied in a two-dimensional signal that contains $N \times N$ samples is the following: each row of one image is filtered with a low and high-pass filter (LPF and HPF) and the output of each filter is sampled by two in order to produce an image known as L and H . L is the image originally filtered in a low-pass (LPF) and divided into direction x , and H is the image originally filtered and divided into direction x .

Afterwards, each column of the new images is filtered with a LPF and HPF and sampled by two to produce 4 subimages (LL, LH, HL, and HH). LL is the original image filtered with LPF in a horizontal and vertical direction, sampled by two. LH is the original image filtered with LPF in a vertical direction sampled by two. HL is the original image filtered with HPF in a vertical direction, sampled by two. HH is the original image filtered with HPF in a horizontal and vertical direction, sampled by two. The four subband images contain all the information present in the original image, but their dispersed nature LH, HL, and HH makes them susceptible to compression [29].

In the case of the DDWT, it is defined in the same manner as the HDWT. If the input signal f has N values, then, the transform level 1 for the dB4 is the signal mapping f , $D1 \rightarrow (LH-HL)$ of signal f for the decomposition wavelet LH and HL. The main difference between the HDWT and the DDWT is in the definition of the escalation and the wavelets. The DDWT belongs to the orthogonal wavelet family, defined in a discrete manner and characterized by the number of vanishing moments for a given support. Each wavelet of this type generates a multiresolution analysis of different signal frequencies.

3.2. Detection of Threshold Noise Estimator. In the white Gaussian noise, there is a generalized way because of the frequency components in which it occurs. In the case of the images, this type of noise presents a normal distribution with a mean equal to zero and with an unknown variance σ^2 . In this specific case, to detect this kind of noise, we used the Gaussian white noise estimator (t_n) proposed by [30].

$$t_n = \sigma \sqrt{2 \log(n)} \quad (5)$$

σ is the noise standard deviation and n is the signal length. The SD is estimated using the first decomposition wavelet level, which contains a high frequency band inside the image and a high number of coefficients with noise. The main aim of the noise estimator is to quantify the noisy coefficients inside the decomposed image subbands. To achieve this, the estimation methods are used to provide a coefficient reduction. The main idea of a noise estimator is to detect the noisy coefficient to be able to preserve the information related to the image. We propose the implementation of the FMW, which serves as a threshold to noise discrimination along with the adapted NE-LML.

The FMW of an image can be considered as $FMW \geq 3\sigma_{n1}^4$, where n_1 represents the noise in the host image obtained from the first wavelet transform [18, 19].

The FMW of the subband LL, which contains information larger than $3\sigma_{nLL}^2$, where σ_{nLL}^2 denotes the subband LL noise power. Using this, the coefficients that represent noise can be localized and the threshold for the selection of the embedding region can be proposed.

We can estimate the noise power by applying the following equation:

$$\sigma_{IC}^2 = \arg \max R_{xx}(\tau) \quad (6)$$

where σ_{IC}^2 is the standard deviation of the cover image.

Finally, the power of then noise after going through the decomposition wavelet is

$$\sigma_{nLL}^2 = \frac{G \cdot \sigma_{nj}^2}{2}; \quad j = 1, 2 \quad (7)$$

where G represents the filter profits of the low and high-pass filters. Generalizing the formula, the noise power for any decomposition level of the subband LL is given by

$$\sigma_{njLL}^2 = \frac{G \cdot \sigma_{njLL}^2}{2}; \quad j = 1, 2 \quad (8)$$

If the focus is the filter profit as in [19], then

$$\sigma_{njLL}^2 = \sigma_{nj}^2; \quad j = 1, 2 \quad (9)$$

Thus, to detect the noisy coefficients, the following condition is defined as

$$LL_i = \begin{cases} LL_j; & \text{Si } E\{LL_j^4\} \geq (3\sigma_{nj}^4) \\ 0; & \text{otherwise} \end{cases} \quad (10)$$

To finally obtain the threshold value for the embedding of information using the noise estimator function of the filter NE-LML.

The function proposed for the embedding of information is proposed under the name of noise estimator for the embedding of information based on the local maximum likelihood of the image (NEII-LML) as follows:

$$NEII - LML = \arg \max_{\sigma, A_k} \left\{ \sum_{r=0}^R \sum_{c=0}^C \log \frac{LL(r, c)}{\sigma_{LL}^2} - \sum_{r=0}^R \sum_{c=0}^C \frac{LL(r, c) + A_k^2}{2\sigma_{LL}^2} + \sum_{r=0}^R \sum_{c=0}^C \log I_0 \left(\frac{LL(r, c) A_k}{\sigma^2} \right) \right\} \quad (11)$$

To finally propose the following threshold criterion,

$$Umbral = \arg \max_{\sigma, A_k} \left\{ \sum_{r=0}^R \sum_{c=0}^C \log \frac{LL(r, c)}{\sigma_{LL}^2} - \sum_{r=0}^R \sum_{c=0}^C \frac{LL(r, c) + A_k^2}{2\sigma_{LL}^2} + \sum_{r=0}^R \sum_{c=0}^C \log I_0 \left(\frac{LL(r, c) A_k}{\sigma^2} \right) \right\} \quad (12)$$

– FMW

4. Proposed Method

In summary, the algorithm for the information concealment process is presented in Algorithm 1.

The proposed concealment method consists of two sections, which are concealment, and information mapping, generating the *stego*-image. Now, the sections of the proposed steganography algorithm will be explained in detail.

4.1. Information Concealment. To analyze the concealment process of an image with the proposed algorithm, it is

1: Preprocessing: RGB cover image and image to be hidden are separated in their respective layers. Each layer is an 8-bit grayscale image.

2: **for** each layer **do**

3: Cover layer *dwt* decomposition: The discrete wavelet transformation or *dwt* Haar is applied to cover layer.

$$\xi(C) = C^\theta$$

Where $\xi(\cdot)$ denotes the *dwt* decomposition, C is the cover layer and $\theta = (LL, LH, HL, HH)$.

4: Hidden layer *dwt* decomposition: The discrete wavelet transformation or *dwt* Haar and Daubechies 4 are applied to the layer to be hidden.

$$\xi(H) = H^\theta$$

Where $\xi(\cdot)$ denotes the *dwt* decomposition, H is the layer to be hidden and $\theta = (ll, lh, hl, hh)$.

$$\xi(ll) = ll^\theta$$

Where $\xi(\cdot)$ denotes the *dwt* decomposition, ll is the approximation sub-band of first level of decomposition and $\theta = (ll1, lh1, hl1, hh1)$

5: Adjust information of sub-band: An adjust operation is applied to the sub-band $ll1$

$$ll1 = \left(\frac{ll1}{\sqrt{2^{24}}} \right)$$

6: Noise detection: Using a 3x3 Kernel as noise detection mechanism based on the local maximum likelihood is determined the umbral of change

$$Umbra1 = \operatorname{argmax}_{\sigma, A_k} \left\{ \sum_{r=0}^R \sum_{c=0}^C \log \frac{LL(r, c)}{\sigma_{LL}^2} - \sum_{r=0}^R \sum_{c=0}^C \frac{LL(r, c) + A_k^2}{2\sigma_{LL}^2} + \sum_{r=0}^R \sum_{c=0}^C \log I_0 \left(\frac{LL(r, c) A_k}{\sigma^2} \right) \right\} - FMW$$

7: **if** The element of the kernel meet the condition $k(i, j) \leq umbra1$ **then**

8: Do the change in the sub-band HH for the element in the sub-band $ll1$

$$New_HH(x, y) = ll1(x1, y1)$$

9: Do the change in the subband LH for the element in the sub-band HL

$$New_LH(x, y) = HL(x, y)$$

10: **if** The element changed in the sub-band HL meet the condition $HL(x, y) \geq 0$ **then**

11: Change the element in the sub-band HL according to

$$New_HL(x, y) = HL(x, y) + ll1(x1, y1)$$

12: **else**

13: Change the element in the sub-band HL according to

$$New_{HL(x,y)} = HL(x, y) - ll1(x1, y1)$$

14: **end if**

15: **end if**

16: Generate Stego layer: Obtain modified sub-bands coefficients and apply inverse discrete wavelet transform or *idwt* Haar to form the stego layer

$$\xi^{-1}(C^\theta) = S$$

Where $\xi^{-1}(\cdot)$ denotes the inverse discrete wavelet transform, $\theta = (L, New_{LH}, New_{HL}, New_{HH})$ and S the stego layer

17: **end for**

19: Generate Stego Image: The resulting layers are combined to obtain a RGB image.

ALGORITHM 1: Information concealment.

necessary to separate the cover image and the image to be hidden in their respective layers; in this case, we worked on RGB color space. Because of the aforementioned, the layers obtained in each image correspond to the color red (R), green (G), and blue (B). After, a “Haar” wavelet decomposition level is applied to each layer of the cover image (IC), as a result, four subimages are obtained: the approximation (LL), the horizontal details (LH), the vertical details (HL), and the diagonal details (HH).

For the image to be hidden (IO), each of its layers receives two levels of wavelets decomposition; in the first level, the “Haar” wavelet is employed, obtaining 4 subbands (ll, lh, hl, and hh) in the case of the layers of the image to be hidden; the Daubechies 4 (db4) is applied to the second decomposition level, to the approximation (LL), obtaining 4 new subbands: the approximation (ll1), the horizontal details (lh1), the vertical details (hl1), and the diagonal details (hh1).

Once they are obtained, the subbands to be employed are separated as in the following method: from the layers of the image, the LH, HL, and HH are used; they contain the coefficient values and the diagonal details; that is to say, they keep the information from the edges of the image, which, by going through modifications, is not affected in comparison with the original. In the case of the layers of IO, the ll1 is used, which contains the coefficients values from approximations corresponding to the second level of decomposition. The reason why this subband is chosen is because the information that it contains defines the majority of the image to conceal [31].

Previous to the information concealing, an adjustment to the escalation is done, based on the work [24]. This process is carried out in the ll1 to avoid that any inserted values in the IC visually alter the information and thus provoke changes in the resulting image. Because you are working in a RGB space,

the employed image is at a depth of 24 bits. Taking these into consideration, the adjustment operation is described as in the following equation [13]:

$$ll1 = \left(\frac{ll1}{\sqrt{2^{24}}} \right) \quad (13)$$

where $ll1$ is the coefficients subband of the image approximation to conceal from its second level of wavelet decomposition, $\sqrt{2^{24}}$ factor corresponding to the base 2 (bit) raise to the image depth (24 bits).

As a result of the escalation adjustment, an adjustment of the $ll1$ subband values is obtained; these new bands are identified as New_LH , New_HL , and New_HH . From these new information subbands, we go through them though a windowing, using 3x3 Kernel detection mechanism ($K_{i,j}$, $i,j= 1,2,3,\dots, 9$), which will scroll thought the subband to detect in detail the values prone to be replaced. This Kernel acts as a noise detector in the subband HH, using the following condition: “the corresponding noise threshold will be calculated every time the Kernel positions itself in the subband; if any of the values is minor or equal to the obtained threshold, this value is changed for one of the values to hide in subband $ll1$ ”, defined for

$$SI = \begin{cases} ll1; & K(i, j) \leq umbral \\ LL; & de otra manera \end{cases} \quad (14)$$

where $ll1$ is the second level of wavelet decomposition in IO, $K_{i,j}$ is the current position of the Kernel in the subband, and LL is the first level of decomposition in IC.

4.2. Mapping Embedded Information. To ensure that the embedded data is recovered, the substitution of the proposed values in this research is done in the subband New_HH in order not to alter the calculation of the threshold value in the moment of applying the Inverse Discrete Wavelet Transformation (IDWT). In the subband New_LH , a change is made to store now the original value of the HL subband in the corresponding position. In New_HL subband, the change is made according to the following function:

$$New_HL(x, y) = \begin{cases} HL(x, y) + ll1(x_1, y_1), & si \ HL(x, y) \geq 0 \\ HL(x, y) - ll1(x_1, y_1), & si \ HL(x, y) < 0 \end{cases} \quad (15)$$

where $HL(x, y)$ is the current value of subband HL, $ll1(x_1, y_1)$ is the current value of subband $ll1$, $New_HL(x, y)$ is the new value of subband HL, x, y is current position in the obtained subband of IC, and x_1, y_1 is the current position of the obtained subband of IO.

The mapping condition was proposed to guarantee minimal distortion and the information retrieval so that the complement of the operation between the original HL subband and the value to hide of subband $ll1$ is stored in subband New_HL , according to the condition given by (15).

While the complement of the obtained value (key) is stored in subband New_LH , for New_HL as of the condition given for (16), it is defined next

$$New_LH(x, y) = \begin{cases} New_HL(x, y) - ll1(x_1, y_1), & si \ HL(x, y) \geq 0 \\ NNew_HL(x, y) + ll1(x_1, y_1), & si \ HL(x, y) < 0 \end{cases} \quad (16)$$

In this way, subband New_HL is used as another level of access security to the information called *key*. With the generated key and applying the complement with New_LH , the positions where the embedding was carried out will be secured.

Once the subband $ll1$ values are hidden inside subband New_HH , the reconstruction process through the “Haar” wavelet is carried out, using the subbands LL , New_LH , and New_HH , in each obtained layer according to the color space, in this case the RGB. As a result, a new image, known as steganography image, is obtained.

4.3. Image Recovery. In summary, the algorithm for the image recovery process is shown in Algorithm 2.

In order to carry out the extraction process using the proposed algorithm, it is necessary to separate the RGB steganography image (SI) in each layer; during the separation into layers, the red (RSI), green (GSI), and blue (BSI) layers participate. Afterwards, each layer receives a level of wavelet decomposition, employing the “Haar” wavelet. As a result of the decomposition in the RGB layers, four subbands are obtained, corresponding to the approximation coefficients (LLSI), the horizontal detail coefficients (LHSI), the vertical detail coefficients (HLSI), and the diagonal detail coefficients (HHSI).

Once the first level of wavelet decomposition is applied, the corresponding subbands are obtained, in the case of subband LHSI, where the recovery map is stored, which allows us to identify the areas where the information of the IO is stored.

Subband HL is used as a key, which allows confirming that the localized values in the given positions in the map correspond to the hidden image, and, finally, in subband HH, the original values of the hidden image are stored.

With the purpose of identifying the correct embedded information, it is necessary to use the stored values in subband New_HL because the generated key and the stored value in subband New_HH have to coincide; this corresponds to one of the original values of IO, obeying the following condition:

$$Imagen \ Recuperada(x, y) = \begin{cases} LHIE + HLIE, & si \ HHIE \geq 0 \\ LHIE - HILE & si \ HHIE < 0 \end{cases} \quad (17)$$

Next, the subband identified as New_LL is created, in which the extracted values will be stored. From the subband separation, the Kernel 3x3 is defined; it will be used to extract the position values where there might be a value corresponding

```

1: Preprocessing: RGB stego-image is separated in its respective layers.
2: for each layer do
3:   Stego layer dwt decomposition: The discrete wavelet transform or dwt Haar is applied to stego layer.
       $\xi(S) = S^\theta$ 
Where  $\xi(\cdot)$  denotes the dwt decomposition,  $S$  is the cover layer and  $\theta = (LL1, LH1, HL1, HH1)$ .
4:   Extraction process: Using a 3x3 Kernel as reconstruct detector is applied to the sub-band LH1 (Map)
5:   if The element in the Kernel meet the condition  $K(i, j) \geq 0$  then
6:     Calculate the confirmation element as
       $N = HL1(x, y) - HH1(x, y)$ 
7:   else
8:     Calculate the confirmation element as
       $N = HL1(x, y) + HH1(x, y)$ 
9:   end if
10:  if  $K(i, j) - N = 0$  then
11:    Abstract the element of the sub-band HH1 to the recover sub-band
       $New\_ll(x1, y1) = HH1(x, y)$ 
12:  end if
13:  Adjust information of sub-band: An adjust operation is applied to the information in the recover sub-band New_ll
       $New\_ll = New\_ll * \sqrt{2^{24}}$ 
14:  Generate recover layer: Is applied the inverse discrete wavelet transform or idwt Daubechis 4 to the recover sub-bands to form
the recover sub-band ll, also is applied the inverse discrete wavelet transform Haar to the recover sub-band ll and sub-bands lh, hl, hh
to form the recover layer
       $\xi^{-1}(ll^\theta) = ll$ 
Where  $\xi^{-1}(\cdot)$  denotes the idwt, ll is the recover sub-band and  $\theta = (New\_ll, lh1, hl1, hh1)$ .
       $\xi^{-1}(R^\theta) = R$ 
Where  $\xi^{-1}(\cdot)$  denotes the idwt, R is the recover layer and  $\theta = (ll, lh, hl, hh)$ .
15: end for
16: Generate Recover Image: The resulting layers are combined to obtain a RGB image

```

ALGORITHM 2: Image recovery.

to the hidden image. This Kernel runs through the subband LH as a sliding window to extract the values in the correct order for the reconstruction.

Every time the Kernel is positioned in the subband a verification is executed in each of the values contained in the Kernel; in this verification, the obtained key is used by the subband HL. If a hidden value is found in the corresponding position, the supplement of the operation performed when the image was hidden must be stored, while the subband HH stores the original values of the hidden image. Thus, the result should be equal or approximate to the original value stored in subband LH; the latter is used as a map. The function used to the verification is defined next:

$$N = \begin{cases} HL(x, y) - HH(x, y), & \text{si } Kernel(i, j) \geq 0 \\ HL(x, y) + HH(x, y), & \text{si } Kernel(i, j) < 0 \end{cases} \quad (18)$$

where N is a value to be corroborated with the map (subband LH) to obtain the position of the value to be extracted; $HL(x, y)$ is the value of subband HL in the current position and stores the supplement of the operation performed when the image was hidden; $HH(x, y)$ is the value of subband HH in the current position and stores the original value of the hidden image; $Kernel(i, j)$ is the Kernel value in the current position.

Once the verification of the result is performed, it is corroborated with the value in the map contained in subband LH or in the Kernel. If the difference between these values lies

within the range -1 and 1, then, the value corresponding to the current position, stored in subband HH, corresponds to the value of the hidden image, for which the identified value is copied in the subband *New_LL*.

Once all the values of the hidden image are extracted, an adjustment operation is carried out to recover the original values of the hidden image.

Due to the fact that all of this is done in the color space RGB and that all of the images have a depth of 24 bits, the adjustment operation is described as follows:

$$New_LL = New_LL * \sqrt{2^{24}} \quad (19)$$

where *New_LL* is the approximation coefficients subband of the extracted image in a second level of wavelet decomposition; $\sqrt{2^{24}}$ adjustment factor corresponding to base 2 (bit) rose to the image depth (24 bits). As a result of applying the adjustment operation, a new subband *New_LL* is obtained.

This is used, along with the subband of the second level of decomposition of the hidden image *lh1*, *hl1*, and *hh1*, to perform the wavelet recomposition.

This process employs the wavelet “db4”, and, as a result, the approximation *ll* coefficients subband, corresponding to the first level, is obtained. Then, the recomposition process is performed again, using the resulting subband *ll*, and subbands *lh*, *hl*, and *hh*. For this level, the “Haar” wavelet is used.

The layers obtained in the reconstruction process are combined according to the color space in which the process

FIGURE 1: Image pairings formed for the experiment done with the proposed steganography algorithm. Cover images: (a) boat (1024 x 768 pixels); (c) sphinx (1024 x 768 pixels); (e) paradise (1024 x 768 pixels); (g) prayer (1024 x 768 pixels); (i) mountain (1024 x 768 pixels); (k) fire (1024 x 768 pixels); (m) wood fire (1024 x 768 pixels); and (o) lena (256 x 256 pixels). Images to be hidden: (b) Agfa (712 x 534 pixels); (d) snow (712 x 534 pixels); (f) desert (1024 x 768 pixels); (h) skullcap (1024 x 768 pixels); (j) landscape (1024 x 768 pixels); (l) mosque (1024 x 768 pixels); (n) cactus (576 x 768 pixels); and (p) mandrill (256 x 256 pixels).

was performed. As a result, a new image is obtained, which is called recovered image.

5. Results and Discussion

5.1. Testing and Results. In this section, the robustness, the embedded data imperceptibility, and the information retrieval are validated, as well as the quality of the stego-image and of the recovered one.

The experiments were done with a group of images ordered in pairs. In each pair, one image is used as the cover object, while the other is the image to be hidden. The pairs were formed randomly, resulting in the pairing shown in Figure 1.

The images selected for the validation tests have a .jpg format, with a depth of 24 bytes in the color space RGB. Each test was done following the procedure described next:

- (1) The proposed algorithm was used to hide the selected image inside the cover image, obtaining a new image tagged as stego-image.
- (2) Once the stego-image was obtained, the cover and the stego-image were compared with the following criteria:
 - (a) Correlation: it represents the statistical dependency: it establishes the lineal relation between the change in magnitude and direction between two different signals. The correlation is defined as

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right) \left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \quad (20)$$

- (b) The mean square error (MSE): the mean square error is a risk function between two images that allows identifying the squares of the loss regarding the expected value and the obtained value; that is to say, it reflects the difference between both images in relation to the expected values. Equation (21) served to calculate this coefficient,

$$MSE = \frac{1}{mn} \sum_m \sum_n (A_{mn} - B_{mn})^2 \quad (21)$$

where MSE is the mean square error, A_{mn} is the image original size $m \times n$, and B_{mn} is the obtained image size $m \times n$.

The MSE serves as a base to calculate the following metric used. The peak signal-to-noise ratio (PSNR) is a term used to define the relation between the maximum possible power of an image and the noise that affects it. In this case, the noise is the presence of the new information embedded during the concealment, or the loss of information during the retrieval of the information from the stego-image.

With a lower MSE, the PSNR will tend to infinity, which means that the image compared with the original is a faithful copy. Equation (22) was used to obtain this coefficient.

$$PSNR = 10 * \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (22)$$

where $PSNR$ is the relation coefficient of the peak signal-to-noise ratio and MAX_I^2 is the maximum value in the layer I squared. For the color space RGB, the maximum value is 255.

- (c) Root mean square error is given by

$$RMSE = \sqrt{\frac{1}{mn} \sum_m \sum_n (A_{mn} - B_{mn})^2} \quad (23)$$

- (d) Normalized absolute error and image fidelity can be expressed as

$$NAE = \frac{\sum_m \sum_n (A_{mn} - B_{mn})}{\sum_m \sum_n (A_{mn})} \quad (24)$$

$$IF = 1 - \frac{\sum_m \sum_n (A_{mn} - B_{mn})^2}{\sum_m \sum_n (A_{mn})^2} \quad (25)$$

- (e) Histogram: the histogram of the images allows having a notion of their spectrum and how it is affected during the hiding and retrieval process. Besides, it allows the calculation of other metrics as it is the case of the standard deviation.

- (f) Standard deviation: the standard deviation of an image reflects the dispersion of the values regarding its mean value; this value is obtained from the square of the variance of the image. In order to obtain the variance out of the histogram of the image, (26) is employed.

$$\sigma^2 = \sum_{i=0}^n p_i * (x_i - \mu)^2 \quad (26)$$

where σ^2 is the variance of the image, p_i is the appearance frequency of the value, x_i , x_i are the pixel intensity, and μ is average intensity of the image.

Each of these measures was compared in each layer and in the image in general. The recuperation process of the hidden image followed, obtaining a new image tagged as the recovered image.

Having obtained the recovered image, a second comparison was made between the latter and the image to be hidden, using the metrics described in the point 2, for the case of the cover and the stego-image. Finally, the cover image and the image to be hidden were rotated, repeating the process from point 1. The rotation applied to the images was done according to what is established in Table 1, where the column of the number of the rounds specifies the type of rotation that will be made to each image. The set of rounds is applied to each pair of images, because there are only 2 types of rotations, which apply to the 8 pairs of images; in total 16 images are obtained.

From Figure 1, 4 sets in total are obtained. The rotation column makes reference to the rotation in grades of each of the images. Towards the end, the first set obtained a rotation of 0° in each image; in the second round, the cover image is rotated 45° and the image to be hidden is rotated 0° ; in the third round, the cover image is rotated 0° and the hidden image 180° ; finally, in the fourth round, the images are rotated 45° and 180° , respectively.

As previously mentioned, the proposed algorithm was evaluated by means of quality image metrics applied to each obtained steganographic image and to each recovered image. Figure 2 shows a group of steganographic images obtained from the first round of tests together with the quality metrics of each one, from which it can be seen that any alteration in the images is not visible.

From (20), (21), (22), (23), (24), (25), and (26), the algorithm performance rate is calculated, comparing the new obtained images and the original ones. From the correlation between the images, it is possible to establish the degree of similarity between them, based on the fact that the correlation coefficient between the images reflects the level of the lineal relation between them, that is to say, the existing relation between the quantities of energy that they possess. When the coefficient value approaches 1, it reflects that the changes in energy, in terms of magnitude and direction, are similar; thus, it can be said that they are the same image. Whereas when it approaches 0, the coefficient value reflects a drastic change between the images, which implies that the original image

TABLE 1: Image rotation.

Round No.	Rotation of the cover image with respect to 0°	Rotation of the image to be hidden with respect to 0°
1	0°	0°
2	45°	0°
3	0°	180°
4	45°	180°

(a) PSNR = 52.6092. RMSE = 0.5974. NAE = -0.00006. IF = 0.9999. $r = 0.9998$

(b) PSNR = 51.6823. RMSE = 0.6644. NAE = -0.00004. IF = 0.9999. $r = 0.9995$

(c) PSNR = 38.9523. RMSE = 2.8769. NAE = 0.0002. IF = 0.9985. $r = 0.9969$

(d) PSNR = 39.7741. RMSE = 2.6171. NAE = -0.00009. IF = 0.9986. $r = 0.9948$

(e) PSNR = 40.6538. RMSE = 2.3650. NAE = -0.0001. IF = 0.9986. $r = 0.9973$

(f) PSNR = 46.9981. RMSE = 1.1395. NAE = -0.0025. IF = 0.9851. $r = 0.9851$

(g) PSNR = 51.3264. RMSE = 0.6923. NAE = -0.0001. IF = 0.9998. $r = 0.9998$

(h) PSNR = 41.3803. RMSE = 2.1762. NAE = -0.0001. IF = 0.9988. $r = 0.9950$

FIGURE 2: Resulting stego-images obtained. Imperceptibility of proposed algorithm via image quality metrics for test images.

was drastically changed. In order to obtain this coefficient, we used (20).

In Tables 2 and 3, the results of the correlation coefficients obtained are shown. Based on this data, the worst result in the concealment process was in test 6 during round 3, in which the stego-image presents a difference of 1.5 % with respect to the cover image. The best result was test 7 in rounds 1 and 3, in which the stego-image barely differs in 0.02% in respect to the cover image. Despite the fact that the stego-image differs in all the tests, the change is not visually perceptible. The best correlation found per layer is in the red layer in test 7 in both round 2 and round 4, the best overall result is in test 7 in round 1 and round 4, and it was also identified that the layer with the best correlation between the original image and the stego-image is the red layer. The layer with the worst correlation was found in test 6 in round 3; in the same test and round, the worst general correlation was presented; the layer with the worst correlation between original image and stego-image is blue.

In contrast with the results of the comparison between the cover and the stego-image, the results of the comparison between the recovered image and the image to be hidden

shown in Table 3 reflect that, in 75% of the cases, the same image was recovered. However, in 81.25 % of the cases, the images are visually perceived as identical. The worst result was in test 6, during round 3, in which the recovered image differs by 19.5% from the image to be hidden. This case coincides with the worst case identified in the concealment process. In this table, the best results were not marked because in most cases they present the best possible result 1, which indicates that the stored image was recovered exactly; the layer with the best correlation identified is the red layer.

In order to validate the results, metrics MSE and PSNR were used. The MSE allows identifying the alteration level that the obtained image had in regard to the original image, whereas the PSNR, being used with the images, allows us to measure the alteration level of the information in regard to its format. The PSNR of the RGB image is in the JPG format between 35dB and 55dB. So, by presenting values out of this range, the images show drastic visual alterations, and so does their perception.

In Tables 4 and 5, the results of the MSE between the cover and the stego-image are shown and between the recovered and the image to be hidden, respectively. The obtained data

TABLE 2: Correlation between the cover image and the stego-image.

Test	Round	Red color channel	Green color channel	Blue color channel	General
1	1	0.999782	0.999864	0.999894	0.999894
	2	0.999319	0.999509	0.999529	0.999452
	3	0.999782	0.999864	0.999894	0.999894
	4	0.999319	0.999509	0.999529	0.999452
2	1	0.999281	0.999628	0.999835	0.999581
	2	0.999727	0.999763	0.999721	0.999737
	3	0.999281	0.999628	0.999835	0.999581
	4	0.999727	0.999763	0.999721	0.999737
3	1	0.997414	0.996376	0.996962	0.996917
	2	0.998442	0.998682	0.998661	0.998595
	3	0.997414	0.996376	0.996962	0.996917
	4	0.998442	0.998682	0.998661	0.998595
4	1	0.994611	0.994202	0.995620	0.994811
	2	0.999071	0.998778	0.998276	0.998708
	3	0.994611	0.994202	0.995620	0.994811
	4	0.999071	0.998778	0.998276	0.998708
5	1	0.997158	0.997126	0.997914	0.997399
	2	0.997915	0.997978	0.997952	0.997948
	3	0.997158	0.997126	0.997914	0.997399
	4	0.997915	0.997978	0.997952	0.997948
6	1	0.997515	0.992386	0.965509	0.985137
	2	0.997548	0.993451	0.975926	0.988975
	3	0.997515	0.992386	0.965507	0.985136
	4	0.997548	0.993451	0.975927	0.988975
7	1	0.999924	0.999907	0.999853	0.999895
	2	0.999936	0.999876	0.999809	0.999873
	3	0.999924	0.999907	0.999853	0.999895
	4	0.999936	0.999876	0.999809	0.999873
8	1	0.996496	0.996155	0.992594	0.995082
	2	0.998677	0.997524	0.997884	0.998028
	3	0.996496	0.996155	0.992595	0.995082
	4	0.998677	0.997524	0.997884	0.998028
Average		0.998192	0.99757531	0.99474619	0.99687697

confirmed what was stated by the correlation. Presenting MSE minor to 10, the image distortion is noticeable to the naked eye. The obtained data show that the more drastic distortions occurred in test 6, confirming so with the PSNR data.

As can be seen in Table 4, the lower the MSE, the lower will be the distortion obtained in the resulting image and, therefore, the stego-image will have the highest quality. The lowest MSE detected was presented in test 2 round 2 green layer, in which also the best overall result of the stego-image was obtained according to this metric. On the other hand, the worst result was presented in test 3 round 1 green layer; in the same way in the same test and round, the worst result of this metric was detected. When analyzing each layer, it was detected that on average the layer that presents an MSE is the blue layer and the one that presented the worst results is the green layer; these results are at the end of Table 4.

In the case of Table 5, the results obtained allow us to observe that the MSE between the recovered image and the original image to be hidden in 75% of the cases is 0; in other words, the best possible result is obtained. The worst result that was obtained was presented in the test 6 round 3 in the blue layer; in the same way in the same test and round the general result was obtained. When an analysis of each layer was made, it was detected that on average the layer with the lowest MSE and the best quality is the red layer and the one with the highest MSE and the worst quality is the blue layer; these results are shown at the end of Table 5.

Tables 6 and 7 show the results between the cover and the stego-image and the recovered image and the image to be hidden, respectively. These values confirm the distortion presented by the image. In the case of the cover images, as they are in a range between 35 dB and 55 dB, the distortion is almost imperceptible, being the most notorious case when

TABLE 3: Correlation between the recovered image and the image to be hidden.

Test	Round	Red color channel	Green color channel	Blue color channel	General
1	1	1	1	1	1
	2	1	1	1	1
	3	1	1	1	1
	4	1	1	1	1
2	1	1	1	1	1
	2	1	1	1	1
	3	0.968956	0.934658	0.978830	0.960815
	4	0.968956	0.934573	0.978830	0.960786
3	1	1	1	0.974247	0.991415
	2	1	1	0.974247	0.991415
	3	1	1	1	1
	4	1	1	1	1
4	1	1	1	1	1
	2	1	1	1	1
	3	1	1	1	1
	4	1	1	1	1
5	1	1	1	1	1
	2	1	1	1	1
	3	1	1	1	1
	4	1	1	1	1
6	1	0.903405	0.941577	0.969175	0.938052
	2	0.902387	0.940640	0.966733	0.936587
	3	0.937927	0.775679	0.703393	0.805666
	4	0.937927	0.775711	0.704134	0.805924
7	1	1	1	1	1
	2	1	1	1	1
	3	1	1	1	1
	4	1	1	1	1
8	1	1	1	1	1
	2	1	1	1	1
	3	1	1	1	1
	4	1	1	1	1
Average		0.98811119	0.97821369	0.97654966	0.98095813

it approaches the inferior limit. In the case of the recovered images, being exactly the same recovered image, a MSE of 0 is obtained, so the PSNR tends to infinity, proving, thus, that the information is not lost and that the image has not been distorted, excluding the cases in which the MSE is very big and stays out of the range in which the visual distortion is noticeable.

The results of Table 6 allow us to observe that there is a change in the cover images and stego-images; however, the higher the PSNR the lower the change that can be perceived quantitatively. The best detected result was presented in the green layer in the round 2 test 2. In the same test and round the best overall result was obtained. The worst result was detected in test 3 round 1 in the red layer; in turn, in the same test and round the worst result was detected in a general way. On average, as shown in Table 6, the red layer is the one that presents the least similarity according to this metric, while the

blue layer shows the greatest possible similarity; these results are shown in the lower part of Table 6.

In Table 7, it can be seen that the best possible result to obtain from the PSNR is when it tends to infinity, meaning that both images compared are the same. The worst result obtained in the recovery process was presented in test 6 round 3 in the blue layer; in the same way in the same test and round the worst result was obtained in a general way.

From the histograms of each layer of the images, it was identified that, in the recovered images where a distortion is present, it is due to the fact that the cover image has two characteristics that limit the random behavior of the same, reducing the areas where the information can be hidden without causing distortions: the spectrum of the cover images is very small, in addition to the fact that the distribution of its energy is mostly concentrated in only one area. In the case of the cover images that are distorted, it was identified

TABLE 4: MSE between the cover and the stego-image.

Test	Round	Red color channel	Green color channel	Blue color channel (%)	General
1	1	0.365856	0.325675	0.380532	0.357354
	2	0.758291	0.734674	0.729939	0.740968
	3	0.365821	0.325683	0.380537	0.357347
	4	0.758284	0.734668	0.729982	0.740978
2	1	0.423123	0.451900	0.449883	0.441635
	2	0.261577	0.257414	0.262264	0.260418
	3	0.423122	0.451886	0.449836	0.441615
	4	0.261567	0.257416	0.262247	0.260410
3	1	8.319886	8.328872	8.181875	8.276878
	2	3.189513	3.13534	3.124408	3.149753
	3	8.319661	8.329120	8.181615	8.276799
	4	3.189538	3.135373	3.124438	3.149783
4	1	6.777896	6.880593	6.890575	6.849688
	2	2.850955	2.735148	2.949328	2.845144
	3	6.777959	6.880584	6.890474	6.849672
	4	2.850997	2.735156	2.949315	2.845156
5	1	5.630324	5.569602	5.581381	5.593769
	2	3.001218	3.008714	3.038632	3.016188
	3	5.630263	5.569493	5.581288	5.593681
	4	3.001173	3.008617	3.038642	3.016144
6	1	1.362135	1.312413	1.223167	1.299238
	2	0.668241	0.627319	0.592154	0.629238
	3	1.362071	1.312585	1.223302	1.299319
	4	0.668210	0.627351	0.592130	0.629230
7	1	0.508318	0.468532	0.461859	0.479570
	2	0.332260	0.315941	0.311096	0.319766
	3	0.508345	0.468496	0.461882	0.479574
	4	0.332215	0.315927	0.311113	0.319752
8	1	4.661071	5.125930	4.435363	4.740788
	2	2.573647	3.008151	2.636386	2.739397
	3	4.661636	5.125854	4.435012	4.740834
	4	2.573647	3.008151	2.636386	2.739397
Average		2.60527563	2.64289306	2.57803253	2.60873384

that the images to be hidden present a very broad spectrum with an inclination of the energy after an abrupt change of its distribution.

The histograms of the cover images and stego-images are shown in Figure 3; for each pair of images the corresponding histogram was graphed for each layer that make them; each one of them is shown with the color of each layer. The histograms corresponding to the cover images are shown in a light tone, while the histograms of the stego-images are shown in a darker tone. When being plotted in an overlapping way, it is possible to identify the changes in energy that may occur between the images; as a sign of the imperceptibility of the proposed algorithm changes in intensity are not perceptible in most cases. The cases with the most notorious alterations were detected in tests 4 (d), 6 (f), and 8 (h); in these cases a visual distortion was perceived between the cover image and the stego-image.

The histograms of the images to be hidden and recovered images are shown in Figure 4; as for the cover images and stego-images, the histograms of each layer that make up the images were plotted. The light tone histograms correspond to the original images, while the dark tone histograms correspond to the recovered images. The comparison of the histograms of these pairs of images allows us to evaluate the integrity of the recovery process. By analyzing the histograms obtained, the results obtained were reaffirmed by means of the previously mentioned metrics such as correlation, MSE, and PSNR. Within the results obtained, the histogram corresponding to test 6 (f) is the one in which a greater number of discrepancies are distinguished between the original image and the recovered image.

Lastly, the metric that conformed how the distribution of the obtained images was affected in relation to the originals, the standard deviation, was calculated from the

TABLE 5: MSE between the recovered image and the image to be hidden.

Test	Round	Red color channel	Green color channel	Blue color channel	General
1	1	0	0	0	0
	2	0	0	0	0
	3	0	0	0	0
	4	0	0	0	0
2	1	0	0	0	0
	2	0	0	0	0
	3	17.697502	24.401398	16.299265	19.466055
	4	17.697502	24.393350	16.299265	19.463372
3	1	0	0	19.684749	6.561583
	2	0	0	19.684749	6.561583
	3	0	0	0	0
	4	0	0	0	0
4	1	0	0	0	0
	2	0	0	0	0
	3	0	0	0	0
	4	0	0	0	0
5	1	0	0	0	0
	2	0	0	0	0
	3	0	0	0	0
	4	0	0	0	0
6	1	24.257998	24.717053	22.891731	23.955594
	2	24.215700	24.671521	22.810550	23.899257
	3	24.280156	41.341527	58.075026	41.232236
	4	24.280156	41.322372	57.923755	41.175428
7	1	0	0	0	0
	2	0	0	0	0
	3	0	0	0	0
	4	0	0	0	0
8	1	0	0	0	0
	2	0	0	0	0
	3	0	0	0	0
	4	0	0	0	0
Average		4.13840669	5.65147566	7.30215906	5.69734713

information in the histograms. Table 8 shows the comparison of the standard deviation between the cover image and the stego-image; Table 9 shows the comparison of the standard deviation between the recovered image and the one to be hidden.

The results in Table 8 allow us to identify the difference between the standard deviation of the cover image and the image-steamer. The smaller difference between these smaller changes will be shown in the information contained in each image; the smallest difference was detected in test 2 round 3 in the red layer; in the same way it was in the same test and round and detected the best result in a general way. Regarding the greatest difference detected, it was detected in test 6 round 4 in the blue layer; likewise in general, the difference was detected in the same test and round.

The results shown in Table 9 allow us to observe that in 75% quantitatively no change in the distribution of

information between the recovered image and the original image was presented. The greatest difference detected was presented in test 6 round 2 in the green layer, and in the same way in the same test and round the greater general difference between the images was detected.

Through the standard deviation, the structural change that the obtained images suffered was identified. The value distribution was affected, as indicated in the histogram, which is reflected in the visual distortion, even though the structure is preserved. By having changes in the energy distribution, the perception of ghost images is provoked, as shown in Figure 5.

The recovered images as well as the cover images were subjected to image quality metrics to check the efficiency of the algorithm proposed in the recovery process. Figure 6 shows the recovered images as well as the metrics corresponding to each one; with these metrics it can be perceived

TABLE 6: PSNR between the cover image and the stego-image.

Test	Round	Red color channel (dB)	Green color channel (dB)	Blue color channel (dB)	General
1	1	52.497699	53.002946	52.326885	52.609177
	2	49.332439	49.469855	49.497932	49.433408
	3	52.498107	53.002844	52.326827	52.609259
	4	49.332481	49.469888	49.497680	49.433350
2	1	51.866130	51.580375	51.599800	51.682102
	2	53.954805	54.024465	53.943410	53.974227
	3	51.866143	51.580509	51.600254	51.682302
	4	53.954960	54.024444	53.943688	53.974364
3	1	38.929629	38.924941	39.002274	38.952281
	2	43.093559	43.167957	43.183125	43.148214
	3	38.929747	38.924812	39.002413	38.952324
	4	43.093524	43.167910	43.183083	43.148173
4	1	39.819854	39.754544	39.748248	39.774215
	2	43.580898	43.760993	43.433572	43.591821
	3	39.819814	39.754550	39.748312	39.774225
	4	43.580834	43.760982	43.433590	43.591802
5	1	40.625469	40.672561	40.663386	40.653805
	2	43.357827	43.346994	43.304021	43.336280
	3	40.625516	40.672646	40.663458	40.653874
	4	43.357893	43.347133	43.304007	43.336344
6	1	46.788600	46.950096	47.255944	46.998213
	2	49.881468	50.155912	50.406454	50.147945
	3	46.788802	46.949528	47.255466	46.997932
	4	46.788802	46.949528	47.255466	46.997932
7	1	51.069443	51.423405	51.485705	51.326185
	2	52.916019	53.134731	53.201847	53.084199
	3	51.069215	51.423735	51.485490	51.326147
	4	52.916605	53.134927	53.201621	53.084384
8	1	41.445945	41.033076	41.661511	41.380177
	2	44.025312	43.347796	43.920712	43.764607
	3	41.445419	41.033140	41.661854	41.380138
	4	44.025312	43.347796	43.920712	43.764607
Average(dB)		46.3524459	46.3842193	46.4412108	46.3926254

that the quality of the images is maintained in 87.5% of the cases.

Figure 7 shows a comparison of the cover images and the obtained stego-images. As it can be noticed visually, not in all the cases an alteration in the image can be appreciated, without detecting that they contain hidden information inside.

Figure 8 shows the comparison between the recovered images and the original images to be hidden. In contrast to the concealment contrast, during the retrieval process the case of test 6 was presented, in which the visual distortion is noticeable, while in the rest of the cases, distortions, if any, were imperceptible.

In addition to the validation tests carried out, an insertion capacity test was carried out, during this test the amount of information that is inserted in the cover image corresponding to the image to be hidden was measured, this information

corresponds to the values of each pixel of each layer, as well as the values of the key and map employees. Equation (27) describes the measurement of capacity and insertion:

$$In = C * 8 \text{ bits} * l \quad (27)$$

where In corresponds to the information that has been inserted, C corresponds to the amount of data to be inserted (pixels, key, and map), and l is the number of layers that make up the image; in this case it is equal to 3 for the space of color RGB.

Table 10 showed the results of this test.

With this test, it is verified that the proposed algorithm allows inserting information in the cover image in a small fraction of it; on average, it is observed that the information of the image to be hidden is in 5.01% of the cover image. The smallest result identified is 3.03% in tests 1 and 2; in the

TABLE 7: PSNR between the recovered image and the image to be hidden.

Test	Round	Red color channel (dB)	Green color channel (dB)	Blue color channel (dB)	General (dB)
1	1	∞	∞	∞	∞
	2	∞	∞	∞	∞
	3	∞	∞	∞	∞
	4	∞	∞	∞	∞
2	1	∞	∞	∞	∞
	2	∞	∞	∞	∞
	3	35.651683	34.256656	36.009123	36.009123
	4	35.651683	34.258089	36.009123	35.306298
3	1	∞	∞	35.189504	∞
	2	∞	∞	35.189504	∞
	3	∞	∞	∞	∞
	4	∞	∞	∞	∞
4	1	∞	∞	∞	∞
	2	∞	∞	∞	∞
	3	∞	∞	∞	∞
	4	∞	∞	∞	∞
5	1	∞	∞	∞	∞
	2	∞	∞	∞	∞
	3	∞	∞	∞	∞
	4	∞	∞	∞	∞
6	1	34.282254	34.200836	34.534017	34.339035
	2	34.289833	34.208844	34.549445	34.349374
	3	34.278288	31.966938	30.490909	32.245378
	4	34.278288	31.968951	30.502236	32.249825
7	1	∞	∞	∞	∞
	2	∞	∞	∞	∞
	3	∞	∞	∞	∞
	4	∞	∞	∞	∞
8	1	∞	∞	∞	∞
	2	∞	∞	∞	∞
	3	∞	∞	∞	∞
	4	∞	∞	∞	∞
Average(dB)		∞	∞	∞	∞

test that the best results were obtained, 3.51% was obtained, and in the worst result, 6.25% was obtained, which indicates that despite obtaining measurements efficient quantitative, qualitatively errors can be presented as was shown in the previous statements.

5.2. Comparison. From Table 11, different proposed steganographic algorithms are shown, which show different results with classical images in the image processing. **Carvajal et al. (2013)** [27] proposed the use of color complexity analysis (CLCES) accompanied by filters for the insertion of information with a **PSNR = 49.1956 dB**, with a similarity index of **0.9962** and the maximum **capacity** for the secret message is **4.3204 e03 Kb**. This paper shows the analysis of steganalysis through the IQM method with the best result of 1/9 images detected as a possible carrier of information.

Carvajal et al. (2014) [14] proposed an adaptation of the algorithm based on variance estimation (VFES), presenting

a result with **PSNR = 34.3736dB**, a similarity index of **0.9969**, and an insertion capacity of **165.336 Kb**. In this work we do not show results of attacks made on host images.

Sidhik et al. (2015) [15] proposed a steganographic algorithm based on the wavelet fusion technique which has a **PSNR = 37.45 dB**, does not show a similarity index, and shows an insertion capacity of **600x600 bits**. This work does not show results of attacks made to the host images.

Nazari S. et al. (2015) [16] proposed a steganographic algorithm which maps the cover image into a morphological representation in which they contain morphological coefficients and then insert the bits of the secret message applying permutation and a coding matrix. The results obtained in the work are for the **PSNR = 49.38dB**; it does not show the index of similarity and it obtains an insertion capacity of **4096 bits**. This work does not show results of attacks made to the host images.

TABLE 8: Standard deviation between the cover image and the stego-image.

Test	Round	Red color channel	Green color channel	Blue color channel	General
1	1	0.440569	0.502007	0.534010	0.492195
		0.440599	0.502032	0.534038	0.492223
	2	0.216114	0.245910	0.261501	0.241175
		0.215749	0.245643	0.261274	0.240888
	3	0.440569	0.502007	0.534010	0.492195
		0.440599	0.502032	0.534038	0.492223
	4	0.216114	0.245910	0.261501	0.241175
		0.215749	0.245643	0.261274	0.240888
2	1	0.584381	0.544214	0.475694	0.534763
		0.584401	0.544235	0.475715	0.534784
	2	0.286027	0.266488	0.233207	0.261907
		0.285871	0.266282	0.232901	0.261685
	3	0.584381	0.544214	0.475694	0.534763
		0.584401	0.544235	0.475715	0.534784
	4	0.286027	0.266488	0.233207	0.261907
		0.285871	0.266282	0.232901	0.261685
3	1	0.408481	0.514495	0.492052	0.471676
		0.408335	0.514345	0.491905	0.471528
	2	0.200647	0.252068	0.241177	0.231297
		0.200129	0.251762	0.240835	0.230909
	3	0.408481	0.514495	0.492052	0.471676
		0.408335	0.514345	0.491905	0.471528
	4	0.200647	0.252068	0.241177	0.231297
		0.200129	0.251762	0.240835	0.230909
4	1	0.613440	0.505246	0.371941	0.496876
		0.613467	0.505290	0.372000	0.496919
	2	0.300155	0.247529	0.182978	0.243554
		0.300049	0.247288	0.182452	0.243263
	3	0.613440	0.505246	0.371941	0.496876
		0.613467	0.505290	0.372000	0.496919
	4	0.300155	0.247529	0.182978	0.243554
		0.300049	0.247288	0.182452	0.243263
5	1	0.428864	0.453885	0.416717	0.433155
		0.428927	0.453945	0.416778	0.433217
	2	0.210543	0.222666	0.204646	0.212618
		0.210163	0.222337	0.204241	0.212247
	3	0.428864	0.453885	0.416717	0.433155
		0.428927	0.453945	0.416778	0.433217
	4	0.210543	0.222666	0.204646	0.212618
		0.210163	0.222337	0.204241	0.212247
6	1	0.055659	0.040007	0.028091	0.041252
		0.055694	0.040022	0.028069	0.041262
	2	0.041434	0.037299	0.035184	0.037973
		0.036975	0.032131	0.029434	0.032847
	3	0.055659	0.040007	0.028091	0.041252
		0.055694	0.040022	0.028069	0.041262
	4	0.041434	0.037299	0.035184	0.037973
		0.036975	0.032131	0.029434	0.032847
7	1	0.451941	0.240767	0.173620	0.288776
		0.451968	0.240803	0.173655	0.288808
	2	0.221483	0.120090	0.088852	0.143475
		0.221121	0.119017	0.087216	0.142451
	3	0.451941	0.240767	0.173620	0.288776
		0.451968	0.240803	0.173655	0.288808
	4	0.221483	0.120090	0.088852	0.143475
		0.221121	0.119017	0.087216	0.142451

TABLE 8: Continued.

Test	Round	Red color channel	Green color channel	Blue color channel	General
8	1	0.701288	0.382072	0.409695	0.497685
		0.701312	0.382164	0.409761	0.497746
	2	0.350049	0.191525	0.205166	0.248913
		0.350071	0.191120	0.204810	0.248667
	3	0.701288	0.382072	0.409695	0.497685
		0.701312	0.382164	0.409761	0.497745
	4	0.350049	0.191525	0.205166	0.248913
		0.350071	0.191120	0.204810	0.248667

FIGURE 3: Histograms per layer between the cover image and the stego-image.

FIGURE 4: Histograms per layer between the recovered image and the image to be hidden.

TABLE 9: Standard deviation between the recovered image and the image to be hidden.

Test	Round	Red color channel	Green color channel	Blue color channel	General
1	1	0.547939	0.542266	0.549022	0.546409
		0.547939	0.542266	0.549022	0.546409
	2	0.547939	0.542266	0.549022	0.546409
		0.547939	0.542266	0.549022	0.546409
	3	0.547939	0.542266	0.549022	0.546409
		0.547939	0.542266	0.549022	0.546409
	4	0.547939	0.542266	0.549022	0.546409
		0.547939	0.542266	0.549022	0.546409
2	1	0.509814	0.550694	0.583284	0.547931
		0.509814	0.550694	0.583284	0.547931
	2	0.509814	0.550694	0.583284	0.547931
		0.509814	0.550694	0.583284	0.547931
	3	0.509814	0.550694	0.583284	0.547931
		0.509897	0.550755	0.583348	0.548000
	4	0.509814	0.550694	0.583284	0.547931
		0.509897	0.550777	0.583348	0.548007
3	1	0.552109	0.502464	0.438230	0.497601
		0.552109	0.502464	0.437731	0.497435
	2	0.552109	0.502464	0.438230	0.497601
		0.552109	0.502464	0.437731	0.497435
	3	0.552109	0.502464	0.438230	0.497601
		0.552109	0.502464	0.438230	0.497601
	4	0.552109	0.502464	0.438230	0.497601
		0.552109	0.502464	0.438230	0.497601
4	1	0.540507	0.570493	0.590322	0.567107
		0.540507	0.570493	0.590322	0.567107
	2	0.540507	0.570493	0.590322	0.567107
		0.540507	0.570493	0.590322	0.567107
	3	0.540507	0.570493	0.590322	0.567107
		0.540507	0.570493	0.590322	0.567107
	4	0.540507	0.570493	0.590322	0.567107
		0.540507	0.570493	0.590322	0.567107
5	1	0.465200	0.468867	0.438334	0.457467
		0.465200	0.468867	0.438334	0.457467
	2	0.465200	0.468867	0.438334	0.457467
		0.465200	0.468867	0.438334	0.457467
	3	0.465200	0.468867	0.438334	0.457467
		0.465200	0.468867	0.438334	0.457467
	4	0.465200	0.468867	0.438334	0.457467
		0.465200	0.468867	0.438334	0.457467
6	1	0.480343	0.469753	0.445325	0.465140
		0.480482	0.470215	0.446338	0.465679
	2	0.480343	0.469753	0.445325	0.465140
		0.480636	0.470382	0.446843	0.465954
	3	0.480343	0.469753	0.445325	0.465140
		0.480516	0.469996	0.444935	0.465149
	4	0.480343	0.469753	0.445325	0.465140
		0.480516	0.470052	0.445401	0.465323
7	1	0.557072	0.524134	0.430416	0.503874
		0.557072	0.524134	0.430416	0.503874
	2	0.557072	0.524134	0.430416	0.503874
		0.557072	0.524134	0.430416	0.503874
	3	0.557072	0.524134	0.430416	0.503874
		0.557072	0.524134	0.430416	0.503874
	4	0.557072	0.524134	0.430416	0.503874
		0.557072	0.524134	0.430416	0.503874

TABLE 9: Continued.

Test	Round	Red color channel	Green color channel	Blue color channel	General
8	1	0.532984	0.499369	0.438593	0.490315
		0.532984	0.499369	0.438593	0.490315
	2	0.532984	0.499369	0.438593	0.490315
		0.532984	0.499369	0.438593	0.490315
	3	0.532984	0.499369	0.438593	0.490315
		0.532984	0.499369	0.438593	0.490315
	4	0.532984	0.499369	0.438593	0.490315
		0.532984	0.499369	0.438593	0.490315

FIGURE 5: Recovered images with visual distortions.

(a) PSNR = ∞ . RMSE = 0. NAE = 0. IF = 1. $r = 1$ (b) PSNR = ∞ . RMSE = 0. NAE = 0. IF = 1. $r = 1$ (c) PSNR = ∞ . RMSE = 1.4789. NAE = 0.0003. IF = 0.9953. $r = 0.9914$ (d) PSNR = ∞ . RMSE = 0. NAE = 0. IF = 1. $r = 1$ (e) PSNR = ∞ . RMSE = 0. NAE = 0. IF = 1. $r = 1$ (f) PSNR = 34.3408. RMSE = 4.8927. NAE = -0.0016. IF = 0.9790. $r = 0.9364$ (g) PSNR = ∞ . RMSE = 0. NAE = 0. IF = 1. $r = 1$ (h) PSNR = ∞ . RMSE = 0. NAE = 0. IF = 1. $r = 1$

FIGURE 6: Resulting recover images obtained. Efficiency of the proposed algorithm via image quality metrics for test images.

Gulve et al. (2015) [17] proposed a steganographic algorithm which makes a combination of spatial and frequency domain for the insertion of information. The results obtained in the work are for the **PSNR = 40.29 dB**, with similarity index of **0.800** and an insertion capacity of **650.608 bits**.

This work does not show results of attacks made to the host images.

Subhedar M. et al. (2016) [11] proposed a steganographic algorithm applying the redundant wavelet redundant transform (RDWT) and the QR factorization. The results obtained

FIGURE 7: Comparison between the obtained stego-image: (a), (c), (e), (g), (i), (k), (m), and (o) and the cover image: (b) (d), (f), (h), (j), (l), (n), and (p) in each test.

TABLE 10: Results of insertion test.

Test	Pixels Image to be hidden	Data insertion	% of cover image
1	712 x 534	572,448 bits	3.03%
2	712 x 534	572,448 bits	3.03%
3	1024 x 768	1'179,648 bits	6.25%
4	1024 x 768	1'179,648 bits	6.25%
5	1024 x 768	1'179,648 bits	6.25%
6	1024 x 768	1'179,648 bits	6.25%
7	576 x 768	663,552 bits	3.51%
8	256 x 256	98,304 bits	6.25%
Average			5.01%

in the work are for the **PSNR = 54.8019 dB**, with a similarity index of **0.9997** and an insertion capacity of **256x256 bits**. In this work, an analysis of attacks is carried out through various tests such as trimming, rotation, accentuation of edges, noise attacks, filtering, equalization, and compression. These techniques are not concentrated in a steganalyzer, such as IQM; however, the mentioned tests are contained in the

IQM metrics. The author presents resistance tests against attacks of **52% for attacks with the DWT** and **59% for attacks applying the contourlet**.

The algorithm proposed in this paper uses an adaptation of the nonlocal maximum likelihood filter in the wavelet domain as a filter detector of edges, reliefs, or abrupt changes within the host image, accompanied by the noise detector

FIGURE 8: Comparison between the original image to be hidden: (b), (d), (f), (h), (j), (l), (n), and (p) and the recovered image: (a), (c), (e), (g), (i), (k), (m), and (o) in each test.

threshold using the fourth moment wavelet, which is obtained from first-order statistics.

The information to be inserted is mapped in the submatrices obtained in the wavelet domain in such a way that the total recovery of the hidden information is guaranteed, together with the recovery criteria described in the work.

The main difference in this work lies in the adaptation of the nonlocal maximum likelihood filter in the wavelet domain and its noise detection sensitivity in the images, which allows selecting optimal zones for the insertion of information. By preserving the conditions of maximum adaptability to the medium, the PSNR visual quality measure is guaranteed, which indicates the power ratio of the image information against the noise power (everything that is not of the original image) of the image. In the present work, the ratio of information against noise PSNR is **56.1082 dB** for the Splash test image.

5.3. Steganalysis. The reverse process of hiding information is known as steganalysis. Steganalysis is a technique which allows the identification and detection of information that is

not coherent within the context in which the information is found.

In the application of steganalysis in digital images, advanced steganographic algorithms have now been developed, as well, making algorithms focused on the detection of information a complicated task, especially if current steganographic algorithms are focused on hiding information in noise.

Even when the images generated after the insertion of the information appear to be of good visual quality, so that the changes made are not identifiable at first sight, the insertion can affect the statistical behavior of the image, as well as its behavior in its different decompositions in frequency.

Steganographic algorithms can pass through different types of communication channels; and these communication channels can go through different types of surveillance that can be (i) passive, in which the communication channel is not a review of the information sent; (ii) active, in which the communication channel is continuously in review; and finally (iii) the passive-active mix in which the channel may or may not go through the monitoring of the channel.

TABLE II: Algorithm comparison.

Algorithm	Secret size	Cover image	RMSE	PSNR (dB)	R
Carvajal et al. 2013 [13]	2.1127Kb	Baboon	-----	49.1956	0.9998
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
Carvajal et al. 2014 [14]	165336Kb	Splash	-----	34.3736	0.9969
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
Sidhik S. et al. 2015 [15]	600x600	-----	-----	37.4587	0.9901
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
Nazari S. et al. 2015 [16]	2000 bits 5000 bits 10000 bits	Lena	-----	49.3800	-----
		Peppers	-----	47.7800	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
Gulve Avinash K. et al. 2015 [17]	81326 bits 82933 bits 81387 bits	Lena	-----	39.8400	-----
		Baboon	-----	39.6200	-----
		Peppers	-----	40.2900	-----
		-----	-----	-----	-----
		-----	-----	-----	-----
Subhedar M.S. et al. 2016 [11]	256 x 256 Gray Scale	Lena	0.9009	49.0369	0.9996
		Airplane	0.8780	49.2608	0.9997
		Peppers	0.7927	50.1480	0.9997
		Baboon	3.3218	37.7031	0.9966
		Splash	0.4639	54.8019	0.9996
Algoritmo propuesto	256 x 256 RGB	Lena	0.4602	54.9135	0.9998
		Airplane	0.4453	55.5070	0.9996
		Peppers	0.6811	51.5549	0.9990
		Baboon	1.2711	46.0482	0.9977
		Splash	0.4008	56.1082	0.9999

For this work, the analysis of the Image Quality Measures (IQM) is chosen, which consists of 10 tests that are based on the characteristics of the image, which are related through a function that must correlate well with the degree of satisfaction of an observer [12]. The objective of the quality measures have been used functions for the coding, evaluation, and prediction of performance of image quality algorithms, as well as loss of image information.

The 10 values obtained for the IQM are also classified depending on the type of possible attacks that can have the stego-images; these are listed below:

For an active surveillance in the stego-images, the following are used: M_1 = mean absolute error (MAE), M_2 = mean square error (MSE), M_3 = correlation measure Czekznowski, M_5 = image fidelity (IF), M_6 = cross correlation, M_7 = magnitude of the spectral distance, and M_{10} = standardized quadratic mean HVS error.

For a passive surveillance in stego-images, the following are used: M_4 = average angle, M_8 = average distance of the block in the spectral phase, M_9 = average distance of the block of spectral weight, and M_{10} = standardized quadratic mean HVS error.

For a mixed surveillance (active-passive) in the stego-images, the following are used: M_1 = mean absolute error (MAE), M_2 = mean square error (MSE), M_3 = correlation measure Czekznowski, M_7 = magnitude of the spectral distance, M_8 = average distance of the block in the spectral phase, M_9 = average distance of the block of spectral weight, and M_{10} = standardized quadratic mean HVS error.

For this work mixed surveillance was chosen, and the results obtained are shown in Table 12.

The results obtained from the IQM steganalysis tests are shown in Table 12. Of the 8 tests performed, 7 obtained 85.71% of message imperceptibility and 1 obtained 100% of imperceptibility.

The test that obtained a result in which it can be interpreted as noise added to the image is in the M_{10} test; this indicates the standardized squared error of the stego-image. The next test in which it can be interpreted as noise is in the M_7 test; it is in the alteration of the spectrum of the image. However, the results obtained may be negligible because the present values are small.

5.4. Discussion. In the presented work, a steganographic algorithm was proposed applying filtering techniques in multispectral images modifying the discrimination criteria of the nonlocal maximum likelihood filter models, applying the wavelet domain in obtaining the fourth moment; in this way it is possible to propose a detector to select in a more precise way the possible points of insertion of information within the host image.

The wavelet domain in the implementation of the steganographic algorithm collaborated in the decrease in the distortion of stego-image because each subimage obtained represents a level of frequency which highlights or diminishes the edges and/or edges of the image.

To evaluate the performance of the algorithm as well as the quality of the images obtained, correlation, MSE, and PSNR measurements are used, which reach values of 100% to infinity, which indicates that the difference between the original image and stego-image is not perceived quantitatively. The results obtained from the proposed steganographic algorithm still present in conditions of angle of view variability. The results obtained show that the adaptations of the filters, as well as the use of the fourth wavelet moment as a noise discriminant, allow the minimum distortion in the stego-image.

The proposed steganographic algorithm was also subjected to steganalysis tests to evaluate the resistance it had, to various factors such as image recovery capacity, similitude between stego-image and host image, invariance in time, frequency, changes phase, and fidelity of the image, showing results above 85%, which demonstrates the degree of reliability of information recovery, as well as imperceptibility of the information inserted.

6. Conclusions

The proposed algorithm adapts Nonlocal Maximum Likelihood Filters, in the wavelet domain using the fourth wavelet moment to obtain a discriminant with considerable levels

of noise detection in the host image, with the aim that the information inserted is the least perceptible possible both for the eyesight and for quantitative estimators of the quality of the image. From the results obtained using each of the aforementioned metrics (correlation, MSE, PSNR, and standard deviation) it was observed that in the case of the correlation between the cover image and the stego-image the result with the lowest performance is presented in test 6 round 3 with a correlation of 0.985136, while the best performance was obtained in test 7 both in round 1, as well as in round 3 with a correlation of 0.999895. On average, using the correlation metric between the cover image and the steganographic image, a value of 0.99687697 was obtained.

In the case of the correlation between the recovered image and the image to be hidden, the lowest performance obtained in the correlation metric between both images was obtained in test 6 round 3 with a value of 0.805666; on the other hand, the best performance obtained in the correlation that was obtained was in test 1 in all rounds, in test 2 rounds 1 and 2, test 3 rounds 3 and 4, test 4 all rounds, test 5 all rounds, test 7 all rounds, and test 8 all rounds with a value of 1. On average, the correlation between the recovered image and the image to be hidden, considering all the scenarios, gives a value of 0.98095813.

In the case of the MSE between the cover image and the stego-image, it can be seen in the results obtained that the minor performance in the MSE metric is presented in the 2 round 4 test with a value of 0.260410, and the highest performance for the MSE which is 8.276878 was in test 3 round 1. The average performance obtained in the MSE between the cover image and the steganographic image obtained a value of 2.60873384 taking into account all the scenarios of the tests performed.

Calculating the performance in the MSE metric between the recovered image and the image to be hidden, it is observed that the lowest performance obtained was obtained in test 1 in all rounds, test 2 in rounds 1 and 2, test 3 in rounds 3 and 4, test 4 in all rounds, test 5 in all rounds, test 7 in all rounds, and test 8 in all rounds with a performance obtained by the MSE of 0; on the other hand, the highest performance is present in round 6 test 3 with a performance in the MSE of 41.232236. The average performance obtained in this metric, taking into account all test scenarios, of the MSE between the recovered image and the image to be hidden has a value of 5.69734713.

In the case of the performance calculation for the PSNR between the cover image and the stego-image, it was observed that the highest value was obtained in round 2 test 4 with a performance in the PSNR of 53.974364 dB, while the lowest performance was of 38.952281 dB; this was obtained in round 3 test 1. The average value obtained in the case of PSNR, taking into consideration all the scenarios of the tests, was 46.3926254 dB.

The case of the calculation of the performance obtained in the PSNR between the recovered image and the image to be hidden was obtained where the highest performance of the PSNR tends to infinity; this value was presented in test 1 all rounds, test 2 rounds 1 and 2, test 3 in all rounds, test 4 in all rounds, test 5 in all rounds, test 7 in all rounds, and test

TABLE 12: Image quality measures results.

Cover Image	Image to be hidden	Test	Stego-image	Test	Result
boat	Agfa	M1=0.0	boat-Agfa	M1=0.0	No message
		M2=0.0		M2=0.0	No message
		M3=9.7656 e-4		M3=5.5443e-4	No message
		M7=0.0		M7=0.0	No message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0		M10=0.0	No message
100%					
sphinx	snow	M1=0.0561	sphinx-snow	M1=0.0416	No message
		M2=0.0763		M2=0.0446	No message
		M3=9.7689 e-4		M3=4.7118e-4	No message
		M7=6.2867e-11		M7=6.3748e-11	No message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0179		M10=0.1966	Message
1/7=85.71%					
prayer	skullcap	M1=0.0	prayer-skullcap	M1=0.0094	No message
		M2=0.0		M2=0.0156	No message
		M3=9.7656e-4		M3=2.0933 e-4	No message
		M7=0.0		M7=8.2075e-10	No message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0		M10=0.0171	Message
1/7=85.71%					
Mountain	landscape	M1=0.0	Mountain-landscape	M1=0.0091	No message
		M2=0.0		M2=0.0015	No message
		M3=9.8769e-4		M3=3.2700e-4	No message
		M7=0.0		M7=8.2127e-10	No message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0		M10=3.4568e-4	Message
1/7=85.71%					
Fire	Mosque	M1=0.0029	Fire-Mosque	M1=0.0036	No message
		M2=0.0067		M2=0.0058	No message
		M3=9.8769e-4		M3=2.7198e-4	No message
		M7=0.0		M7=1.7288e-4	Message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0		M10=0.0	No message
1/7=85.71%					
Wood fire	Cactus	M1=0.0	Wood fire-Cactus	M1=0.0004	No message
		M2=0.0		M2=0.0006	No message
		M3=8.9765e-4		M3=3.5126e-4	No message
		M7=0.0		M7=5.8662e-10	No message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0		M10=0.0018	Message
1/7=85.71%					
Lena	Mandrill	M1=0.0	Lena-Mandrill	M1=0.0029	No message
		M2=0.0		M2=0.0348	No message
		M3=8.9765e-4		M3=6.0930e-4	No message
		M7=0.0		M7=1.5928e-8	No message
		M8=0.0		M8=0.0	No message
		M9=0.0		M9=0.0	No message
		M10=0.0		M10=0.0053	Message
1/7=85.71%					

8 in all rounds; on the other hand, the lowest performance obtained was 32.245378 dB of PSNR; this was obtained in test 6 round 3. In this case, the average performance obtained for the PSNR, considering all the tests, yields a value that tends to infinity; this result is obtained from the fact that there is no difference between the power of the energy of the original image and the stego-image. In the same way, it is presented in the image to be hidden and in the recovered image.

In the case of the metric of the SD obtained from the cover image and the stego-image, the performance obtained in the highest difference detected between both images is obtained in the test 6 rounds 2 and 4 with a value of 0.005126, while the performance obtained with the smallest difference is in test 6 rounds 1 and 3 with a value of 0.000010. On average, the difference obtained between the SD of the cover image and the SD of the stego-image, taking into consideration all the test scenarios, yields a value of 0.00052246.

In the case of the performance calculation obtained in the SD between the image recovered and the image to be hidden, the highest difference detected which has a value of 0.000814 is obtained in test 6 round 2, while the performance obtained with the smallest difference detected was a value of 0 which was obtained in test 1 in all rounds, test 2 round 1 and 2, test 3 round 3 and 4, test 4 in all rounds, test 5 in all rounds, test 7 in all rounds, and test 8 in all rounds. On average, the difference between the SD of the recovered image and the image to be hidden shows a value of 0.00006318.

The algorithm proposed in this document was also subjected to tests of resistance to attacks based on the IQM measures, which showed a performance above 85%, thus demonstrating the reliability of the imperceptibility of the data, to possible guardians of active-type channels such as what are currently mobile communications. Likewise, an insertion capacity performance of 1,179,648 bits was obtained, occupying only 6.25% of the image, demonstrating that the three important factors of the steganographic algorithm were maintained: insertion capacity, stego-image quality, and message retrieval.

Data Availability

The images, data, and datasets generated and/or analyzed during the current study are not publicly available but are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Blanca E. Carvajal-Gómez presented the main idea, conceived the experiments, interpreted the results, and wrote the paper. Manuel A. Díaz-Casco carried out the simulation; he also contributed to the interpretation of the results. All authors read and approved the final manuscript for publication.

Acknowledgments

The authors express their gratitude to Instituto Politécnico Nacional (SIP-IPN 20180410) for the support during this work, in particular to the Secretaría de Ciencia, Tecnología e Innovación of CDMX (SECITI/072/206) for all the facilities granted.

References

- [1] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: a survey," *Computer Science Review*, vol. 13-14, pp. 95–113, 2014.
- [2] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.
- [3] M. Hussain, A. W. Wahab, Y. I. Idris, A. T. Ho, and K. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.
- [4] H.-D. Yuan, "Secret sharing with multi-cover adaptive steganography," *Information Sciences*, vol. 254, pp. 197–212, 2014.
- [5] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [6] S. Sajasi and A.-M. Eftekhari Moghadam, "An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method," *Applied Soft Computing*, vol. 30, pp. 375–389, 2015.
- [7] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215–224, 2010.
- [8] H. Zhang, X. Ping, M. Xu, and R. Wang, "Steganalysis by subtractive pixel adjacency matrix and dimensionality reduction," *Science China Information Sciences*, vol. 57, no. 4, pp. 1–7, 2014.
- [9] C. C. Chang, P. Tsai, and M. H. Lin, "An adaptive steganography for index-based images using codeword grouping?" in *Advances in Multimedia Information Processing—PCM 2004*, vol. 3333 of *Lecture Notes in Computer Science*, pp. 731–738, Springer, Berlin, Germany, 2004.
- [10] H. Hioki, "A data embedding method using bpcs principle with new complexity measures," in *Proceedings of Pacific Rim Workshop on Digital Steganography*, pp. 30–47, 2002.
- [11] M. S. Subhedar and V. H. Mankar, "Image steganography using redundant discrete wavelet transform and QR factorization," *Computers and Electrical Engineering*, vol. 54, pp. 406–422, 2016.
- [12] R. Vijayarajan and S. Muttan, "Discrete wavelet transform based principal component averaging fusion for medical images," *AEÜ - International Journal of Electronics and Communications*, vol. 69, no. 6, pp. 896–902, 2015.
- [13] E. C. Blanca, J. G. Francisco, J. R. Alberto, and L. L. Joseacute, "Adjust of energy with compactly supported orthogonal wavelet for steganographic algorithms using the scaling function," *International Journal of Physical Sciences*, vol. 8, no. 4, pp. 157–166, 2013.
- [14] B. E. Carvajal-Gamez, F. J. Gallegos-Funes, and A. J. Rosales-Silva, "Variance field estimation-based steganographic (VFES) method for RGB colour images," *Imaging Science Journal*, vol. 62, no. 8, pp. 449–452, 2014.

- [15] S. Sidhik, S. K. Sudheer, and V. P. Mahadhevan Pillai, "Performance and analysis of high capacity Steganography of color images involving Wavelet Transform," *Optik - International Journal for Light and Electron Optics*, vol. 126, no. 23, pp. 3755–3760, 2015.
- [16] S. Nazari, A.-M. Eftekhari-Moghadam, and M.-S. Moin, "A novel image steganography scheme based on morphological associative memory and permutation schema," *Security and Communication Networks*, vol. 8, no. 2, pp. 110–121, 2015.
- [17] A. K. Gulve and M. S. Joshi, "A high capacity secured image steganography method with five pixel pair differencing and lsb substitution," *International Journal of Image, Graphics and Signal Processing*, vol. 7, no. 5, pp. 66–74, 2015.
- [18] M. Zahangir Alam, M. Saifur Rahman, N. Parvin, and M. Abdus Sobhan, "Wavelet denoising spproach using fourth order moment to remove wireless random noise," in *Proceedings of the 2012 1st International Conference on Informatics, Electronics and Vision, ICIEV 2012*, pp. 1124–1129, Bangladesh, May 2012.
- [19] U. Aktas and R. Hippenstiel, "Localization of GSM signals based on fourth order moment wavelet denoising," pp. 457–461.
- [20] A. Khan, M. Waqas, M. R. Ali, A. Altalhi, S. Alshomrani, and S.-O. Shim, "Image de-noising using noise ratio estimation, K-means clustering and non-local means-based estimator," *Computers and Electrical Engineering*, vol. 54, pp. 370–381, 2016.
- [21] P. V. Sudeep, P. Palanisamy, J. Rajan et al., "Speckle reduction in medical ultrasound images using an unbiased non-local means method," *Biomedical Signal Processing and Control*, vol. 28, pp. 1–8, 2016.
- [22] J. Fridrich, D. Soukal, and M. Goljan, "Maximum likelihood estimation of length of secret message embedded using $\pm K$ steganography in spatial domain," in *Proceedings of SPIE-IS and T Electronic Imaging - Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, pp. 595–606, January 2005.
- [23] A. den Dekker and J. Sijbers, "Maximum likelihood estimation of signal amplitude and noise variance from complex valued data," *IFAC Proceedings Volumes*, vol. 36, no. 16, pp. 127–132, 2003.
- [24] P. Jain and V. Tyagi, "A survey of edge-preserving image denoising methods," *Information Systems Frontiers*, vol. 18, no. 1, pp. 159–170, 2016.
- [25] S. Aja-Fernandez, C. Alberola-Lopez, and C.-F. Westin, "Noise and signal estimation in magnitude MRI and Rician distributed images: a LMMSE approach," *IEEE Transactions on Image Processing*, vol. 17, no. 8, pp. 1383–1398, 2008.
- [26] J. Sijbers, D. Poot, A. J. Den Dekker, and W. Pintjens, "Automatic estimation of the noise variance from the histogram of a magnetic resonance image," *Physics in Medicine and Biology*, vol. 52, no. 5, article no. 009, pp. 1335–1348, 2007.
- [27] J. Sijbers and A. J. Den Dekker, "Maximum Likelihood Estimation of Signal Amplitude and Noise Variance from MR Data," *Magnetic Resonance in Medicine*, vol. 51, no. 3, pp. 586–594, 2004.
- [28] M. Bouhrara, J.-M. Bonny, B. G. Ashinsky, M. C. Maring, and R. G. Spencer, "Noise Estimation and Reduction in Magnetic Resonance Imaging Using a New Multispectral Nonlocal Maximum-likelihood Filter," *IEEE Transactions on Medical Imaging*, vol. 36, no. 1, pp. 181–193, 2017.
- [29] S. Tedmori and N. Al-Najdawi, "Image cryptographic algorithm based on the Haar wavelet transform," *Information Sciences*, vol. 269, pp. 21–34, 2014.
- [30] D. L. Donoho, "De-noising by soft-thresholding," *IEEE Transactions on Information Theory*, vol. 41, no. 3, pp. 613–627, 1995.
- [31] J. Walker, *A Primer on Wavelets and their Scientific Applications*, Chapman & Hall/CRC, 1999.