VISIÓN
ELECTRÓNICA

Covert communication of grayscale images within color images
Comunicación encubierta de imágenes a escala de grises en imágenes a color

Dora M. Ballesteros[1]
Diego Renza[2]
Ramiro Rincón[3]

Fecha de envío: 17 de julio de 2015
Fecha de recepción: 15 de septiembre de 2015
Fecha de aceptación: 18 de noviembre de 2015

Abstract: This manuscript shows a proposal of covert communication of grayscale images into color images. The main parameter taken into account in the design of the scheme is the transparency of the covert image; meaning that the covert image should be highly similar (perceptually and statistically) to the original color image. Several tests were conducted in order to measure both the transparency of the covert image and the quality of the recovered secret image (i.e. gray image).

Keywords: covert communication, color image, grayscale image, quality assessment, transparency

Resumen: En este documento se presenta un esquema de comunicación encubierta de imágenes en escala de grises ocultas en imágenes a color. El criterio principal en el diseño del esquema es la transparencia de la imagen encubierta, lo que significa que la imagen final (stego) es altamente similar a la imagen de color original, tanto a nivel visual como a nivel estadístico. Se realizan pruebas para medir la transparencia y la calidad de la imagen a escala de grises recuperada en el receptor.

Palabras clave: comunicación encubierta, imagen a color, imagen a escala de grises, medición de calidad, transparencia.

[1] BSc. In Electronic Engineering, Universidad Industrial de Santander, Colombia; MSc. in Electronic Engineering, Universidad de los Andes, Colombia; PhD. in Electronic Engineering, Universidad Politécnica de Cataluña, Spain. GISSIC research group. Current position: Professor Universidad Militar Nueva Granada, Colombia. E-mail: dora.ballesteros@unimilitar.edu.co

[2] BSc. In Electronic Engineering, Universidad SurColombiana, Colombia. MSc. in Telecommunications Engineering, Universidad Nacional de Colombia, Colombia. PhD. (c) in Advanced Computing for Science and Engineering, Universidad Politécnica de Madrid, Spain. GISSIC research group. Current position: Professor Universidad Militar Nueva Granada, Colombia. E-mail: diego.renza@unimilitar.edu.co

[3] BSc. In Telecommunications Engineering, Universidad Militar Nueva Granada, Colombia. Member of the GISSIC research group Universidad Militar Nueva Granada, Colombia.E-mail: u1400932@unimilitar.edu.co

Citar este artículo como: D. M. Ballesteros, D. Renza y R. Rincón,
"Covert communication of grayscale images within color images".
Visión Electrónica, algo más que un estado sólido.
Vol. 9, No. 2, julio-diciembre 2015, pp. 253-262.

1. Introduction

Because of the rapid increase of internet use, amount of digital information published in web sites or attached in emails has significantly increased. People use this media to transmit sensitive or not-sensitive information; sometimes data are posted in public sites, but in other cases, data is sent to a dedicated final user. In the last scenario, the transmitter (*Alice*) sends the intended recipient (*Bob*) sensitive data and she only wants him to be able to access the secret information. However, a non-authorized user (*Eva*) can intercept the secret information and then the privacy goal is not satisfied.

In order to preserve the privacy of information, there are two options: the first is the use of dedicated channels (i.e. secure channels) to pass data; the second is to conceal the secret information (i.e. sensitive data) before the transmission process. In this paper, we explore the second option.

Images are one of the most popular digital data and the amount of color images is high enough on the Internet. Therefore, if Alice wants to pass a (secret) grayscale image, she may select a color image as the host of the covert communication process.

Methods of concealing data into images are classified in two groups: spatial domain [1-4] and transform domain [5-7]. The latter could have a little advantage in terms of the transparency of the covert image; however, the former is less expensive computationally.

In the traditional approach, a grayscale image is hidden into another grayscale image. However, this condition has an important disadvantage, as hiding capacity is low. Since color images have three bands (e.g. Red, Green and Blue in the RGB model), the quantity of pixels available to hide the secret content (grayscale image) is three times greater than having a grayscale image as the host image. For example, in [8] the color image is transformed to the YC_hC_r space color and then the wavelet coefficients of the chrominance component are obtained. Then, the hiding process is carried out.

In this work, an adaptive search criterion is used. The aim is to select the best band (Red, Green or Red) to hide the secret grayscale image. Therefore, selected pixels depend on the histogram of both the secret image and the host image. It means that if one changes, it is expected that the selected pixels hide data change as well.

2. The proposed scheme

In this section, the proposed scheme is explained. Firstly, the embedding module will be shown, then the extraction module.

2.1 Proposed embedding module

The algorithm is shown in Figure 1. It has the following blocks: separation of the bands, search band criterion, pixel selection and band composition. The inputs of the module are the secret image and the host image; the outputs are the stego image and the key.

Separation of the bands: since the host image is represented in RGB format, three color-bands (Red, Green, Blue) are obtained.

Search band criterion: the aim is to select the band which is the most similar to the secret image. Once the band has been selected, the others are not changed.

Pixel selection: sequentially, every pixel of the secret image is compared with each pixel of the host image. When the first match is found (with a range criterion) the position of the pixel is marked. Then, the marked position is filled out with the pixel value of the secret image and the position is saved (key). If a pixel of the secret message is not matched with at least one pixel of the host image, then a value of zero is saved in the key. The outputs of this block are the modified selected band and the key. Key has the following information: size of the logo, name of the selected band, and the marked positions (i.e. positions of the host image that were changed with the value of the pixels of the secret image).

In order to illustrate this step, the following example is presented. Suppose that the secret image and the host image are as Figure 2.

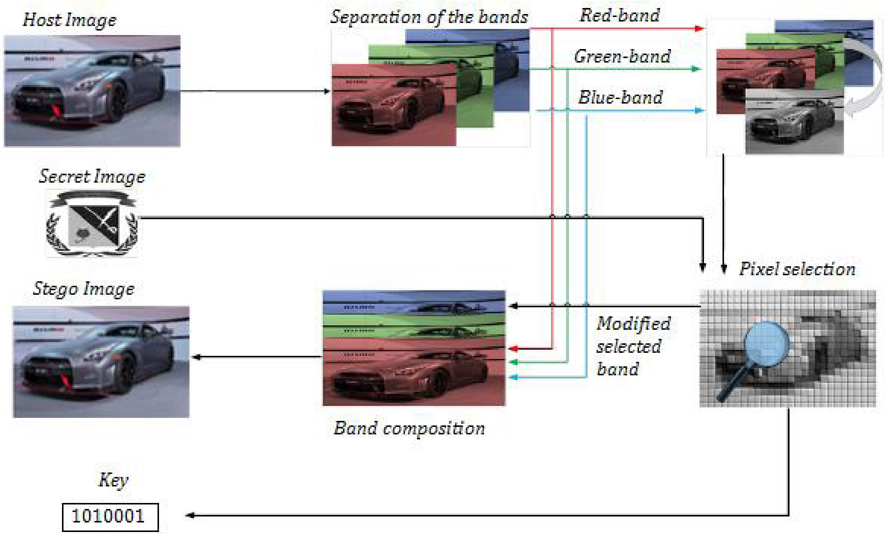


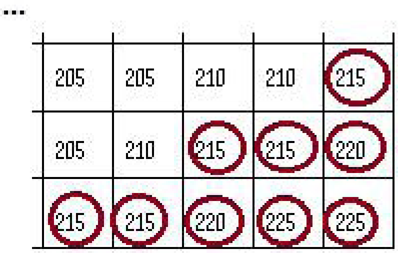
Figure 1. Flowchart of the embedding module. Source: own.

220	180	150
190	170	160
180	160	150

130	135	140	135	145	150	155	160	165
140	145	150	150	155	160	165	170	175
140	150	155	160	165	170	165	175	175
145	150	160	165	170	170	175	180	185
145	150	150	155	160	165	170	175	180
180	185	180	185	190	195	190	200	200
190	195	200	205	205	205	210	210	215
195	195	200	205	205	210	215	215	220
200	205	205	210	215	215	220	225	225

Figure 2. Example of secret image (left) and host image (right). Source: own.

The first pixel of the secret image is selected to be concealed. A delta must be defined, and suppose that for this case is +/- 5. Then, a search process is carried out looking for pixels of the host image with values between 215 and 225. Nine pixels are found (Figure 3).


...

205	205	210	210	215
205	210	215	215	220
215	215	220	225	225

Figure 3. Matched pixels for the first value of the secret image. Source: own.

Although there are nine available places to hide the pixel of the secret message, the first match is selected. In this case, the place of the seventh row and ninth column (i.e the key keep the value 63) is selected and then the new value is 220. The above procedure is carried out for every pixel of the secret image. At the end, if the histograms of the images (logo and host) are similar, there is a match between every pixel of the secret image with one pixel of the host image.

Band composition: once the pixel search has been finished, the next step consists of putting the three-bands together again. Two of them are unchanged, and the other (the selected plane) contains the secret data. The output of this step is the stego image. It has the same size of the host image, and it is expected that the level of similarity between them is high enough.

2.2 Proposed extraction module

The algorithm of this module is shown in Figure 4. It consists on separation of the bands and recovering.

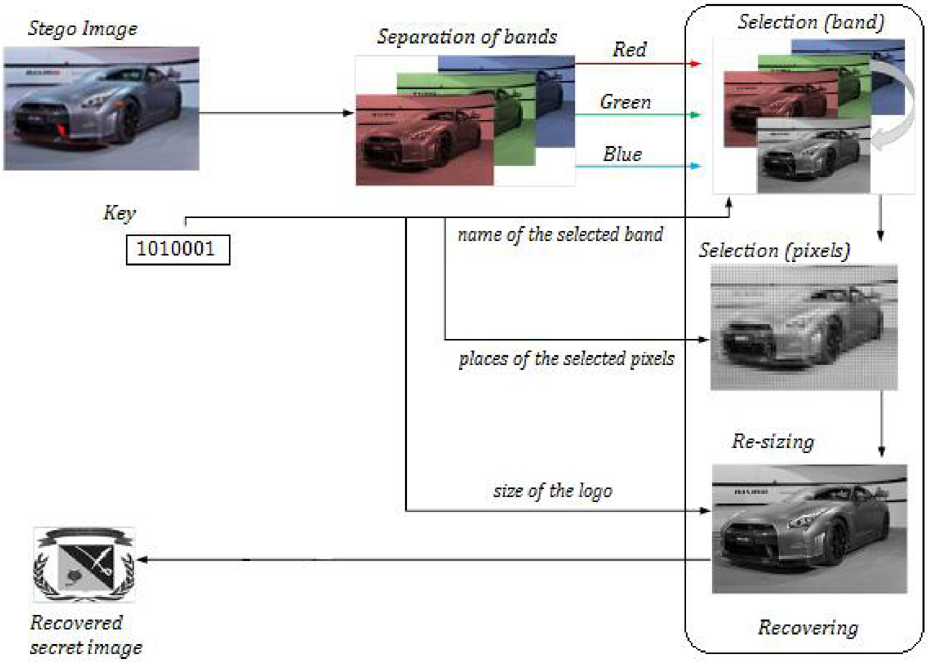


Figure 4. Flowchart of the embedding module. Source: own.

Separation of the bands: since the stego image is represented in RGB format, the three bands are extracted.

Recovering: in this step, the key data are used to select the band, the pixels of the stego image which have the logo, and the size of the recovered logo. Firstly, the band which contains secret data is selected. Secondly, pixels of the selected band with info of the logo are extracted. The output is a vector with the selected pixels. Finally, with the size of the original logo, the selected pixels are arranged in a matrix form. At the output of this step, the recovered secret image is obtained. In an ideal case, the recovered secret image is equal to the original secret image; nevertheless, if the histogram of the secret image is not highly similar to the histogram of the host image, the recovered secret image will be similar, but not equal to the original. The amount of missing pixels is equal to the total number of zero in the key. In this case, the pixel value is equal to the most probable pixel of the histogram.

3. Results

Several tests were carried out in order to illustrate the performance of the proposed scheme. The aim is to evaluate the host, stego, secret, and recovered images in terms of quality and transparency. Quality metrics are obtained by means of the comparison between secret and recovered images, whereas transparency is evaluated between the host and stego images. In both cases the selected metrics are: Mean Square Error (MSE), PSNR (Peak signal-to-noise ratio), and Normalized Correlation Coefficient (NC).

Mean Square Error (MSE): it is the parameter that allows evaluating the difference in the intensity levels of the original image (Xmn) regarding stego image (Ymn), as follows:

$$RMSE = \frac{1}{M * N} \sum_{m}^{M} \sum_{n}^{N} (X_{mn} - Y_{mn})^2 \quad (1)$$

With MxN as the dimension of the images. The ideal value of MSE is zero, meaning that there is no difference in intensity levels between the two images. The higher the quality, the lower the value of MSE.

While MSE measures the cumulative squared error, PSNR (Peak signal-to-noise ratio), represents a measure of the peak error; PSNR express the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. The index can be calculated as follows:

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

Where R is the maximum fluctuation in the input image data type (e.g. 255 in 8-bit unsigned integer data type). The higher the PSNR, the better the quality of the modified image and the transparency of the stego image.

Normalized Correlation Coefficient (NC) allows estimating structural differences between two images. It is defined by,

$$NC(X,Y) = \frac{\sum_{m} \sum_{n} \left[\left(X_{mn} - \overline{X} \right) \left(Y_{mn} - \overline{Y} \right) \right]}{\sqrt{\sum_{m,n} \left(X_{mn} - \overline{X} \right)^2 \sum_{m,n} \left(Y_{mn} - \overline{Y} \right)^2}} \quad (3)$$

Where X denotes the original image, Y the modified image, and MxN are the dimensions of the image. In evaluation, if the value of the NC is close to 1, it means that the quality is high enough.

3.1 Quality & Transparency

To evaluate the proposed method, a grayscale logo with a size of 128x128 pixels was selected (Figure 5) and twenty host images with several sizes were used. In every case, six values were estimated: MSE, PSNR and NC between the original logo and the recovered logo; MSE, PSNR and NC between the host image and the stego image.

Universidad Militar Nueva Granada
Scientia, Patria et Familia

Figure 5. Logo of the trials. Source: own.

Figure 6 shows the results in terms of MSE, PSNR and NC. According to the results, transparency of the stego image is high enough to not generate suspicion about the existence of the secret message. It is confirmed by the low value of the MSE (under 1.25), high value of the PSNR (over 45 dB) and very high NC (~1).

In the case of the quality of the recovered secret image, it was found that most of results (95% of confidence) have NC over 0.85. It means that the similarity between the original logo and the recovered logo is enough. In terms of MSE and PSNR, these results are better than in the transparency analysis.

3.2 Cases of study

In this section two cases will be shown: the best (Fig. 7) and the worst case (Fig. 8) of the twenty trials.

According to Figure 7, visual differences between the host image & the stego image and between the logo & the recovered logo are not noticeable to the naked eye. Looking at the histograms of the bands corresponding to these images, that similarity is corroborated.

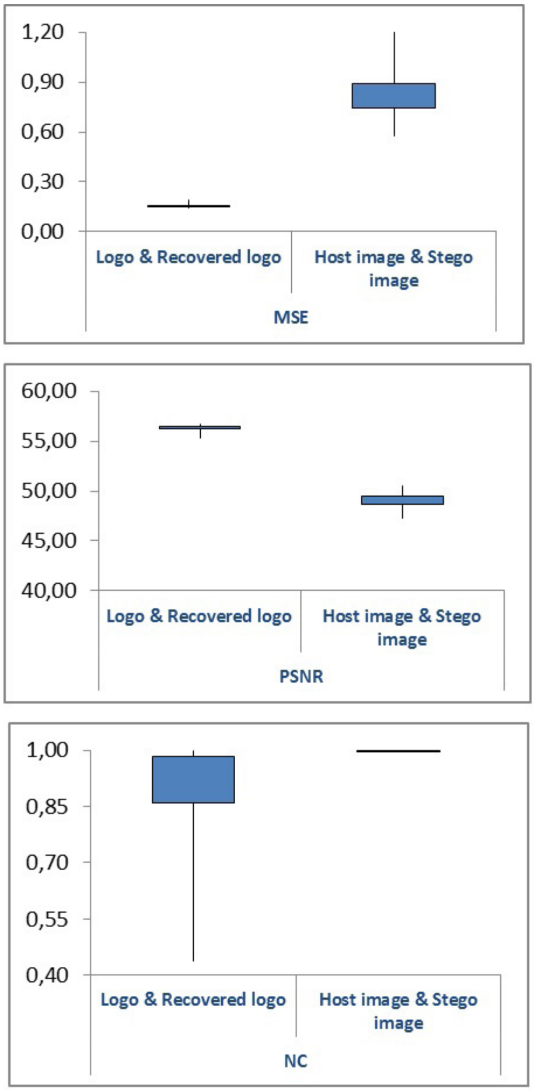
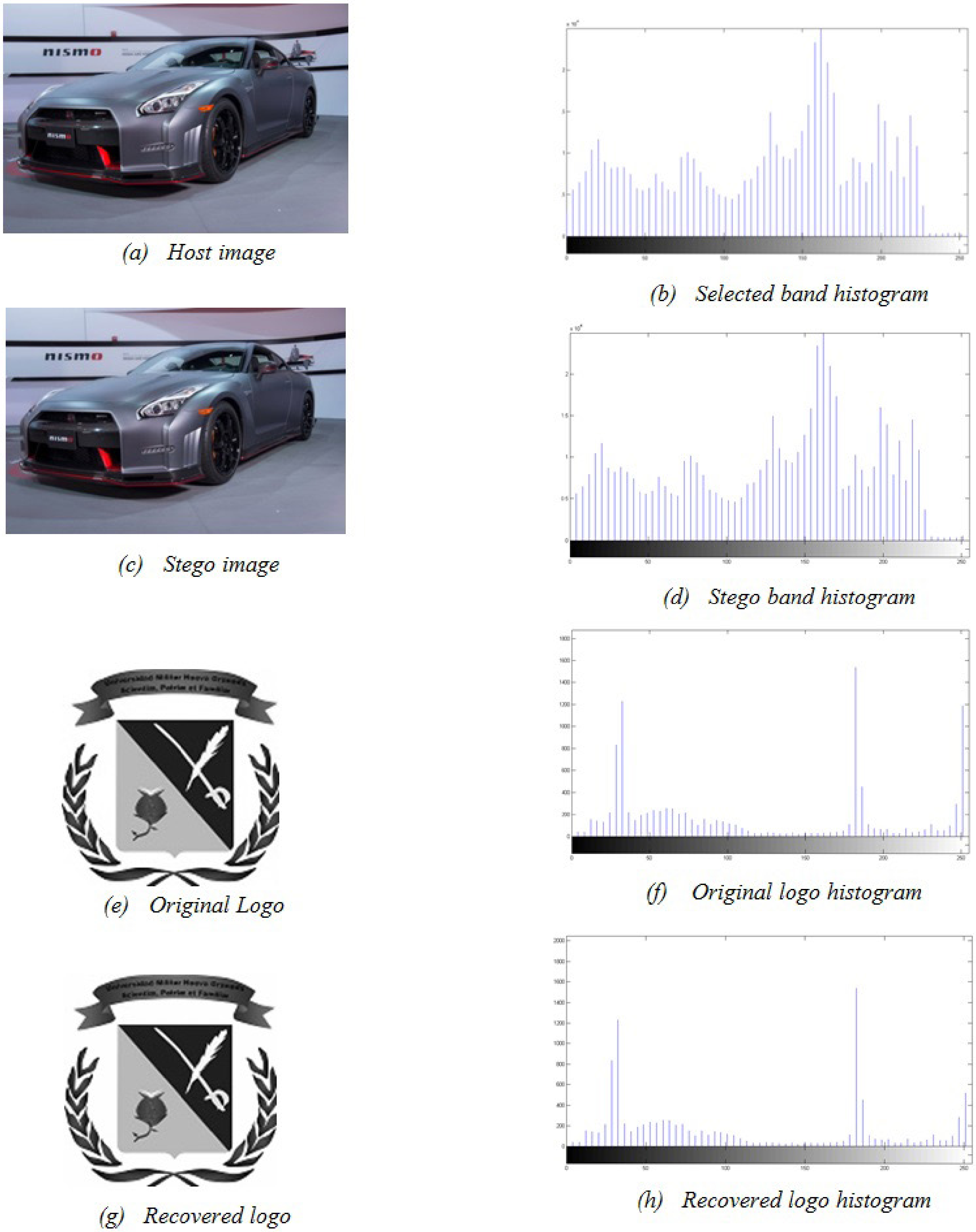


Figure 6. Logo of the trials (up to down): MSE, PSNR and NC. Source: own



(a) Host image

(b) Selected band histogram

(c) Stego image

(d) Stego band histogram

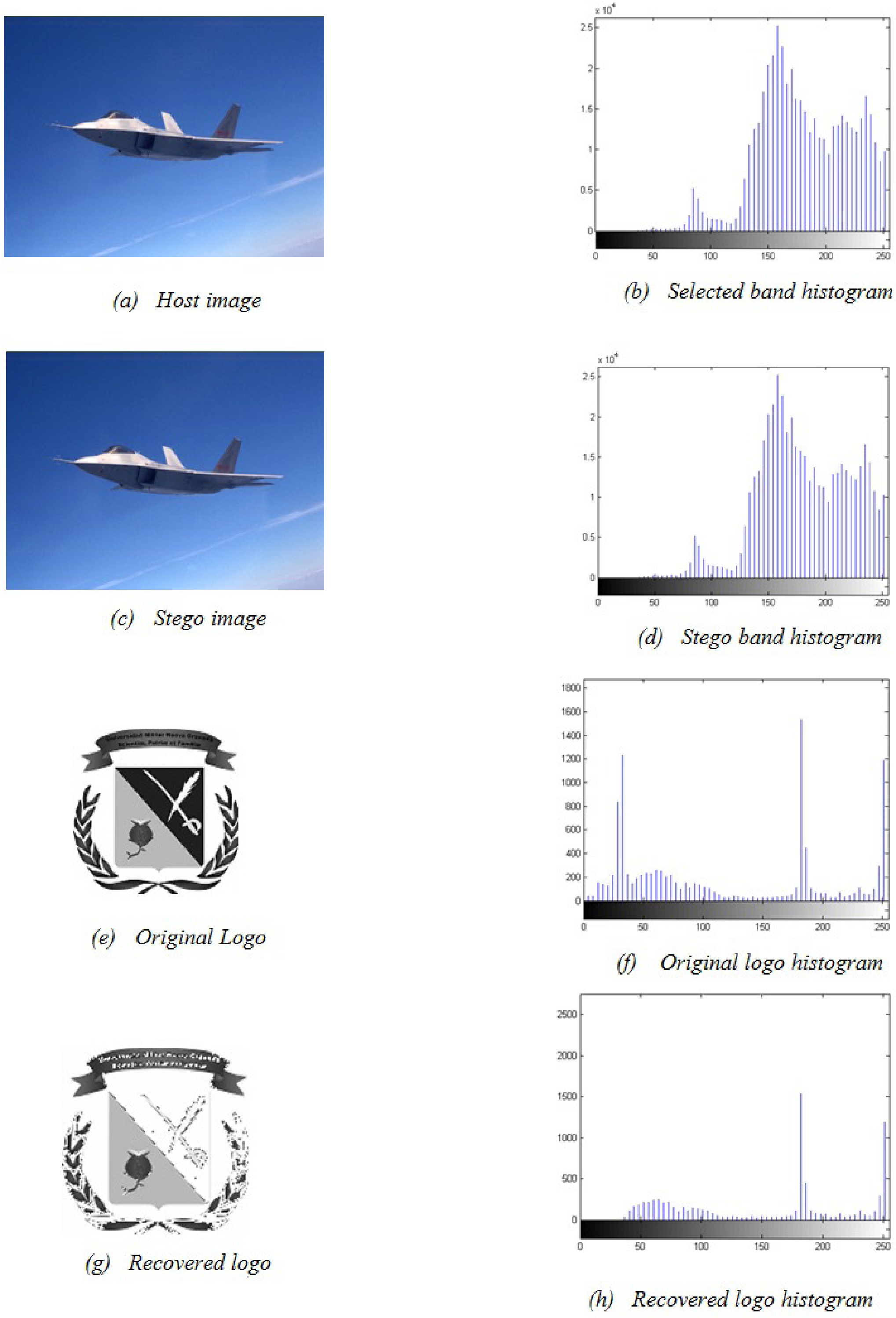
(e) Original Logo

(f) Original logo histogram

(g) Recovered logo

(h) Recovered logo histogram

Figure 7. Results for the best case. Source: own.



(a) Host image

(b) Selected band histogram

(c) Stego image

(d) Stego band histogram

(e) Original Logo

(f) Original logo histogram

(g) Recovered logo

(h) Recovered logo histogram

Figure 8. Results for the worst case. Source: own.

On the other hand, according to Figure 8, in the worst case, pixels of black levels are not hidden because the histogram of the host image does not have pixels of black levels.

4. Conclusions

Our proposal is a scheme of covert communication of grayscale images with high transparency which can be used in steganography systems. Transparency of the stego image is guaranteed as the first requirement of the concealment process; this is borne out by the low dispersion of the results of NC between the host image and the stego image.

An important characteristic of our proposal is that the key is not pre-defined by the user; it is created by the system and depends of the pair of selected images (host and logo). The key is not fixed; it is due to iterative search criteria.

On the other hand, quality of the recovered logo depends on the similarity between the histogram of the host image and the histogram of the logo but not the total number of pixels of the images (i.e the size). The higher the similarity between them, the higher is the quality of the recovered logo. It is desirable that the dynamic range of the histograms be very close.

As future work, the algorithm will be improved, looking for a higher transparency, an increase in the matching speed, and a method of compensation by the unmatched pixels in the host image.

Acknowledgment

This work is supported by the Universidad Militar Nueva Granada under the grant INV-ING-1768 of 2015.

References

[1] 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, DOI: http://dx.doi.org/10.1016/j.patcog. 2003.08.007.

[2] H. R. Kanan and B. Nazeri, “A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm,” Expert Systems with Applications, Vol. 41, no. 14, pp. 6123-6130, 2014; DOI: http://dx.doi.org/10.1016/j.eswa.2014.04.022.

[3] X. Liao, et al., “A steganographic method for digital images with four-pixel differencing and modified LSB substitution,” Journal of Visual Communication and Image Representation, Vol. 22, no. 1, pp. 1-8, 2011; [online] Available: DOI: http://dx.doi.org/10.1016/j.jvcir.2010.08.007.

[4] R. Z. Wang, et al., “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognition, Vol. 34, no. 3, pp. 671-683, 2001; DOI: http://dx.doi.org/10.1016/S0031-3203(00)00015-7.

[5] C. Agarwal, et al., “Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm,” Expert Systems with Applications, DOI: http://dx.doi.org/10.1016/j.eswa.2014.06.011.

[6] M. R. Keyvanpour and F. Merrikh-Bayat, “Robust dynamic block-based image watermarking in DWT domain,” Procedia Computer Science, Vol. 3, no. 0, pp. 671-683, 2011; DOI: http://dx.doi.org/10.1016/j.procs.2010.12.040.

[7] S. H. Lee, “DWT based coding DNA watermarking for DNA copyright protection,” Information Sciences, Vol. 273, no. 0, pp. 263-286, 2014; DOI: http://dx.doi.org/10.1016/j.ins.2014.03.039.

[8] L. Tong and Z. D. Qiu, “A DWT-based color image steganography scheme,” Proc. Signal Processing, 2002 6th International Conference on, Vol.1562, pp. 1568-1571, 2002.