

Gray-scale Images within Color Images using Similarity Histogram-Based Selection and Replacement Algorithm

Dora M. Ballesteros L., Diego Renza and Ramiron Rincon

Telecommunications Engineering
Universidad Militar Nueva Granada
Carrera 11 101-80, Bogota-Colombia
dora.ballesteros@unimilitar.edu.co, diego.renza@unimilitar.edu.co, u1400932@unimilitar.edu.co

Received April, 2015; revised August, 2015

ABSTRACT. *In this paper, we propose a scheme to hide a gray-scale image within an RGB image based on two features: band selection of the cover image through the similarity between the secret image histogram and the histogram of each band, and a pixel searching process. Every pair of images (secret and cover) produces an adaptive key that contains the following data: secret image size and its average, selected band number (Red, Blue or Green) and the locations of the replaced data. To obtain a trade-off between imperceptibility (stego image) and quality (recovered secret image), we use a range in the pixel searching process. Several experiments were conducted with ten cover images, five secret images, and five ranges of the pixel selection process. It was found that the imperceptibility of the stego image is high enough to avoid arousing suspicions regarding the existence of the secret image. The findings also indicate that the recovered secret image correlates highly with the original secret image.*

Keywords: Image steganography, Gray-level modification technique, Pixel in Block hiding method.

1. **Introduction.** Nowadays the amount of digital data transmitted over the internet is very high, images being one of the most available data types. In some cases, these images are not sensitive content and private communication is not a requirement. Nevertheless, in other cases, confidentiality of the content plays an important role. In this regard, steganography is one way to protect the existence of the secret content. Most image steganography schemes are performed in spatial domain or in transform domain [1, 2]. In the case of spatial domain, the hiding process is directly performed over the image data, as seen in Least Significant Bit (LSB) substitution, gray-level modification, pixel value differencing and quantization index modulation techniques. In LSB substitution, some of the least significant bits of the pixel are replaced with the secret data [3, 4, 5, 6, 7, 8]. In gray-level modification, some pixels of the cover image are changed according to a mathematical function [9, 10]. Specifically, the Pixel in Block Hiding Method (BPHM) changes some pixels of one band of the color cover image with the pixels of the secret image [11]. In Pixel Value Differencing (PVD), the hiding process is performed by changing the difference between two or more adjacent pixels [12, 13, 14, 15, 16, 17, 18]. In Quantization Index Modulation (QIM) the cover image is quantized in some ranges and the value of the hidden bit is related to the value of the quantized pixel [19, 20, 21, 22]. Some of the

above techniques use the concept of histogram similarity, which can be applied to the entire image [23] or for a specific band of the color image.

In the case of transform domain, the data are embedded in spectral coefficients using a form of transformation such as the Discrete Cosine Transform (DCT) [24, 25] or the Discrete Wavelet Transform (DWT) [26, 27, 28]. These schemes can be applied in combination with one of the spatial domain techniques.

Regardless of the selected method, the following characteristics should be satisfied: imperceptibility, payload and quality of the recovered secret image. Imperceptibility means that the observer cannot detect any kind of distortion in the image that raises suspicions about the existence of the secret content. Payload is related to amount of hidden bits. Quality of the recovered secret image means that the recovered image is very similar to the original secret image and is even more so with reversible data hiding schemes [29, 30]. Some of the above schemes allow high imperceptibility but low quality of the recovered image or low payload, and other schemes only emphasize one of the desired characteristics. For example QIM-based schemes have low data hiding; high quality of the recovered secret image and imperceptibility depends on the step in the quantization process. Therefore, in this project we propose a scheme within the gray-level modification techniques based on the BPHM method, which has a good trade-off between imperceptibility, payload and quality of the recovered image. Several tests were carried out in order to select adequate conditions to strike a good balance between the three characteristics.

2. Background of the pixel in block hiding method. The method known as Pixel in Block Hiding Method (BPHM) was proposed by Moustafa and Badawy [11]. This technique is used to embed a gray-scale image into a color image. The procedure to hide data is defined, as follows:

1. Calculate the number of pixels of the secret image, S , according to the number of rows N_1 and the number of columns M_1 .
2. Select a cover image, C , with size $N_2 \times M_2$ that satisfies: $(N_2 \times M_2) \gg (N_1 \times M_1)$.
3. Separate the cover image into three bands: Red, Green and Blue.
4. Divide every band into L blocks, with $L = N_1 \times M_1$. Therefore, in total there are $3 \times N_1 \times M_1$ blocks.
5. Select the first pixel of the secret image and search for a similar value in every band of the i -th block. A similar value is defined as having a range of $\pm th$. When a match is found, the pixel of the band is replaced with the pixel of the secret message. If the i -th block is selected, this block is ignored in the following search processes.
6. Repeat the above step until all the pixels of the secret image are hidden. Every block hides only one pixel of the secret image.

An example is shown in Figure 1.

The secret key has the following data for every pixel of the secret image: block number, selected band number and place of the selected pixel. It means if there are L pixels to hide, the secret key has $3 \times L$ values.

3. Proposed method. This is composed of three modules: pre-processing, embedding and extraction. In the pre-processing procedure some of the values that are stored in the key are calculated. In the second module, the secret image is embedded using a replacement algorithm which ensures high imperceptibility. The feature in the extraction module is that the recovered secret image is very similar to the original one.

3.1. Pre-processing. Let S the secret image with 8-bit gray-level of size $N_1 \times M_1$ and C the cover image with 3×8 -bit level of size $N_2 \times M_2$. The steps of this module are:

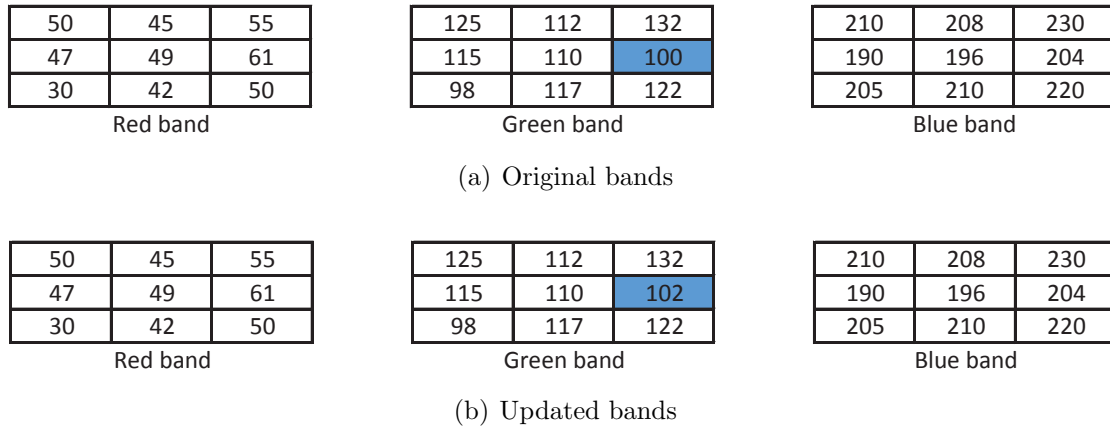


FIGURE 1. Example of the BPHM method with *Pixel of* $S = 102$ and $th = 3$.

1. Calculating the number of rows (N_1) and columns (M_1) of the secret image.
2. Calculating the number of rows (N_2) and columns (M_2) of the cover image.
3. Verifying that the cover image is high enough, which means that:

$$\frac{N_2 \times M_2}{N_1 \times M_1} \geq 10 \quad (1)$$

If the above condition is not satisfied, a new cover image must be selected.

4. Calculating the average of the secret image, as follows:

$$average = \frac{1}{(N_1 \times M_1)} \sum_{x=1}^{N_1} \sum_{y=1}^{M_1} S(x, y) \quad (2)$$

$S(x, y)$ represents a pixel located at coordinate (x, y) in the secret image.

5. Storing the heading of the key, the following data: number of rows of the secret image, number of columns of the secret image, average of the secret image.


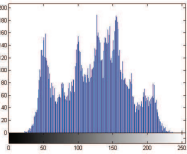

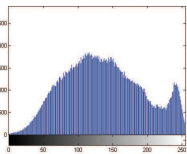


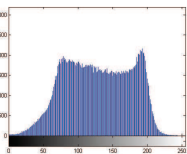

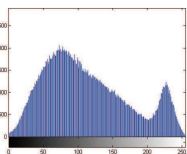
3.2. Embedding module. This consists of band separation and selection, pixel searching process and band composition.

3.2.1. Band separation. The purpose of this step is to separate the color image into three bands using the RGB model: R is the band of the Red component, G is the band of the Green component and B is the band of the Blue component. Each band has 8-bit gray-level precision.

3.2.2. Band selection. Four histograms are calculated to start with, being $H(R)$, $H(G)$, $H(B)$ and $H(S)$ the histogram of the Red-band, the Green-band, the Blue-band and the secret image respectively. Then, the similarity between $H(S)$ and the histogram of every band is calculated. We use the correlation coefficient parameter to evaluate their similarity. Therefore, three correlation coefficients are calculated, as follows: $corr(H(S), H(R))$, $corr(H(S), H(G))$ and $corr(H(S), H(B))$, being $corr(., .)$ the correlation coefficient between a pair of images. The highest value of $corr(., .)$, determines the selected band of the cover image.

Example 1. An example of band selection based on the concept of similarity of the histograms is illustrated (Table 1). The correlation coefficient is calculated for every pair of histograms. According to Table 1, the red band is selected because it has the largest correlation coefficient.

TABLE 1. Example of band separation and band selection process

Image	Gray-scale image	Histogram	Correlation coefficient
Secret image (S)			
Red (R)			$corr(H(S), H(R)) = 0.7479$
 Green (G)			$corr(H(S), H(G)) = 0.6719$
Blue (B)			$corr(H(S), H(B)) = 0.4805$

3.2.3. *Pixel searching process.* The secret image is hidden in one of the bands of the cover image. Once the band has been selected, the next step consists of selecting and replacing some pixels of the band. It is worth noting that both the secret image and the selected band are 8-bit, with similar histograms. This step is performed as follows:

1. The first pixel of the secret image is selected.
2. With the delta value (Δ), the search range is defined, as follows:

$$p_s - \Delta \leq p_{search} \leq p_s + \Delta \tag{3}$$

p_s as the pixel of the secret image and p_{search} as the pixel to be found in the selected band.

3. Within the selected band, the process is looking for a pixel that satisfies the value of p_{search} , through a zigzag displacement. If a pixel that matches with p_{search} is found, the selected pixel is changed with p_s value and the key is filled out with the place of the selected pixel (it uses the absolute position into the matrix). After the replacement process, the selected pixel is marked and remains unchanged.
4. If there is no pixel matching to p_{search} , the key is filled out with a zero value. In this case, the selected band is not updated.

Example 2. Suppose that we want to hide two pixels of the secret image. The first one is $p_s = 95$ and the second one is $p_s = 60$. In both cases, the value of delta is $\Delta = 5$. For the first pixel, $90 \leq p_{search} \leq 100$ is obtained.

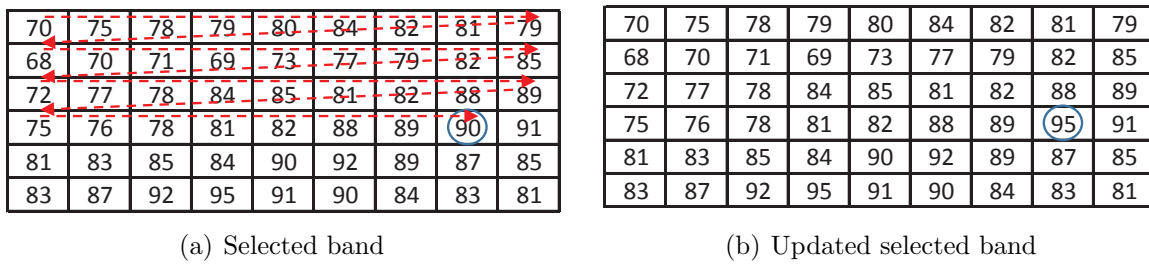


FIGURE 2. Example of pixel searching process.

Figure 2 shows the sweep in the searching process and the replacement data. The selected pixel is replaced with the value of p_s . The first value into the key is equal to the absolute place of the selected pixel in a zigzag displacement. In the current example, this value is 35. For the second pixel of the secret image, $55 \leq p_{search} \leq 65$ is obtained. For this range, a pixel satisfying the selected band of the search criterion is not found. Next, the value of the second place in the key is 0 and none of the pixels are replaced.

At the end, the key is comprised by the following data: secret image size, secret image average, number of the selected band and places of the selected pixels (Figure 3). In total, the key length is equal to $(N_1 \times M_1) + 4$.

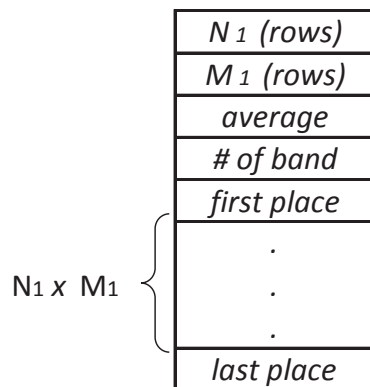


FIGURE 3. Data into the key.

3.2.4. *Band composition.* In the final step of the embedding module, the color image is reconstructed from the three bands; one of them has been updated in the pixel searching process. The output is known as the stego image.

3.3. **Extraction module.** This consists of band separation, band selection and pixel detection. Figure 4 shows the flowchart of this module.

Band separation: the input of this step is the stego image, which is a color image. Three color bands are obtained: the Red, Green and Blue components.

Band selection: with the number of band included in the key, the band which contains the secret image is selected.

Pixel detection: the aim of this step is to extract the pixels of the selected band corresponding with the pixels of the secret image. With the info of places in the key, the pixels of the secret image are extracted. The total number of extracted pixels is $(N_1 \times M_1)$. However, if a value of 0 is found in the key, it means that the pixel of the secret image has not been concealed. Then, it is necessary to fill out the value of the pixel with the

average value. Once the entire pixels have been extracted, they are arranged in a matrix with a size of $N_1 \times M_1$.

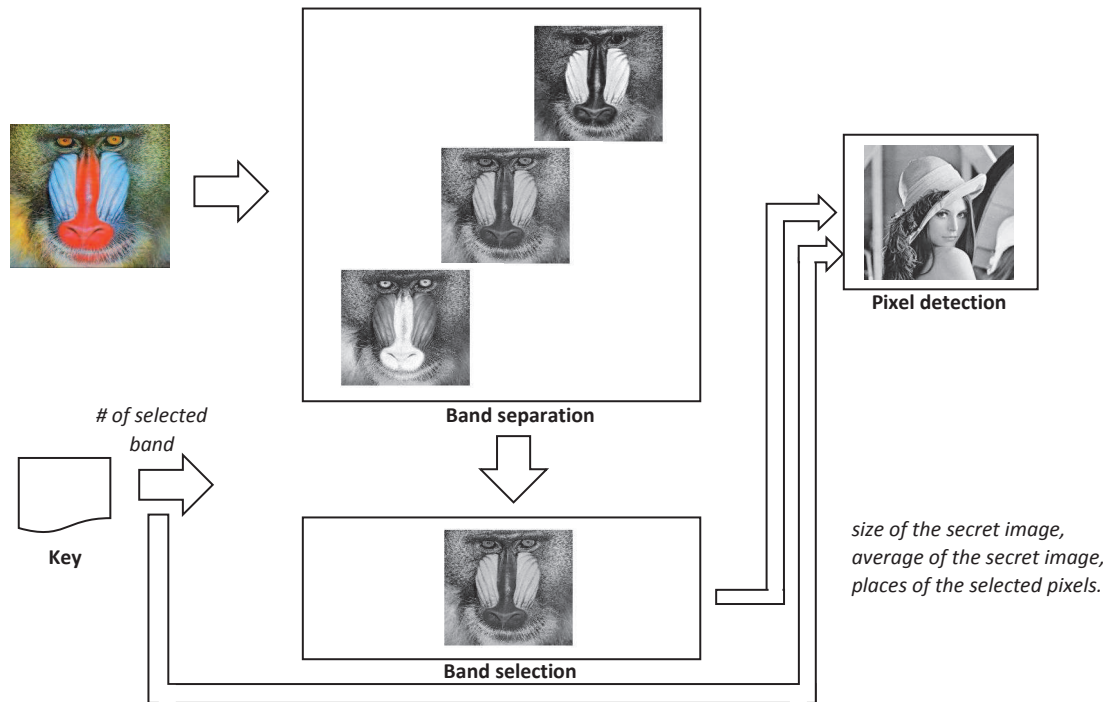


FIGURE 4. Flowchart of the extraction module.

4. Experimental results and analysis. The aim of this section is to validate the proposed scheme in terms of imperceptibility and quality of the recovered secret image. We analyze imperceptibility in two ways: similarity between the cover image and the stego image through the Normalized Correlation (NC) and the Gray Value Degree (GVD). The quality of the recovered secret image is measured through the NC between the original secret image and the recovered secret image. In terms of NC, the closer the value is to one, the higher the level of similarity. In terms of GVD, the closer the value is to zero, the lower the global distortion of the image.

To obtain the GVD, it is necessary to compute the gray value (GN) and the average neighborhood gray difference (AN), by means of the following equations:

$$GN(x, y) = \frac{\sum [I(x, y) - I(x', y')]^2}{4} \tag{4}$$

Where $I(x, y)$ is the pixel value at coordinate (x, y) and $I(x', y')$ is a neighboring pixel at the coordinates (x', y') . Figure 5 shows the four neighboring pixels of the central pixel $I(x, y)$.

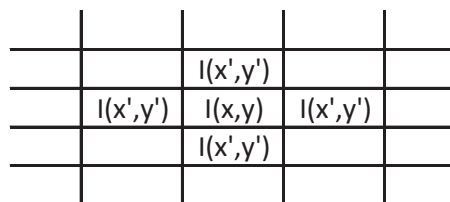


FIGURE 5. Central pixel $I(x, y)$ and its four neighboring pixels.

Since the central pixel needs four neighboring pixels, the pixels located at the border of the image are not taken into account as central pixels. The first central pixel is located at the coordinate $(2, 2)$ and the last central pixel at the coordinates $(N - 1, M - 1)$, where N is the total number of rows of the image and M is the total number of columns. Therefore, the amount of GN values into an image of size $N \times M$ is $(N - 2) \times (M - 2)$. Using all the results of GN , the average neighborhood gray difference (AN) is calculated as follows:

$$AN = \frac{\sum_{x=2}^{N-1} \sum_{y=2}^{M-1} GN(x, y)}{(N - 2) * (M - 2)} \tag{5}$$

Finally, the gray value degree is calculated as follows:

$$GVD = \frac{AN' - AN}{AN' + AN} \tag{6}$$

Where AN' and AN are the average neighborhood gray difference of the stego image and the cover image, respectively.

4.1. Preliminary results. In order to demonstrate the performance of the proposal, we present two examples with size ratio of 16. In the first one, we select the “Baboon” image with a size of $512 \times 512 \times 3$ as the cover image, and the “Lena” image with a size of 128×128 as the secret image. Figure 6 shows some of the results of this test, with $\Delta = 10$.

In this example, the similarity value between the stego and the cover image is 0.9993 and the similarity between the secret image and the recovered secret image is 1.0. On the other hand, the value of GVD between the stego and the cover image is 0.125×10^{-3} .

In the second example, the “Pepper” image with a size of $512 \times 512 \times 3$ hides the gray-scale image “blonde woman” with a size of 128×128 . Figure 7 shows the results of this case. The similarity value between the stego and the cover image is 0.9992 while it is 1.0 between the secret image and the recovered secret image. In this case, the value of GVD between the stego and the cover image is 2.8×10^{-3} .

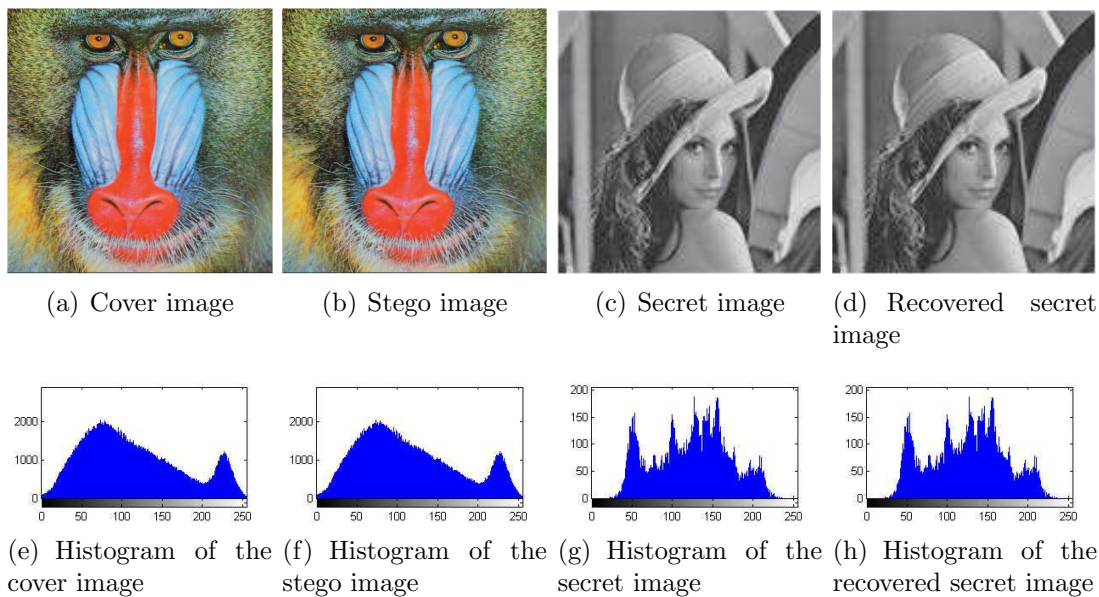


FIGURE 6. Preliminary results: Example No. 1.

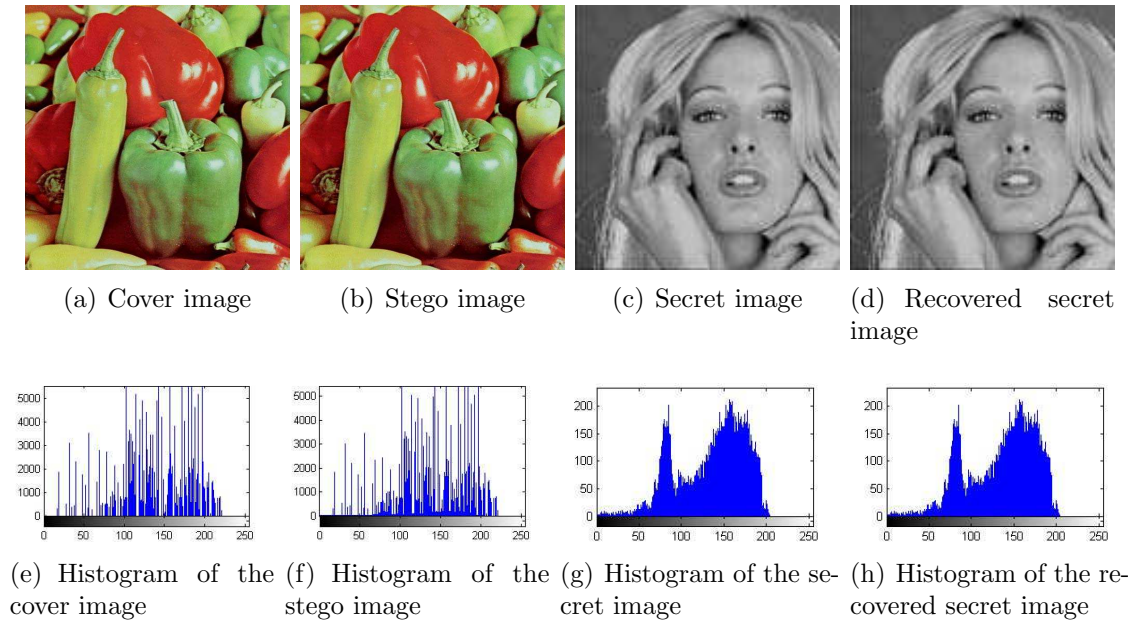


FIGURE 7. Preliminary results: Example No. 2.

According to the results, the distortion of the stego image is low enough to avoid arousing suspicions regarding the existence of the secret image and the quality of the recovered secret image is very high. In both cases, the time to obtain the stego image and the key is twenty seconds, and it took less than one second to recover the secret image (based on an Intel Core 3.1 GHz).

4.2. Summary results. For the entire test, we work with ten cover images, five secret images and five different delta values (i.e. 10, 15, 20, 25 and 30). Cover image sizes range between 472k and 539k pixels and secret image sizes range between 16k and 32k pixels. At the end, the total number of simulations was two hundred and fifty.

Figure 8 shows the results of the imperceptibility tests. These plots use confidence range (with 95% of the data), the minimum value and the highest value of the results. Every box represents the confidence range.

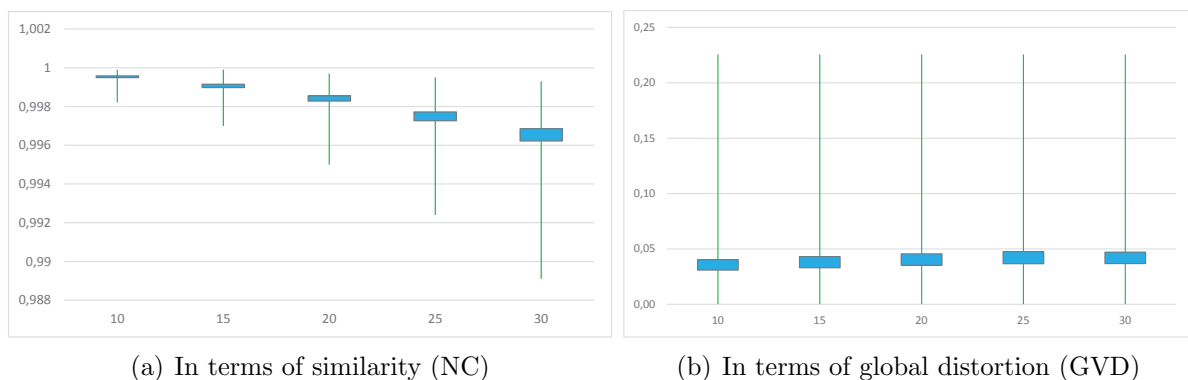


FIGURE 8. Summary imperceptibility tests.

According to the results of Figure 8, GVD is not sensitive to the delta value, but the NC is. However, the similarity between the stego and the cover image is slightly degraded with higher values of delta. In all cases, the values of NC and GVD are very good.

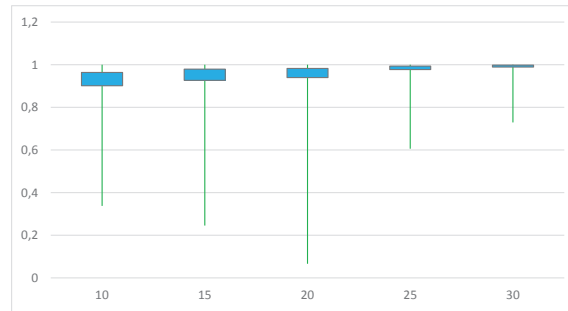


FIGURE 9. Summary quality tests: NC between the original and recovered secret image.

According to the results of Figure 9, delta plays an important role in the quality of the recovered secret image. The higher this value is, the higher the quality of the secret image. However, most cases (at least the 95%) had an NC higher than 0.9. With delta close to 30, the dispersion of the results is the lowest. It means that regardless of the selected cover image, a high quality of the recovered secret image is expected.

4.3. Comparison with the BPHM method. The purpose of this section is to highlight the differences between the BPHM method and the current proposal. The differences are summarized in Table 2.

TABLE 2. Comparison with the BPHM method

	BPHM	Our proposal
Selection of band	The selected band is not predefined. Every pixel of the secret image has its own selected band.	There is a selected band which is highly related to the secret image. The selection criterion is the similarity of the histograms.
Searching process	The cover image is divided into blocks. Every block hides only one pixel of the secret image.	It works with the entire cover image. There is no restriction of the hiding capacity by blocks of the cover image.
Replacement criterion	If a similar pixel of the secret image is found, the pixel of the band is updated with this pixel. However, if the match does not exist, there is no a replacement criterion.	If a similar pixel of the secret image is found, the pixel of the band is updated with this pixel. However, if the match does not exist, the recovered pixel is filled out with the average of the secret image.
Key	The number of the selected band, the number of the block and the place of the pixel are all kept in every pixel of the secret image. The length of the key is $3 \times N_1 \times M_1$.	Since the selected band is the same for all pixels of the secret image and we don't work with blocks, the length of the key is $(N_1 \times M_1) + 4$.

It is expected that the number of unhidden pixels in our proposal will be lower than that of the BPHM scheme because we do not work with the restriction of hiding capacity by block. On the other hand, the length of data in our proposal is significantly lower than that of the BPHM scheme.

5. Conclusion. In this paper a method for embedding a gray-scale image into a color image was presented. It uses two principles: selection of the adequate band to hide the secret image based on the similarity of their histograms, and the selection and replacement of adequate pixels of the selected band with the pixels of the secret image based on a searching range. This proposal has sufficient trade-off between the quality of the recovered image and the imperceptibility of the stego image. It was found that the higher the delta value, the higher the quality of the recovered secret image, but the lower the value of imperceptibility. However, the imperceptibility is less sensitive to the delta value, and therefore a good trade-off with delta equal to thirty was found. Since our proposal is not completely reversible, some pixel values of the secret image may be lost. To overcome this, we used a replacement algorithm that completes the empty pixels of the recovered secret image using its previously calculated average.

6. Acknowledgment. This work is supported by the “Universidad Militar Nueva Granada-Vicerrectoría de Investigaciones” under the grant INV-ING-1768 of 2015.

REFERENCES

- [1] M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” *Computer Science Review*, vol. 13, pp. 95–113, 2014.
- [2] 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.
- [3] 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.
- [4] T.-C. Lu, C.-Y. Tseng, and J.-H. Wu, “Dual imaging-based reversible hiding technique using lsb matching,” *Signal Processing*, vol. 108, pp. 77–89, 2015.
- [5] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, “Image hiding by optimal lsb substitution and genetic algorithm,” *Pattern recognition*, vol. 34, no. 3, pp. 671–683, 2001.
- [6] N. Akhtar, P. Johri, and S. Khan, “Enhancing the security and quality of lsb based image steganography,” in *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on*, pp. 385–390, IEEE, 2013.
- [7] J. Anquan, W. Sheng, and Z. Jie, “A new method for image information hiding based on image scrambling and lsb technology,” in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 4, 2010.
- [8] S. Masud Karim, M. S. Rahman, and M. I. Hossain, “A new approach for lsb based image steganography using secret key,” in *Computer and Information Technology (ICCIT), 2011 14th International Conference on*, pp. 286–291, IEEE, 2011.
- [9] M. A. Khan, V. Potdar, and E. Chang, “An architecture platform for grey level modification steganography system,” in *Industrial Electronics Society, 2004. IECON 2004. 30th Annual Conference of IEEE*, vol. 1, pp. 463–471, IEEE, 2004.
- [10] V. M. Potdar and E. Chang, “Grey level modification steganography for secret communication,” in *Industrial Informatics, 2004. INDIN’04. 2004 2nd IEEE International Conference on*, pp. 223–228, IEEE, 2004.
- [11] K. Moustafa and W. Badawy, “(color/gray) image in color cover hiding using modification of spatial domain hiding method,” in *Future Generation Communication and Networking (FGCN 2007)*, vol. 1, pp. 56–61, IEEE, 2007.
- [12] R. K. Singh, H. K. Verma, C. K. Singh, *et al.*, “Bi-directional pixel-value differencing approach for rgb color image,” in *Contemporary Computing (IC3), 2013 Sixth International Conference on*, pp. 47–52, IEEE, 2013.

- [13] K.-C. Chang, P. S. Huang, T.-M. Tu, and C.-P. Chang, "Adaptive image steganographic scheme based on tri-way pixel-value differencing," in *Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on*, pp. 1165–1170, IEEE, 2007.
- [14] J. Mandal and A. Khamrui, "A data-hiding scheme for digital image using pixel value differencing (dhpvd)," in *Electronic System Design (ISED), 2011 International Symposium on*, pp. 347–351, IEEE, 2011.
- [15] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and lsb replacement methods," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611–615, 2005.
- [16] Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, J. Su, and C.-P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing," *Information Sciences*, vol. 191, pp. 214–225, 2012.
- [17] N.-I. Wu, K.-C. Wu, and C.-M. Wang, "Exploring pixel-value differencing and base decomposition for low distortion data embedding," *Applied Soft Computing*, vol. 12, no. 2, pp. 942–960, 2012.
- [18] C.-H. Yang, C.-Y. Weng, H.-K. Tso, and S.-J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images," *Journal of Systems and Software*, vol. 84, no. 4, pp. 669–678, 2011.
- [19] A. Phadikar and S. P. Maity, "Data hiding based quality access control of digital images using adaptive qim and lifting," *Signal Processing: Image Communication*, vol. 26, no. 10, pp. 646–661, 2011.
- [20] H. Izadinia, F. Sadeghi, and M. Rahmati, "A new secure steganographic method based on predictive coding and quantization index modulation," in *Soft Computing and Pattern Recognition, 2009. SOCPAR'09. International Conference of*, pp. 234–238, IEEE, 2009.
- [21] H. Izadinia, F. Sadeghi, and M. Rahmati, "A new steganographic method using quantization index modulation," in *Computer and Automation Engineering, 2009. ICCAE'09. International Conference on*, pp. 181–185, IEEE, 2009.
- [22] H. Noda, M. Niimi, and E. Kawaguchi, "Application of qim with dead zone for histogram preserving jpeg steganography," in *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, vol. 2, pp. II–1082, IEEE, 2005.
- [23] P. Zhao, S. Li, L. Zhou, L. Li, and X. Guo, "Detecting affine-distorted duplicated regions in images by color histograms," *Information Hiding and Multimedia Signal Processing, Journal of*, vol. 6, no. 1, pp. 163–174, 2015.
- [24] A. Khamrui and J. Mandal, "A genetic algorithm based steganography using discrete cosine transformation (gasdct)," *Procedia Technology*, vol. 10, pp. 105–111, 2013.
- [25] H. Noda, M. Niimi, and E. Kawaguchi, "High-performance jpeg steganography using quantization index modulation in dct domain," *Pattern Recognition Letters*, vol. 27, no. 5, pp. 455–461, 2006.
- [26] K. Zhiweil, L. Jing, and H. Yigang, "Steganography based on wavelet transform and modulus function," *Systems Engineering and Electronics, Journal of*, vol. 18, no. 3, pp. 628–632, 2007.
- [27] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1898–1907, 2014.
- [28] Y.-H. Chen and H.-C. Huang, "Coevolutionary genetic watermarking for owner identification," *Neural Computing and Applications*, vol. 26, no. 2, pp. 291–298, 2014.
- [29] O. Marin and F. Y. Shih, "Reversible data hiding techniques using multiple scanning difference value histogram modification," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 3, pp. 451–460, 2014.
- [30] H.-C. Huang and W.-C. Fang, "Authenticity preservation with histogram-based reversible data hiding and quadtree concepts," *Sensors*, vol. 11, no. 10, pp. 9717–9731, 2011.