Periodicals of Engineering and Natural Sciences
Vol. 9, No. 3, August 2021, pp.615-624

ISSN 2303-4521
Methodology/Method

Pixel steganography method for grayscale image steganography on colour images

Hadi Hussein Madhi[1], Mustafa Sahib Shareef [2], Seham Ahmed Hashem[3], Abdallah Waleed Ali [4]

[1] College of Nursing, Misan University, Iraq
[2] Al Muthanna University, Al-Muthanna, Iraq
[3] Technical Electronic Department, Technical Instructors Training Institute, Middle Technical University, Baghdad, Iraq
[4] Medical Instrumentation Engineering Department, Al-Esraa University College, Baghdad, Iraq

ABSTRACT

The process of hiding secret data within a host signal is known as steganography; its design parameters are imperceptibility, concealment capacity, and recovered data quality. A case of images, one of the existing methods based on modification of the host image pixels is called Block Pixel Hiding Method (*BPHM*), which has good imperceptibility and high-capacity concealment but does not guarantee the quality of the secret image recovered. This article proposes a method that improves results *BPHM* based on band selection and search algorithm global called Improved Pixel Hiding Method (*IPHM*). According to the simulations carried out, the results obtained with *IPHM* are better than those obtained with *BPHM*. They are similar to one of the more popular methods in imaging steganography known as Quantization Index Modulation (*QIM*). Steganography is the method of hiding hidden data within a host signal, with imperceptibility, concealment capacity, and retrieved data quality as design criteria. In the case of images, Block Pixel Hiding Method (*BPHM*) is one of the available methods based on modifying the host picture pixels, which has good imperceptibility and high-capacity concealment but does not guarantee the quality of the hidden picture recovered. Improved Pixel Hiding Method is a method proposed in this article that improves *BPHM* outcomes by using band selection and a global search algorithm (*IPHM*). The results obtained using *IPHM* are better than those achieved with *BPHM*, according to simulations. They're related to Quantization Index Modulation, which is one of the most widely used picture steganography techniques (*QIM*).

Keywords: Steganography, Block Pixel Hiding Method, Improved Pixel Hiding, Picture Steganography Techniques

Corresponding Author:

Hadi Hussein Madhi
College of Nursing, Misan University, Iraq
E-mail: Hadihm8@uomisan.edu.iq

1. Introduction

Transmit information securely through any channel always it has been a necessity in communications. In many cases, when public channels are used, an intruder can intercept the information transmitted, accessing sensitive content or manipulating the information. An alternative to this problem is data hiding (data hiding), to hide sensitive or secret information (steganography) or embed a trademark for copyright protection (watermarking). Although steganography is an ancient technique, Digital steganography has had a great boom with applications in new scenarios such as digital media[1-3], computer networks, and telecommunications services. Regardless of the steganographic method used, three conditions must be guaranteed, in their order: high imperceptibility seen as the non-generation of suspicion of the existence of the secret message hidden, adequate concealment capacity to embed the information secret, and high quality of the recovered information in terms of similarity to the original secret information. In the case of watermarking, the imperceptibility is not the main condition and robustness takes its place, seen as resistance to passive attacks intended to eliminate or impair the embedded mark to prevent the author from proving that he is the owner of the protected information [3]. In both cases, steganography and watermarking, multimedia signals such as audio, text, video[4-7], or image can act as hosts for secret information. When this procedure is done with images, the secret information is inserted within the host image, resulting in a new picture known as a stego image.

The stego image can be obtained from different methods, classified into two large groups: methods in the domain spatial and transform-based methods. The first group covers methods that directly modify pixel values in the host image based on the secret image's pixel values. The second group includes methods that use transformed to conceal the information in the frequency domain or space-frequency[3, 8-12]. Among the most common methods in the domain of space are highlighted the following:

- *LSB (Least Significant Bit)* method. Replace some of the bits less significant of a host image pixel with bits coming from of the secret image. The number of bits to modify in the host image depends on imperceptibility and concealment capacity desired. The higher the number of modified bits, the smaller the imperceptibility, but more significant the concealment capacity. Conventionally, *LSB*-based schemes are reversible. It is said that the recovered image is the same as the secret image original[2, 13, 14].
- *BPHM method (Block Pixel Hiding Method).* Split the host image into *N* square blocks of equal size, where *N* is similar to the secret image's total number of pixels. A sweep is performed in each of the guest image blocks (from left to right and from top to bottom) until a matching, or similar pixel is found with the secret image's pixel value to hide, which replaces the pixel, respectively. The process continues until all pixels are reached in the secret image (and therefore the totality of blocks in the host image). The result of this substitution process generates the stego image and a key that records the positions of the pixels where the information was hidden[15-17].
- *QIM method (Quantization Index Modulation).* This method is based on a quantization process to hide binary information (0/1). Each pixel in the host image can hide one bit of the image secret. The pixels in the host image are quantized according to to a quantization rule and to a pre-defined step value (). A quantization rule is used to hide a '0' and another to hide a '1'. In general, the quantized pixels will belong to data set *[0;Δ ; 2Δ; ...nΔ]* wؤhen a '0' is hidden and when set *[Δ/ 2; 3 Δ/2; .... nΔ / 2]* when a '1' is hidden. The method *QIM* generates better results in terms of image quality recovered with respect to the *BPHM* method and better imperceptibility of the stego image in relation to the *LSB* and *BPHM* methods; without However, the maximum concealment capacity may be less [2, 9, 10, 13-18].

On the other hand, among the transform-based methods, the most common are:

- *DCT (Discrete Cosine Transform).* In this case the carrier image is separated into sub-bands with respect to their frequency components (high, medium and low frequency) obtaining the *DCT* coefficients. The coefficients whose value does not exceed a given threshold, determine the susceptible locations for the insertion of the secret information [12, 19-22].
- *DWT (Discrete Wavelet Transform). DWT* is applied to the image host, obtaining four sub-images or sub-bands, corresponding to the approximation, horizontal, vertical and diagonal details of the original image. Of these four sub-bands, the one with the lowest frequency (approximation) is the most like the original image, while the high frequency sub-bands (detail) only relate information edges, textures, among others. For this reason, typically the data secrets are embedded in the host image detail coefficients to generate the least possible distortion in the stego image[23].

Other alternatives include spread spectrum techniques, methods statistical or adaptive steganography. Although transform-based methods may have greater imperceptibility than the methods in the spatial domain, the computational cost of the former is greater than that of the latter, both for the stage concealment, as for the recovery stage. In this context, proposes an improvement to a method in the spatial domain, specifically to the *BPHM* method, with the aim of increasing the imperceptibility of the stego image and the quality of the recovered secret image, without deteriorating the maximum concealment capacity of the original method. Expected with the proposed improvement, achieve results similar to those obtained with the *QIM* method in terms of imperceptibility and quality, and improve the maximum *QIM* concealment capacity.

2. Proposed method

The proposed method is based on the BPHM method, which will be called de hereinafter referred to as IPHM (Improved Pixel Hiding Method). As well is part of the methods in the spatial domain based on the modification pixel of the guest image. The main differences between the method proposed, IPHM, and the original method, *BPHM*, are: the image data

secret are hidden in a single band which is selected according to the similarity between the color band of the host image and the secret image; the pixel search process is not carried out by blocks but in the entire selected band; there is no concealment capacity restriction

areas of the host image, that is, the modification of pixels within the selected band; a replacement criterion is added in case of not finding a pixel in the selected band that is like the pixel of the secret image.

The stealth and retrieval modules are explained below.

2.1. Concealment module

The objective of this module is to insert a secret image in scale of gray within a color host image, obtaining a stego image, which should be as similar as possible to the original host image. The inputs to the module are a colour guest image of $N_1 \times M_1 \times 3$ and asecret grayscale image of $N_2 \times M_2$. The steps of the module are (see Figure 1):

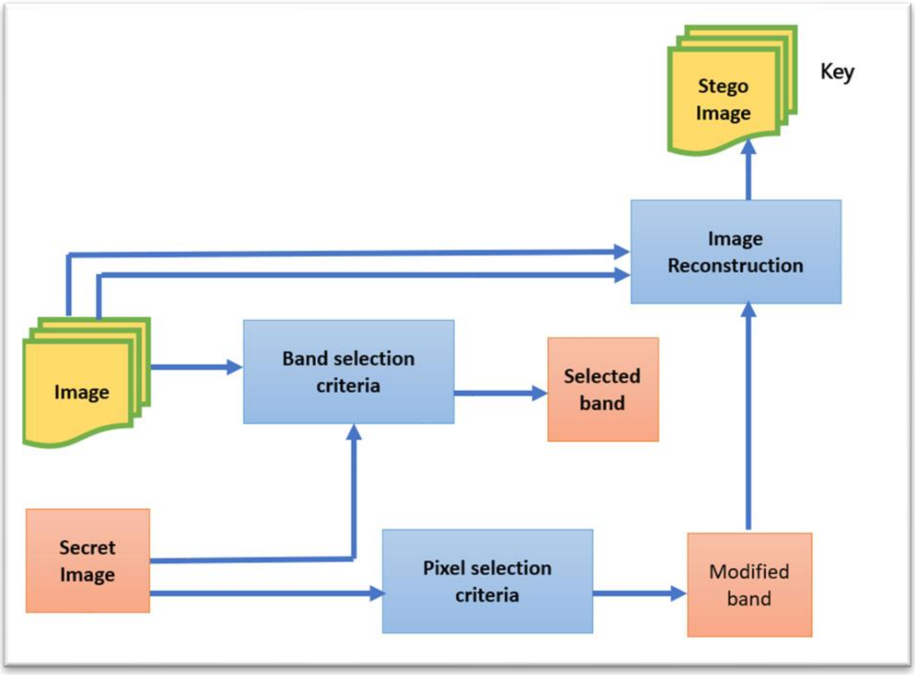


Figure 1. Concealment module

a) The key is initialized with three pieces of information: the total of the rows of the secret image, the total columns of the secret image and the average value of the pixels of the secret image.
b) Separate the three color bands of the host image and select the most suitable band for inserting secret data. The selection is based on the correlation criterion between the image histogram secret and the histogram of each of the bands of the host image. The histogram of the band with the highest degree of correlation (similarity) with the histogram of the secret image, will determine the band selected.
c) The number of the selected band is included in the fourth position of the code in the previous step, like this: 1 if the band is red, 2 if it is green and 3 if it is blue.
d) The search process for a pixel of the selected band is carried out of the host image that is like the secret image pixel a hide. The criterion of similarity implies that they should not necessarily the two pixels are equal, but a certain margin of error is tolerated. This margin of error is known as the range, so that the value of the pixel being searched is between the pixel value of the secret image the range value.
e) When the pixel that satisfies the search criteria is found, the replaced by the pixel value of the secret image and saved in the Key in the absolute position of the modified pixel. For example, if you have a

host image of 100 rows 80 columns and the modified pixel is find in the second row, seventh column, the absolute position of the pixel making a zigzag sweep from left to right and up bottom is 87 (80 positions of the first row plus 7 positions of the second row). To modifying the pixel only once selected from the host image, this pixel is locked and skipped for future searches.

f) If no pixels in the host image meet the search criteria, then the value of 0 is saved in the key. In the extraction module It will explain what value is substituted in the recovered image when the key has a 0.

g) Steps d-f are repeated for each pixel in the secret image. At the end of the search process, there is a band of the image host that presents modifications in some of its pixels and two gangs that did not undergo changes in the information concealment process. The total positions of the key are equal to the total data of complementary information (4 values corresponding to N_2, M_2, average, selected band) plus the total pixels of the secret image $(N_2\times M_2)$.

h) With the band modified and the remaining two unmodified, it is reconstructed.

The color image which corresponds to the stego image. This picture together with the password it is transmitted by two independent channels to the user authorized.

2.2. Recovery module

This module allows to extract the secret image contained within the image stego by means of the secret key. The module has as inputs the stego image of dimensions $N_1\times M_1\times 3$ and the key of $(4 + N_2 \times M_2)$ elements.
The steps to recover the secret image are:

a) Identify the band in which the secret image is contained: the image stego decomposes into the three color bands *(R, G, B)* and to Next you select the number of the band that was stored in the key. This information was recorded in the fourth position of the key in the concealment process.

b) With the information contained in the code, starting from the fifth position, the band pixels of the host image that were modified and containing the secret image information. I know sweeps in a zigzag from left to right and top to bottom to extract modified pixels. This sweep is done in the same way than in the concealment module, since the value of the positions of the modified pixels correspond to the absolute position within the band.

c) If the value of 0 is found in the key, it means that the pixel of the secret image could not be hidden within the selected band of the host image. In such a way that, it is assigned to that pixel of the image secretes the average of the pixels, which was previously stored in the key in the third position. This average is very similar to the value expected from the image (the one with the highest probability of occurrence), but computationally less costly.

d) After completing the pixel extraction process, a vector of $N_2 \times M_2$ elements. This vector is resized according to the information contained in the first two positions of the key ((number rows and columns of the secret image).

A schematic of the recovery module is shown in Figure 2.

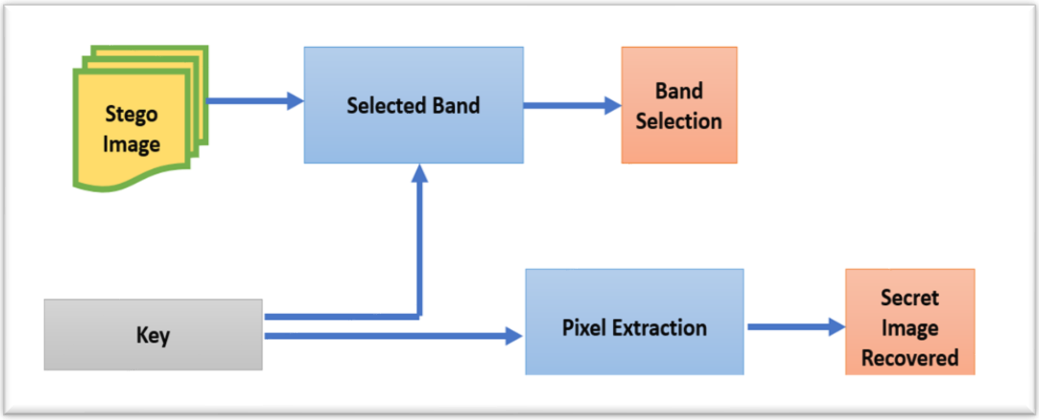


Figure 2. Recovery module

3. Methodology and results

For the validation of the proposed method, 10 images were selected from color (*RGB*) and 10 grayscale images. Image databases were taken from the website http://www.imageprocessingplace.com/, in particular those corresponding to chapter 6 of the Digital Book

Image Processing, 3rd edition by González and Woods [20] and the images standard test, offered by that same website. Color images were cropped to *512× 512* pixels and grayscale image resized to *128 ×128* pixels. The pixel ratio of the image host versus the number of pixels in the secret image is 16: 1.

The test protocol used to validate the three methods under study is as follows:

a) The first secret image is hidden in each of the host images. The imperceptibility of the generated stego images is calculated.
b) From the stego images and the corresponding keys, we obtain the secret images recovered. The quality of the recovered images.
c) Steps a and b are repeated for each of the secret images.
d) At the end of step c, 10 stego images are obtained for each image secret, that is, a total of 100 stego images are obtained for each method.

For the three methods, the total number of simulations carried out was 300. BPHM and IPHM worked with a range of 20, while the method *QIM* with a step of 10. With the 100 simulations per method, we calculate the following evaluation parameters:

Imperceptibility: your goal is to quantify how different the stego image of the host image and if there are areas in which the distortion is appreciable. The similarity between the images is measured with the normalized correlation coefficient (*NC*) and distortion by means of the degree of variation between neighbors (*GVD*). A good stego image is that which has a high *NC* (the closest to 1) and a low *GVD* (the closest to 0).

To calculate the value of *GVD* the following equations [9] are used:

$$\mathrm{GN}(x, y) = \frac{\sum[S(x,y) - s'(x,y)]^{2}}{4} \qquad (1)$$

GN is a matrix that corresponds to the difference in Gray level between the central pixel and its four neighbouring pixels. *S (x; y)* is the evaluated pixel at the coordinates (x; y) and S0

(x; y) are the four neighbours of the central pixel, neighbours being understood as the right pixel, the left pixel, the pixel upper and lower pixel.

The total of *GN* values in an image of size *N ×M* is (N_2) (M_2), since the first and last are excluded from the calculation column, and the first and last row of the image. Subsequently, the average difference in gray level is calculated,

given by the equation:

$$AG = \sum_{x=2}^{i-1} \sum_{y=2}^{j-1} GN(x, y) \qquad (2)$$

Where AG is a scalar.

To obtain the overall distortion level between the stego image and the host image, the *GVD* between them is calculated by means of the equation:

$$GVD = \frac{AG' - AG}{AG' + AG} \qquad (3)$$

Being *AG* the average value of the stego image and *AG* the average value of the host image. *GVD* is a scalar. It is highlighted that if the image stego was the same as the host image, the value of *GVD* would be 0, and as the stego image becomes more distorted, the value of *GVD* becomes moves away from 0.

Recovered Secret Image Quality - In Recovery Module

how similar is the recovered image in relation to the original secret image and how much data was lost in the process. The similarity is measured through the normalized correlation coefficient (*NC*) between the original secret image and the host image, and the amount of data that are lost in the process is measured through the *BER* (Bit Error Rate). The *BER* quantizes the number of erroneous bits in the recovered image.

It is conventionally expressed as a percentage value.

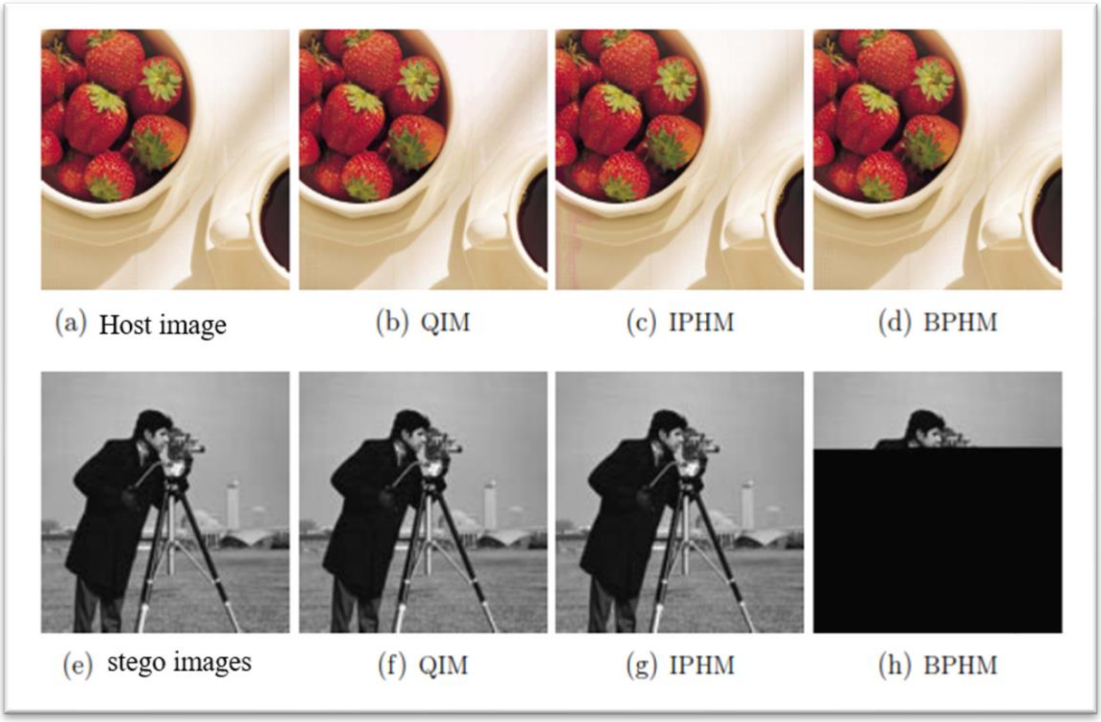


Figure 3. Example 1. (a) - (d) Host image and stego images. (e) - (h) Image secret and recovered images

3.1. Preliminary results

In order to illustrate the performance of the proposed system, Figures 3 and 4 show the results of each of the three methods, along with the corresponding quality indices. In Figure 3, the *QIM* method obtained *NC = 0.9994, GVD = 0.3064* in the stego image and *NC = 1, BER = 0%* in the recovered image. For his On the other hand, the IPHM method obtained similar results, with *NC = 0.9991, GVD = 0.0277* in the stego image and *NC = 1, BER = 0.03%* for the recovered image. Finally, the BPHM method obtained the following results, for the stego image *NC = 0.9999, GVD = 0.02* and for the recovered image *NC = 0.5047, BER = 31.78%.*

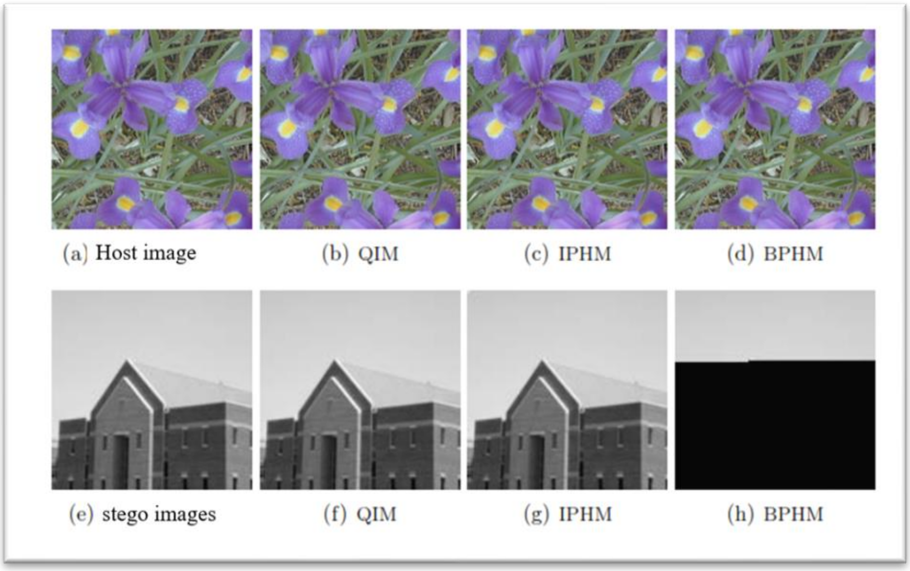


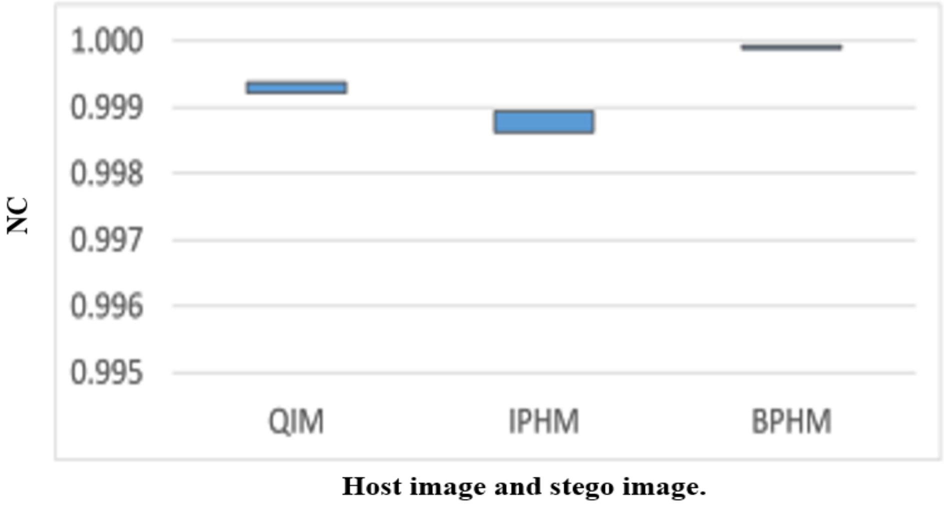
Figure 4. Example 2. (a) - (d) Host image and stego images. (e) - (h) Image secret and recovered images

In Figure 4, the results are very similar and were as follows:
test: QIM: Stego image (NC = 0.9987, GVD = 0.4895) and recovered image (NC = 1, BER = 0%). For IPHM, the image stego (NC = 0.9981, GVD = 0.0570) and in the recovered image (NC = 0.9999, BER = 0.13%). In BPHM, the stego image obtained (NC = 0.9997, GVD = 0.0014) and the image recovered (NC = 0.5998, BER = 32.92%).

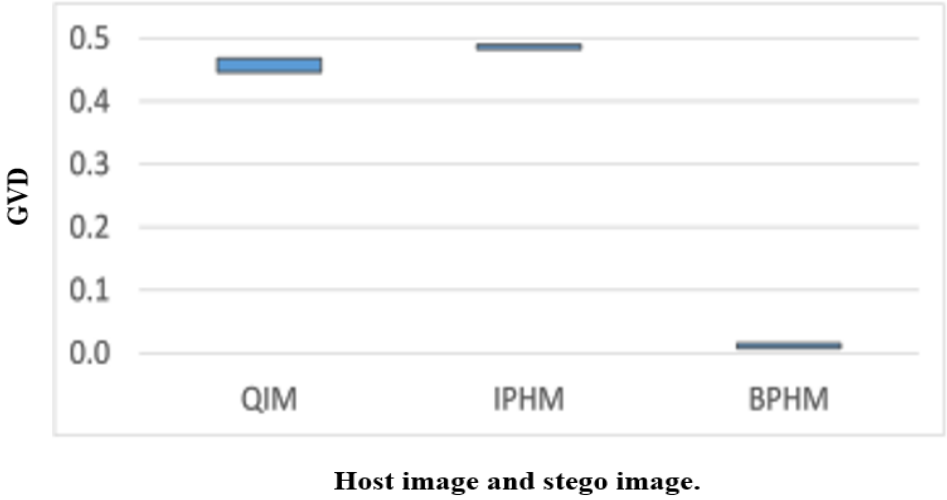
According to the results of Figures 3 and 4, it can be corroborated that all three methods has a high imperceptibility value, but only *QIM* and *IPHM* allow to recover the secret image in large part or in its whole. It is important to note that the *BPHM* method does not guarantee the hiding of all the pixels of the secret image, and consequently, the recovered image may be incomplete.

3.2 Consolidated results in terms of imperceptibility

For each of the methods used in the validation phase,100 stego images, which are compared against host images original, using the parameters *NC* and *GVD*. Figures 5 (a) and 5 (b) present the consolidated results by means of graphs of rank of trust. In these graphs, each "box" contains 95% of the results by method.



(a) NC between host image and stego image



(b) GVD between host image and stego image.

Figure 5: Consolidated imperceptibility: *NC* and *GVD*.

According to the results obtained, in the three methods the values of similarity are above 0.998 and distortion is very low. The method with less distortion is *BPHM* and the values for *QIM* and *IPHM* are very Similar.

3.3. Consolidated results in terms of quality of the recovered image

To measure the quality of the recovered image, the parameters from NC and *BER*. The image with the best quality is the one with an *NC* high (closest to 1) and very low *BER* (closest to 0%). Of Again, confidence charts are used to show the range in which they locate 95% of the results, for each of the evaluated methods. Figure 6 presents the consolidated in terms of *NC*. According to the results, the quality of the image recovered with the proposed method.

IPHM is very high as with the *QIM* method. The quality of the method *BPHM* is low.

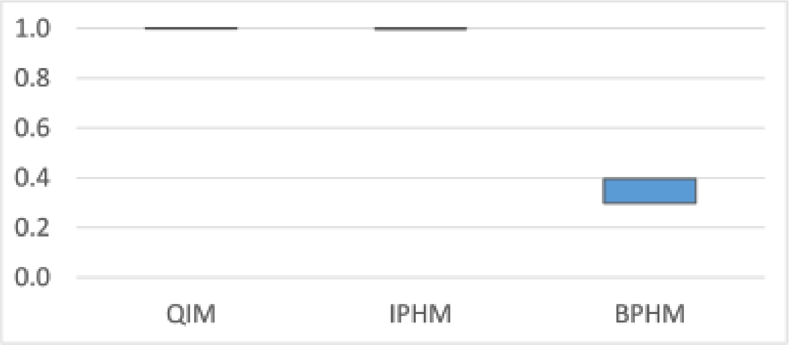


Figure 6. Consolidated quality in terms of *NC*

Figure 7 presents the consolidated in terms of *BER*. Both in the *QIM* methods as in *IPHM*, the *BER* value is less than 5%, while that with the *BPHM* method values close to 40% are obtained.

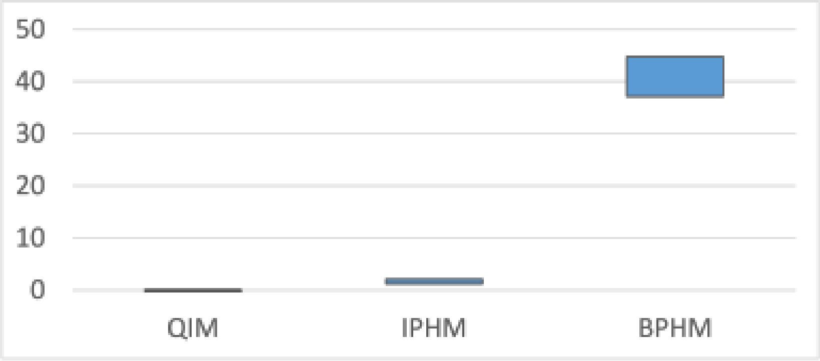


Figure 7. Consolidated quality

Figure 7. Consolidated quality: in terms of *BER* by analyzing the imperceptibility and quality results together From the recovered image, it can be concluded that the *BPHM* method generates less distortion in the stego image because it is the method that hides fewer pixels in the secret image. That is, the *BPHM* method does not guarantee that all secret information is hidden and therefore that can be retrieved by the authorized user. On the other hand, the distortion in the stego image and the quality in the recovered image are very similar between the *QIM* and *IPHM* methods, fulfilling the objective of the present investigation.

3.4. Advantages of *IPHM* over *QIM*

According to the imperceptibility and quality results, the performance of the *QIM* and *IPHM* methods is very similar and superior to that of the *BPHM*. This section discusses the advantage of the IPHM method over *QIM* in the third evaluation parameter of a steganography scheme: the concealment ability.

From various tests carried out with *IPHM*, it was found that the minimum size ratio between host image and secret image is 4: 1, that is, for every 4 pixels of the selected band of the Host image can hide a pixel from the secret image. With the above relationship, suppose you want to hide a secret color image 24-bit within a 24-bit color guest image, so that in each band of the secret image a band of the image is hidden in color (keeping the 4: 1 ratio). In this way, in IPHM the capacity total concealment is 1 pixel of the secret image for every 4 pixels of the host image, that is, a hiding capacity of 25%. On the other hand, in the *QIM* method a single bit of the image can be hidden secret in each pixel of the host image, i.e. to hide one pixel 8 pixels of the host image are required from the secret image, and therefore both its concealment capacity is 12.5%.

When comparing the previous results, it is concluded that the maximum capacity concealment of the IPHM method is twice the maximum capacity concealment of the QIM method, or in other words, that with the IPHM method can hide a secret image twice the size of the image that is hidden in QIM [25-26].

Steganography based on Internet of Things (IoT) and cloud computing [27-29], are feasible future trends to develop this study in terms of security and communication.

4. Conclusions

This research describes the *IPHM* method, which raises a upgrade to one of the image-scale steganography methods Gray on colour images, known as the *BPHM* method. The best performed to the method were based on the following conditions: selection of the band that hides the secret image according to a similarity criterion histograms, global search, and replacement criteria in the data that they cannot be hidden. Although the proposed method is not completely reversible, the amount of information lost is less than 5%, which allows to recover the secret image with a high similarity with respect to the original secret image. In terms of imperceptibility, results are obtained like those obtained with one of the most widely used methods in steganography of images in images, the *QIM* method. Further, the proposed method allows a greater concealment capacity than the *QIM* method, consolidating itself as a solution that allows a good balance between the three design criteria of a steganography scheme: imperceptibility, quality of retrieved information and capacity concealment.

References

[1] S. Jayasudha, “Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm,” International Journal of Engineering and Science, no. 2, pp. 31–35, 2013.

[2] A. J. Qasim et al., "Review on techniques and file formats of image compression", vol. 9, no.2, p. 602–610, 2020.

[3] F. Q. A. Al-Yousuf and R. Din, “Review on secured data capabilities of cryptography, steganography, and watermarking domain,” 2020.

[4] M. Hussain, Image steganography in spatial domain: A survey. Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

[5] H. S. Hussain, R. Din, M. H. Ali, and N. Balqis, “The Embedding Performance of StegSVM Model in Image Steganography,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 12, no. 1, pp. 233–233, 2018.

[6] A. Saini, K. Joshi, and S. Allawadhi, “A Review on Video Steganography Techniques,” International Journal, vol. 8, no. 3, 2017.

[7] V. M. S. V. Tummala, Comparison of Image Compression and Enhancement Techniques for Image Quality in Medical Images, MSC Thesis, Blekinge Institute of Technology, 2017.

[8] A. M. Al-Shatnawi, “A new method in image steganography with improved image quality,” Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907–3915, 2012.

[9] A. A. J. Altaay, S. B. Sahib, and M. Zamani, “An introduction to image steganography techniques,” 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012.

[10] A. A. J. S. Altaay, “Shahrin Bin Zamani, Mazdak. An introduction to image steganography techniques,” 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012.

[11] T. Amarunnishad and A. Nazeer, “Secured Reversible Data Hiding In Encrypted Images Using Hyper Chaos,” International Journal of Image Processing (IJIP), vol. 8, no. 6, pp. 423–423, 2014.

[12] P. K. Amin, N. Liu, and K. P. Subbalakshmi, Statistical attack resilient data hiding. IJ Network Security, vol.5, no.1, pp. 112-120, 2007.

[13] R. Din and A. J. Qasim, “Steganography analysis techniques applied to audio and image files,” 2019.

[14] A. J. Qassim and Y. Sudhakar, Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm, International Journal of Advances in Computer Science and Technology, vol.4, no.4, pp.93-97, 2015.

[15] R. Din, O. Ghazali, and A. J. Qasim, “Analytical Review on Graphical Formats Used in Image Steganographic Compression,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 12, no. 2, pp. 441–441, 2018.

[16] M. Tayel, H. Shawky, A. E, and D. S. Hafez, “A new chaos steganography algorithm for hiding multimedia data,” Advanced Communication Technology (ICACT), 2012.

[17] B. B. Zaidan, A. A. Zaidan, A. Taqa, and F. Othman, “Stego-Image Vs Stego-Analysis System,” International Journal of Computer and Electrical Engi- neering, vol. 1, no. 5, pp. 572–578, 2009.

[18] S. hil, R. S. Garhwal, and D. esh, “Composition of Sewage and Non-Sewage Water of Different District of Haryana, India,” 2019.

[19] R. Amirtharaj and J. B. B. Rayappan, “Steganography-Time to Time: A Review,” Research Journal of Information Technology, vol. 5, no. 2, pp. 53–66, 2013.

[20] R. J. Anderson and F. A. P. Petitcolas, “On the limits of steganography,” IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 474–481, 1998.

[21] A. Tiwari, S. R. Y, and N. K, “A Review on Different Image Steganography Techniques,” International Journal of Engineering and Innovative Technology (IJEIT), no. 3, 2014.

[22] A. Aos, et al, Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File in Computer Science and Information Technology-Spring Conference, 2009.

[23] S. K. Bandyopadhyay, “A tutorial review on steganography,” International conference on contemporary computing, 2008.

[24] B. G. Banik and S. K. Bandyopadhyay, Review on Steganography in Digital Media, International Journal of Science and Research (IJSR), vol.4, no.2, pp.265-274, 2013.

[25] K. A. A. Mutlaq, H. H. Madhi, and H. R. Kareem, “Addressing big data analytics for classification intrusion detection system,” Periodicals of Engineering and Natural Sciences, vol. 8, no. 2, pp. 693–702, 2020. [26] H. R. Kareem, H. H. Madhi, and K. A. A. Mutlaq, “Hiding encrypted text in image steganography,” Periodicals of Engineering and Natural Sciences (PEN), vol. 8, no. 2, pp. 703–707, 2020.

[27] A.A.H. Mohamad, Y. S. Mezaal, S. F. Abdulkareem, "Computerized power transformer monitoring based on internet of things," International Journal of Engineering & Technology 7, no. 4, pp.2773-2778, 2018.

[28] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, & S. F. Abdulkareem," Iraqi e-government and cloud computing development based on unified citizen identification", Periodicals of Engineering and Natural Sciences, vol.7, no.4, pp.1776-1793, 2019.

[29] Y. S. Mezaal, L. N. Yousif, Z. J. Abdulkareem, H. A. Hussein, S. K. Khaleel, “Review about effects of IOT and Nano-technology techniques in the development of IONT in wireless systems,” International Journal of Engineering and Technology (UAE), vol. 7, no. 4, 2018.