Reci
Revista
Iberoamericana de las
Ciencias Computacionales
e Informática
ISSN: 2007 - 9915

Una nueva técnica de transmisión segura de imágenes aplicando transformaciones de color reversibles en zonas ruidosas de la imagen

A new secure image transmission technique applying reversible color transformations in noisy regions of the image

Uma nova técnica para a transmissão segura de imagens através da aplicação de transformações de cores reversíveis em áreas ruidosas da imagem

Cristian Marcelo Vasco Estupiñan
Universidad de las Fuerzas Armadas ESPE, Ecuador
crisvasco93@hotmail.com
https://orcid.org/0000-0002-2997-9510

Freddy Roberto Acosta Buenaño
Universidad de las Fuerzas Armadas ESPE, Ecuador
fracosta@espe.edu.ec
https://orcid.org/0000-0002-2143-5471

Resumen

La esteganografía es un proceso que consiste en ocultar información dentro de un objeto (contenedor). Es un desafío mejorar las técnicas actuales de esteganografía con el fin de que proporcionen seguridad contra ataques de estegoanálisis estadístico. Este artículo propone una nueva técnica de transmisión segura de imágenes mediante la combinación de dos métodos: el primero basado en transformaciones reversibles de color, el cual transforma una imagen secreta en una imagen mosaico que luce similar a una imagen portadora seleccionada previamente; y el segundo busca las áreas más adecuadas (texturas y bordes) en la imagen mosaico creada para ocultar la información relevante requerida y posteriormente recuperar la imagen secreta. Estas zonas son de naturaleza ruidosa, por lo que representan un reto para el estegoanálisis al momento de extraer características encargadas de determinar si una imagen tiene información embebida. La efectividad del método propuesto se evaluó mediante el análisis de histogramas y utilizando la herramienta de estegoanálisis StegExpose.

Palabras clave: estegoanálisis estadístico, esteganografía, estegoimagen, imagen mosaico, transformaciones reversibles de color.

Abstract

The steganography is a process that consists in hiding information inside an object (container). Improving current steganography techniques in order to provide robustness against statistical attacks is a challenge. This article proposes a new secure image transmission technique by combining 2 methods: The first one is based in reversible colors transformations, which turns the secret image into a mosaic that looks similar to the carrier image previously selected. The second one looks for the most suitable areas (border and texture) in the created mosaic to hide relevant information that is required to recover the secret image. These zones are noisy nature, so they represent a challenge for the steganalysis at the moment of extracting characteristics that determine if an image has embedded information. The effectiveness of the proposed method is evaluated by analysis of histograms and using the steganalysis tool StegExpose.

Keywords: statistical steganalysis, steganography, stego image, mosaic image, reversible color transformations.

Resumo

Esteganografia é um processo que envolve a ocultação de informações dentro de um objeto (container). É um desafio melhorar as técnicas atuais de esteganografia para fornecer segurança contra ataques estatísticos de steganálise. Este artigo propõe uma nova técnica de transmissão segura de imagens, combinando dois métodos: o primeiro, baseado em transformações reversíveis de cores, que transforma uma imagem secreta em uma imagem em mosaico semelhante a uma imagem de portadora previamente selecionada; e a segunda pesquisa as áreas mais adequadas (texturas e bordas) na imagem em mosaico criada para ocultar as informações relevantes necessárias e, subsequentemente, recuperar a imagem secreta. Essas áreas são barulhentas por natureza, razão pela qual elas representam um desafio para a esteganálise ao extrair características responsáveis por determinar se uma imagem incorporou informações. A eficácia do método proposto foi avaliada por análise histológica e utilizando a ferramenta steganoanalysis StegExpose.

Palavras-chave: steganálise estatística, esteganografia, stegoimage, imagem em mosaico, transformações de cores reversíveis.

Fecha Recepción: Junio 2017 **Fecha Aceptación:** Diciembre 2017

Introduction

In order to send secret messages of different nature, which are understood exclusively by the recipient to whom they were addressed, steganography has been present throughout human history. Currently one of the great advances in this branch is the use of multimedia content (audio, video and images) to hide messages. The use of images has increased because most of the information present throughout the world is digital, and it is transmitted electronically over the Internet. Therefore, it is important to have security methods such as encryption techniques or access keys to protect sensitive or confidential information. However, just as data is susceptible to being hidden, so are data from being intercepted by people other than the final recipient. Recently, different methods have been proposed to ensure the transmission of images: the most common approaches are cryptography and data concealment, that is, steganography.

As mentioned by Satwinder and Varinder (2015), cryptography uses the characteristic properties of the image to turn it into a noisy image in such a way that its contents can not be visualized, unless the secret key is available to decipher it. However, transmitting an image as noise can attract the attention of an attacker and show the presence of a hidden message. Therefore, another alternative is the application of steganography.

Steganography has different classifications. In this investigation, spatial domain steganography was applied, based on texture and edges, due to its low complexity and its great capacity for embedding. As presented by Nusrati and Karimi (2015) and also by Fridrich, Du and Meng (2000), in this method the secret information travels embedded in a carrier image, in which the bit string of the secret message is introduced into the flow of bits of the pixels of the carrier image.

The main complexity of hiding information in an image is the capacity of embedding, since, when hiding an image inside another carrier image, it is necessary to make sure that both are of the same size; otherwise, one of the images must be compressed before the embedding process. This compression causes distortions and losses in the original image, as mentioned by Lerch-Hostalot and Megías (2014), which is detrimental to images with relevant content.

Many of the current steganographic methods try to improve the embedding algorithm to achieve greater robustness. However, very few focus on the characteristics of the container object where the information is hidden.

For this reason, this article proposes an algorithm that combines a method of image transformation, using the characteristics of color, and a new steganographic method that uses differential operators and filters to detect the most suitable areas of the image to embed the information, with the objective of having steganographic images difficult to detect by tools of stegoanalysis.

This new method has been based on the way in which steganoanalysers work: to detect the use of the more complex techniques known as LSB matching, which can be found in detail in Hu, Zhang, Hu, Yu and Xianfeng (2013). Stenoanalyzers use a database of images and train classifiers that detect images that contain hidden information. For this purpose, the characteristics of the image that are susceptible to be altered when embedding information are sought and these characteristics are modeled to train the classifier.

As for the classifiers, it is known that there are areas that are difficult to model, such as edges and textures. As presented by Lerch-Hostalot and Megías (2014), modern steganographic systems focus their research mainly on methods that hide information in areas of noisy nature, which are difficult to model to train the classifiers.

The following section of this article briefly describes the methodology used for the creation of the mosaic image and the recovery of the secret image. The third section, for its part, exposes the algorithm in detail to find the right areas and then embed the relevant information in those areas. The fourth presents the experimental results obtained with the proposed algorithm that were compared with the results obtained with the algorithm of Ya-Lin and Wen-Hsiang (2014). Finally, the conclusions of this investigation are presented.

Algorithm used by Ya-Lin and Wen-Hsiang

Based on the research methodology used by Ya-Lin and Wen-Hsiang (2014), an algorithm was developed consisting of two main sections: the creation of a mosaic image and the recovery of the secret image (see figure 1).

In this regard, four fundamental elements are observed:

1. Secret image: image that you want to hide.
2. Carrier image: base image for the creation of the mosaic.
3. Mosaic image: image similar to the carrier image that will contain the secret image.
4. Algorithm used.

Figura 1. Metodología del algoritmo empleado

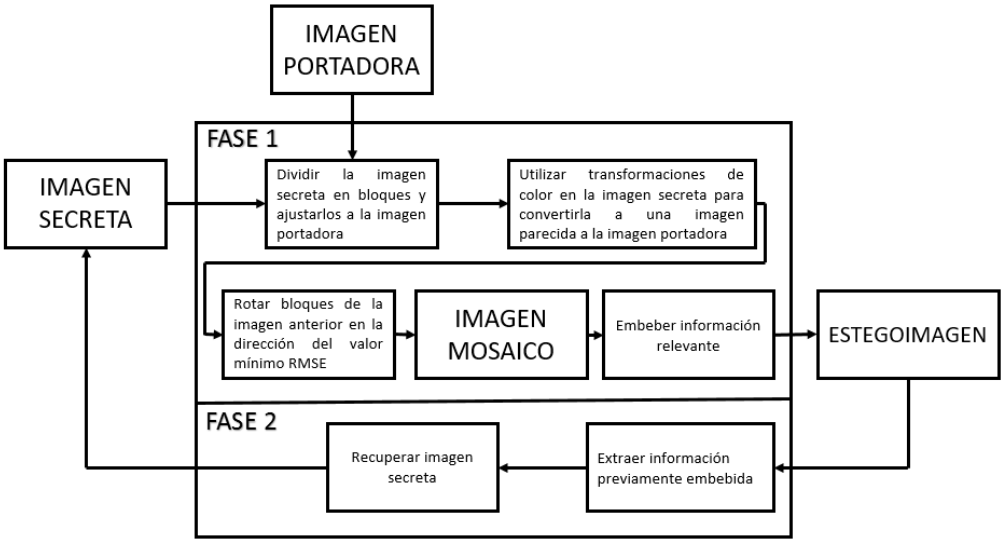


IMAGEN PORTADORA
FASE 1
IMAGEN SECRETA
Dividir la imagen secreta en bloques y ajustarlos a la imagen portadora
Utilizar transformaciones de color en la imagen secreta para convertirla a una imagen parecida a la imagen portadora
Rotar bloques de la imagen anterior en la dirección del valor mínimo RMSE
IMAGEN MOSAICO
Embeber información relevante
ESTEGOIMAGEN
FASE 2
Recuperar imagen secreta
Extraer información previamente embebida

Fuente: Elaboración propia

The first phase of the process aims to obtain a mosaic image that looks similar to the carrier image, thanks to the use of reversible color transformations, applied to the secret image. The mosaic image hides key information about the color characteristics (means and standard deviations) of the secret image using steganographic methods. Unlike the original technique that uses the LSB method throughout the mosaic image, a new technique was used that looks for the noisiest areas (textures and edges) of the image for the embedding process. This method uses filters and differential operators with the purpose of obtaining a statistically more imperceptible mosaic image before these analyzers.

Once the estegoimagen was transmitted, the procedure of the second phase of the algorithm was applied, which consists of the recovery of the secret image. The inverse process of the first phase was performed using again reversible color transformations and parameters such as means and standard deviations hidden in the mosaic image. The process was carried out in color images, so all the applied procedures are carried out in each of the three RGB color matrices (red, green and blue).

The process of obtaining the mosaic image and the recovery of the secret image were developed by the method proposed by Ya-Lin and Wen-Hsiang (2014), as already mentioned, which will be briefly described later, while the new The technique used will be explained in great detail in the third section of this work.

Creation of the mosaic image

First, it is verified that the carrier image denoted as P and the secret image S have the same size. In the case of not being so, a common size must be established. For this work images of 640 x 480 pixels were used, because they are divisible capacity quantities for four, five and eight pixels (image block sizes used in the creation of the mosaic image).

As a second step, P and S were divided into blocks of the same size. When using 8 x 8 pixel blocks, better results were obtained, both in relation to the RMSE value (mean square error) and the number of pixels to be hidden and the execution time, all of which is exposed in the results section.

The objective of dividing the secret image into blocks is to match the fragments of the carrier image to make their color distributions look similar. Obviously the color characteristics between both images are different, so it is necessary to make reversible color transformations beforehand. To do this, the calculation of the mean and standard deviation per block in each RGB channel is required, using the following equations presented by Ya-Lin y Wen-Hsiang (2014):

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad , \quad \mu_c{}' = \frac{1}{n}\sum_{i=1}^{n} c_i{}' \tag{1}$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \quad , \quad \sigma_c{}' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i{}' - \mu_c{}')^2} \tag{2}$$

Where μ_c y μ_c' denote the average y σ_c y σ_c' the standard deviation of the secret image and the carrier image, respectively; c corresponds to the pixel values of the block in each channel (RGB) and n is the total number of pixels in each block. Then you get the new color value of each pixel c_i'' with the following equation:

$$c_i{}'' = q_c(c_i - \mu_c) + \mu_c{}' \tag{3}$$

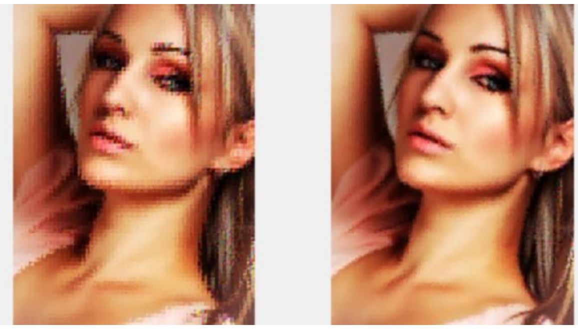
Besides $q_c = \sigma_c'/\sigma_c$ corresponds to the standard deviation coefficient. Then you can easily obtain the original color of the pixel by reversing the equation (3).

$$c_i = \left(\frac{1}{q_c}\right)(c_i{}'' - \mu_c{}') + \mu_c{}' \tag{4}$$

With the equation (4) the original values of the secret image can be recovered, it being necessary to previously embed the relevant information exposed in the following section in the mosaic image.

Likewise, in order to better adjust the blocks of the secret image, after the transformation of the color characteristics, the blocks are rotated in four directions: 0º, 90º, 180º and 270º. In this way, new blocks rotated at the optimum angle are obtained, in order to have the lowest RMSE value with respect to the block of the carrier image, as can be seen in figure 2.

Figura 2. Imagen tras aplicarse las transformaciones reversibles de color en la imagen secreta (a) e imagen tras aplicarse la rotación de bloques también llamada imagen mosaico (b)



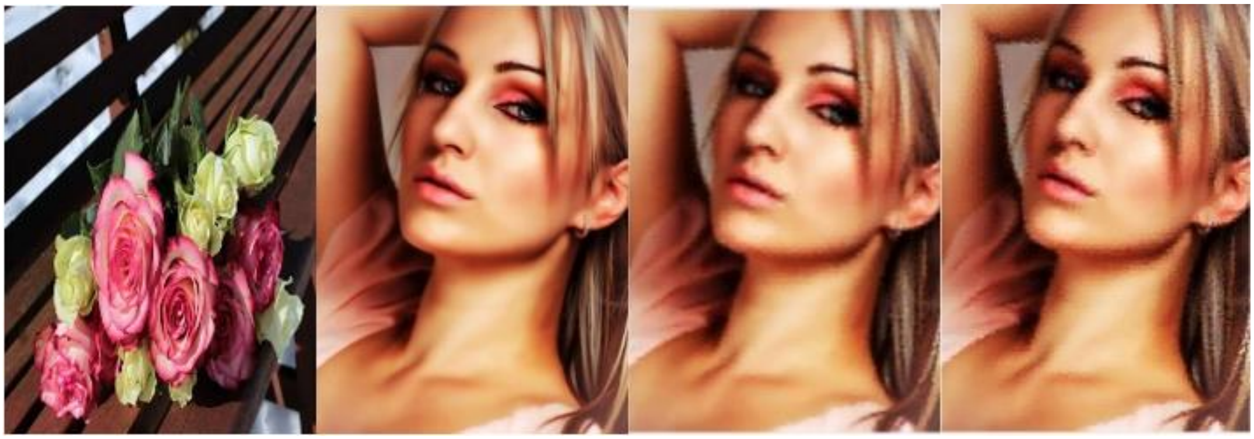
(a) (b)

Fuente: Elaboración propia

After completing the creation of the mosaic image, the new technique is applied, which consists of the detection of noisy areas (textures and edges) of the image and embedding of the relevant information in them, all of which is explained in the following section.

As a result of both processes, the mosaic image is obtained with the hidden information called estegoimagen, which has a bit stream that contains the number of iterations, number of pixels used for the embedding process and the map of edges and textures. This bitstream is used as a K key to improve the security of the algorithm. The estegoimagen can be observed in figure 3.

Figura 3. Resultado obtenido por el método propuesto. Imagen secreta (a), imagen portadora (b), imagen mosaico creada a partir de (a) y (b) mediante el método propuesto (c) y estegoimagen con información embebida (d)



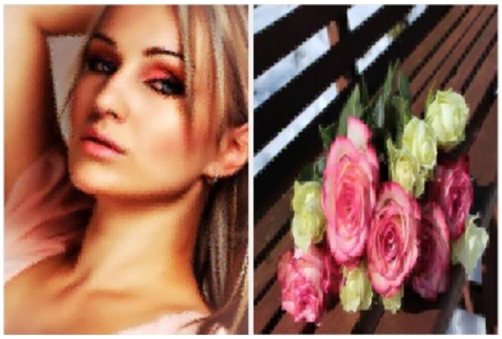
(a) (b) (c) (d)

Fuente: Elaboración propia

Recovery of the secret image

The receiver must have the K key, formed in the previous section, to recover the secret image. Through it, you can get the secret information through the process of extracting bits. Once the altered pixels have been identified by means of the map of edges and textures, the inverse algorithm of the information embedding is applied. This application is carried out only in the specified areas, in order to obtain the hidden message and the mosaic image, as shown in Figure 4.

Figura 4. Resultado de la recuperación de imágenes. Imagen mosaico recuperada por el método de extracción de bits (a) e imagen secreta recuperada (b)



Fuente: Elaboración propia

The hidden message presents enough data to recover the secret image through the following inverse process:

1. Rotate the blocks in the reverse direction of the optimal angle to obtain the original block.
2. Apply equation (4), using the means and coefficients to obtain the original pixel value.
3. Sort the blocks according to the initial positions and thus recover the secret image.

Proposed steganographic algorithm

Once the mosaic image was created, the proposed steganographic algorithm is applied, which consists of two stages: a) detection of suitable zones and b) embedding of the relevant information.

Detection of suitable zones for the creation of the map of edges and textures

Previous studies have proposed techniques that establish a threshold and work with pairs of pixels, in which, if the difference is greater than or equal to the threshold, are considered as edges and textures of the image, as mentioned by Lerch -Hostalot and Megías (2014). However, for this research we used differential operators and filters that consider more neighboring pixels to detect significant variations in the pixel values (see figure 5). In addition, the RGB mosaic image must be converted to a grayscale image, to then apply the edge and texture detection algorithms.

Figura 5. Diagrama de bloques de algoritmo de búsqueda de zonas adecuadas para la incrustación de información

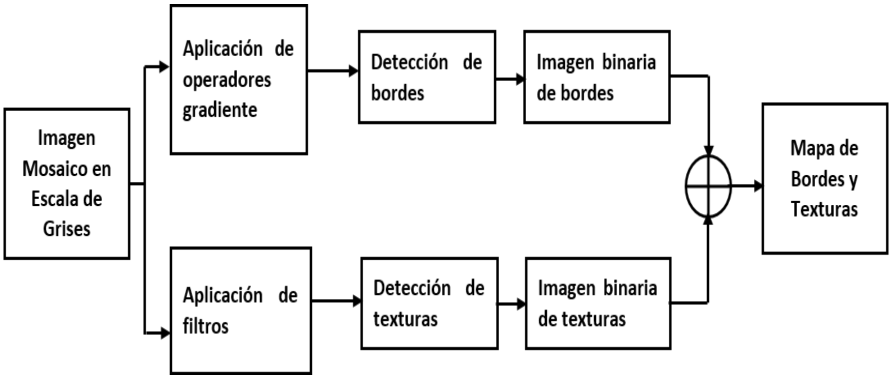


Imagen Mosaico en Escala de Grises
Aplicación de operadores gradiente
Detección de bordes
Imagen binaria de bordes
Aplicación de filtros
Detección de texturas
Imagen binaria de texturas
Mapa de Bordes y Texturas

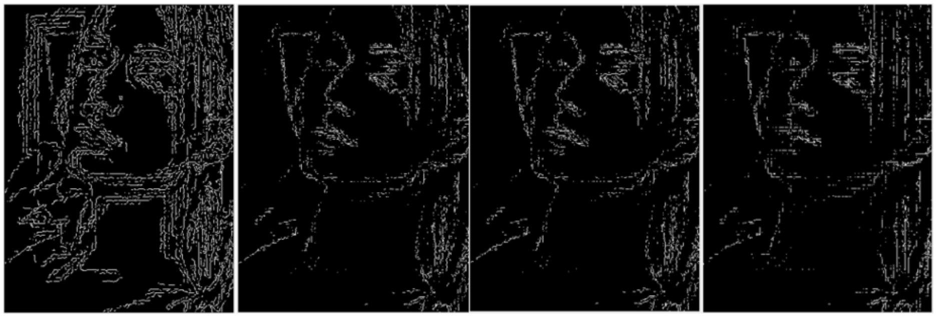
Fuente: Elaboración propia

For the detection of borders there are different methods based on gradient operators, such as Sobel, Prewitt, Roberts and the Canny detector, which are exposed in detail in Moreira, Vladimir and Chávez (2009).

In the proposed algorithm, the Canny operator was used because it yielded better results. This operator, unlike the other methods, consists of two main stages: the first uses the Gaussian filter to reduce the noise in the image (textures and insignificant details), and the second uses differential operators to detect the edges in all the directions (horizontal, vertical and diagonal).

The result of the application of the Canny operator is a binary image, where the zones considered edges are represented in the image with the value of one and the uniform zones with value of zero, as shown in figure 6.

Figura 6. Métodos de detección de bordes: Canny (a), Sobel (b), Prewitt (c) y Roberts (d)

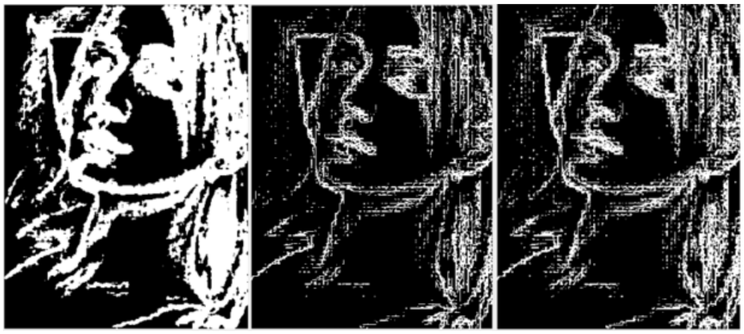


(a) (b) (c) (d)

Fuente: Elaboración propia

On the other hand, for the detection of textures filters were applied in a pixel and in a group of adjacent pixels, where certain characteristics are determined to detect textures in the image. The most common characteristics found in an image are the entropy of the distribution of gray levels, the standard deviation (distribution of gray levels in a region) and the range of values (maximum and minimum). In this regard, the result of the application of the different filters to the mosaic image in gray scale can be observed in figure 7.

Figura 7. Filtros para detección de texturas: entropía (a), desviación estándar (b) y rango de valores (c)



(a) (b) (c)

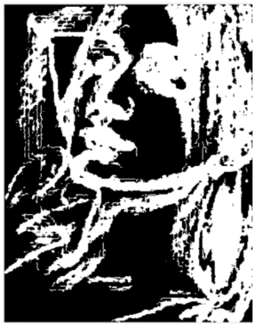
Fuente: Elaboración propia

The proposed algorithm requires a large embedding capacity, and the entropy filter was chosen, because of its number of gray levels and the frequency of each level. The zones with lower entropy represent the textures in the image.

By applying said filter to the mosaic image, an output is obtained with the entropy value of a 9 x 9 matrix of neighboring pixels around the pixel selected in the original image, as mentioned by Benet (2016). This output is converted to binary to have a map of the pixels that can be used in the process of embedding information. In this way, the binary image contains ones, which represent the textures of the image, and zeros, which are uniform zones of the image.

After obtaining two binary images with the edges and textures of the mosaic image, an operation of summing both images was performed. In this way, the map of edges and textures was obtained for the embedding of relevant information (see figure 8).

Figura 8. Mapa de bordes y texturas formadas de las figura 6 (a) + figura 7 (a)



Fuente: Elaboración propia

Embedding relevant information

The information that is hidden in the mosaic is shown in the following items:

1. The indexes of the original positions of the carrier image.
2. The angle of rotation of the blocks of the mosaic image.
3. The means and the standard deviation coefficient of each block within the established range.
4. Waste overflow and underflow.

A fixed number of bits must be established for each item to be hidden, for example, two bits were used for the angle, since it has four different possible directions of rotation. The items of all the blocks must be concatenated forming a single flow of M bits for the RGB channels; that is, three flows are formed that will be independently hidden in the matrix of the corresponding channel. The large number of bits to be hidden makes it necessary to carry out several iterations in the embedding process. This occurs because the number of bits available in the texture and edge map is less than the bit stream that must be hidden.

It is also necessary to create another bit stream, I, with the following data: number of iterations required per channel, number of pixels used in the last iteration per channel and the Huffman table used to encode the residuals. Also, you need to hide the map of textures and edges in another bit stream called *M'*, to know the areas where information was hidden. The flows I and *M'* they are hidden in the R channel and in the G channel, respectively, finally obtaining a stegoimage to be transmitted, shown in Figure 3 (d).

A technique was applied in the pairs of pixels indicated with the ones in the map of edges and textures obtained previously. This requires the use of two fundamental formulas, where e and f represent the pair of pixels of the mosaic and *e'* and *f'* the pair of transformed pixels, as explained in Coltuc and Chasery (2007).

$$e' = 2e - f \quad , \quad f' = 2f - e \qquad (5)$$

$$e = \left\lceil \frac{2}{3}e' + \frac{1}{3}f' \right\rceil \quad , \quad f = \left\lceil \frac{1}{3}e' + \frac{2}{3}f' \right\rceil \qquad (6)$$

The procedure for hiding information consists of moving the image horizontally or vertically, each time having a different pair of neighboring pixels and applying equation (5). On the other hand, the original value of the pixels can be obtained from equation (6). This method provides high embedding capabilities because it allows several iterations. In addition, it is possible to recover the value of the original pixels with the lowest operational complexity and extract the hidden message.

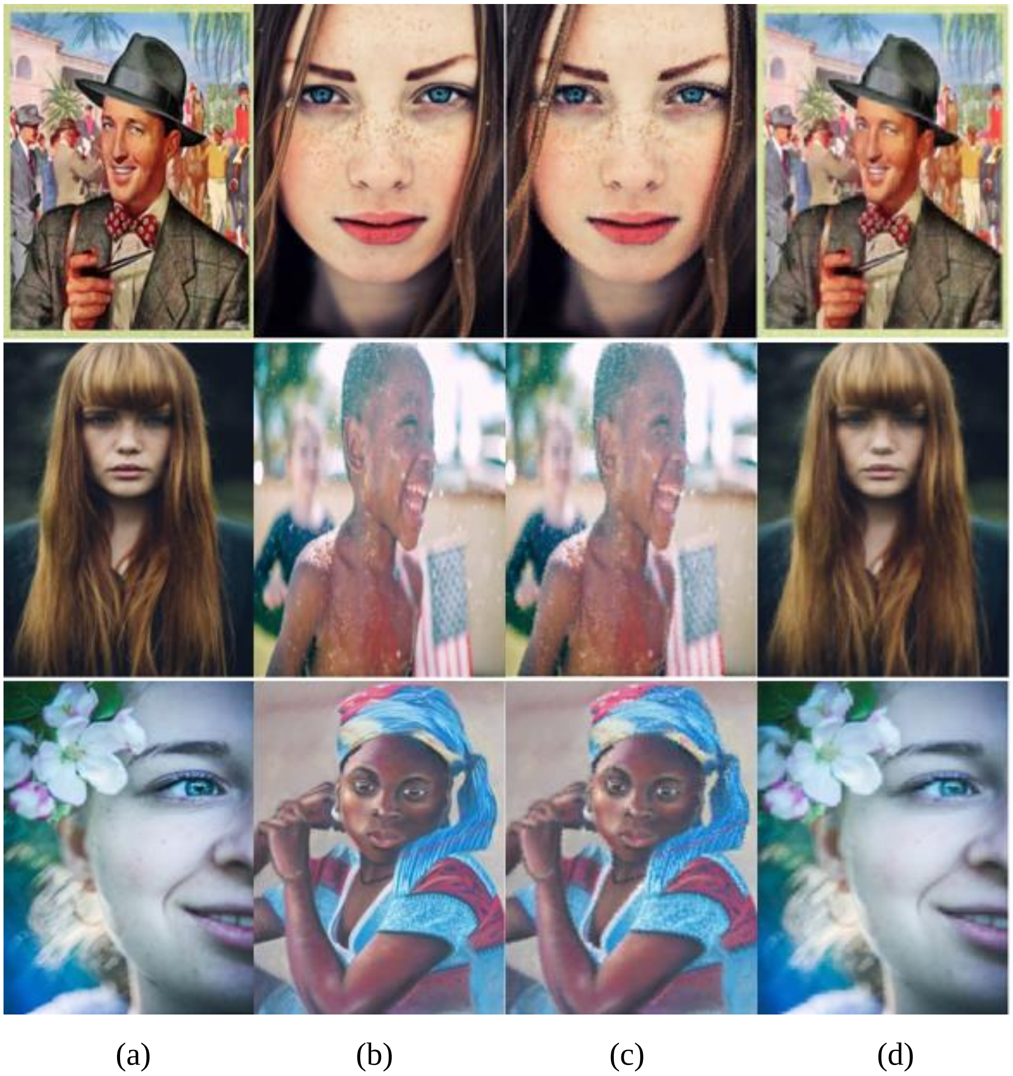
Experimental results

As part of the investigation, a series of experiments was carried out to test the proposed algorithm. The tests were performed with images extracted from a free-use database selected arbitrarily and with a pre-set size of 640 x 480.

The study consisted in comparing the stegoimages created according to the algorithm of Ya-Lin and Wen-Hsiang and the stegoimages according to the proposed algorithm. In both cases the values of the execution times of the algorithm and the number of embedded bits were compiled. Finally, the noise level measurements were obtained in PSNR images (peak signal to noise ratio), the RMSE value and the histograms of the carrier images and the stegoimages obtained with both algorithms.

Some of the stegoimages created using the proposed method can be seen in Figure 9, it is specific in column (c).

Figura 9. Resultados obtenidos por el método propuesto. Columna con imágenes secretas (a), columna con imágenes portadoras (b), columna con estegoimágenes con información embebida (c) y columna con imágenes secretas recuperadas (d)

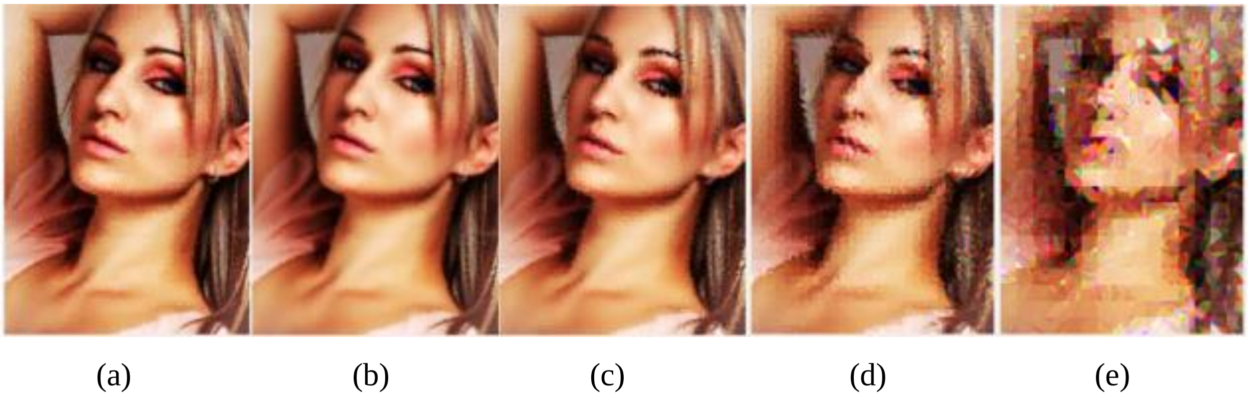


Fuente: Elaboración propia

Block size selection

Likewise, tests with different block sizes were carried out. The results obtained indicate that the RMSE value with the pixel block sizes of 16 x 16 and 32 x 32, although they have a low execution time, have a high RMSE value, that is, a low image quality with distortions. notorious, as can be seen in Figure 10. In the case of images with size 5 x 5, a high RMSE value is observed due to the distortions caused by the large amount of embedded information and also a high execution time in comparison to tests with other block sizes.

Figura 10. Estegoimágenes obtenidas con dimensiones de pixeles de 5 x 5 (a), 8 x 8 (b), 10 x 10 (c), 16 x 16 (d) y 32 x 32 (e)



Fuente: Elaboración propia

The best results were obtained with the images of block sizes 8 x 8 and 10 x 10. However, the first one was selected because it had lower RMSE values as shown in Table 1.

Tabla 1. Comparación de parámetros de imágenes para diferentes tamaños de bloque

Tamaño de bloque					
Parámetros de medición	**5 x 5**	**8 x 8**	**10 x 10**	**16 x 16**	**32 x 32**
RMSE de estegoimagen obtenida	27 709	13 487	14 014	18 676	28 981
Bits incrustados	1 455 506	575 596	376 311	186 640	144 033
Tiempo de ejecución (min)	6819	2644	1824	1061	875

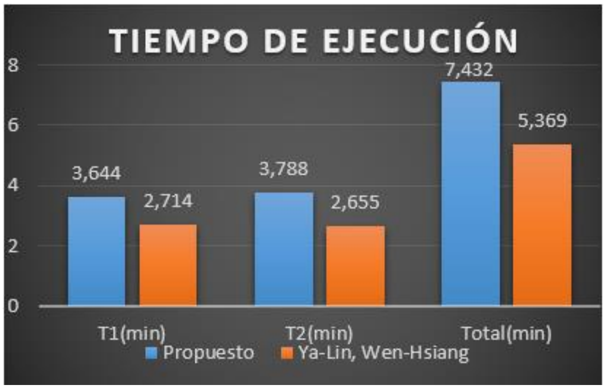
Fuente: Elaboración propia

Comparison of measurement parameters

200 experiments were carried out, that is, 200 stegoimages were created, one hundred according to the Ya-Lin and Wen-Hsiang algorithm and the other according to the algorithm proposed. In each experiment, three measurement parameters were obtained: execution time, PSNR and RMSE value.

In the case of execution time, three variables were used: T1 (mosaic image creation time), T2 (secret image recovery time) and T3 (total time). Figure 11 shows the result of the comparison of execution time between both methods.

Figura 11. Tiempo de ejecución promedio entre algoritmo propuesto y el algoritmo de Ya-Lin y Wen-Hsiang

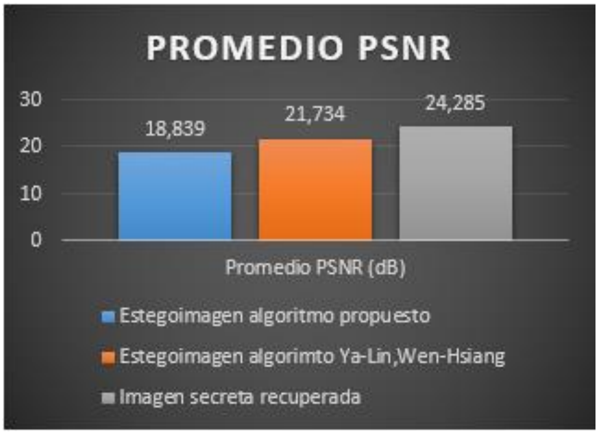


Fuente: Elaboración propia

It can be noted that the average total execution time of the proposed algorithm is greater, with two more minutes approximately (7432 min and 5369 min); this is mainly due to the fact that the proposed method needs a greater number of iterations to embed information.

On the other hand, the calculation of the PSNR value was used, which is a way of measuring the amount of noise in an image with respect to another reference image. To do this, the noise of the estegoimagen was measured with respect to the carrier image and the noise of the secret image with respect to the recovered image. Figure 12 indicates the average values obtained in the measurements made, where a higher value indicates a better image quality.

Figura 12. Tiempo de ejecución promedio entre el algoritmo propuesto y el algoritmo de Ya-Lin y Wen-Hsiang



Fuente: Elaboración propia

When comparing the three average PSNR measurements, it is evident that the recovered secret image, in both algorithms, has the highest average value, which means a better quality in the image. However, a higher value was obtained in the stegoimages created with the Ya-Lin and Wen-Hsiang algorithm because the noise is directly proportional to the number of iterations.

With regard to the average RMSE value, as a measure of image quality, the following measurements were made: the RMSE error between the carrier image and the estegoimagen and the RMSE error between the secret image and the recovered secret image. Table 2 shows the RMSE values of the four measurements, taking into account that the RMSE error between the secret image and the recovered secret image has the same value using both algorithms.

Tabla 2. Comparación de error RMSE

	RMSE de imagen portadora		**RMSE de imagen secreta**
Algoritmo	Propuesto	Ya-Lin y Wen-Hsiang	Ambos algoritmos
Promedio RMSE	29 342	21 647	16 625

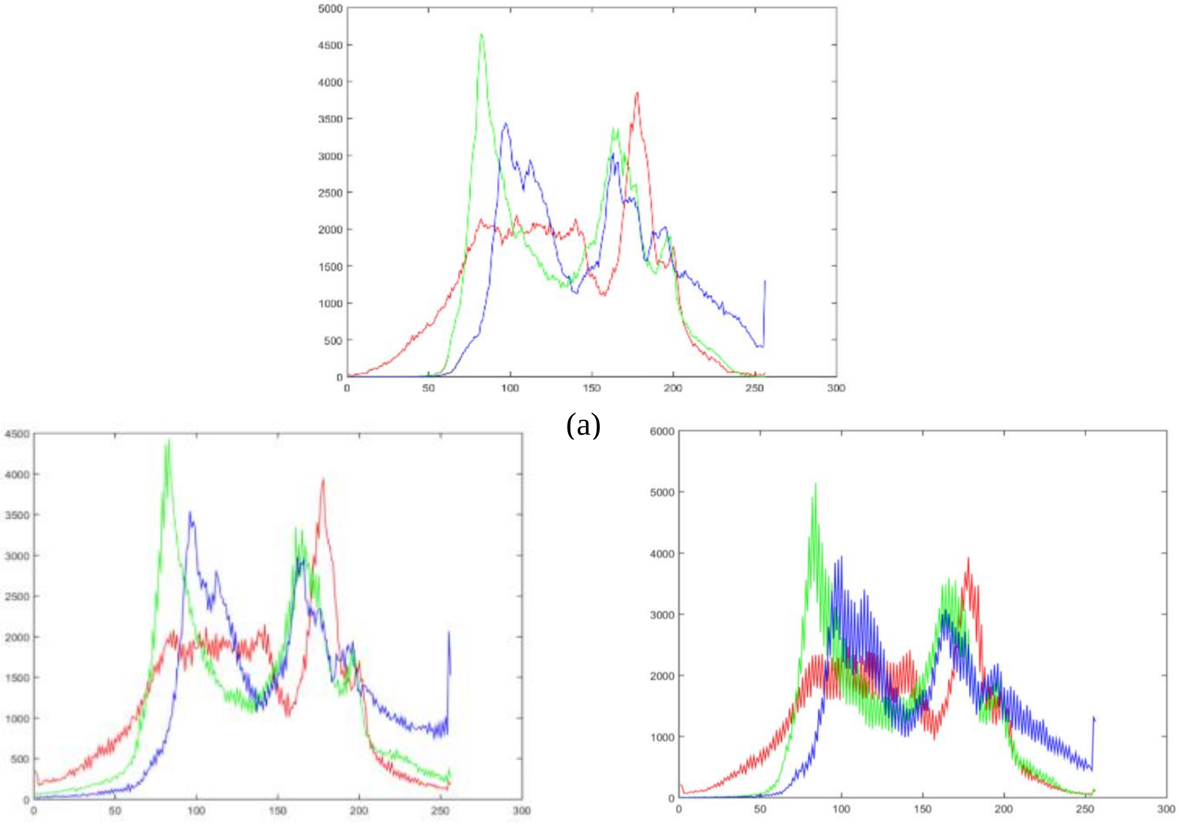
Fuente: Elaboración propia

The average measurements presented in the previous table show that the RMSE error between the stegoimage and the carrier image were greater with the proposed algorithm, in comparison to the Ya-Lin and Wen-Hsiang algorithm. This happens because for the second algorithm there is a distribution of bits embedded in the whole image; while in the proposed method a greater number of bits is embedded in certain areas of the image. On the other hand, the average RMSE error of the secret image with respect to the recovered secret image has a lower value in both algorithms than in the previous cases.

Undetectability against statistical attacks

In order to evaluate the quality of the image, the measurements of the degradations in the estegoimagen were exposed with respect to the original carrier image, calculating perceived errors and changes in the structural information referring to the visual perception of the image. However, the main objective of the research is to evaluate the undetectability of images against statistical attacks, the most common when analyzing a large number of images. For this, an analysis of some obtained histograms was made, which can be seen in figure 13.

Figura 13. Resultado de un histograma obtenido. Imagen portadora (a), estegoimagen con algoritmo propuesto (b) y estegoimagen con algoritmo de Ya-Lin y Wen-Hsiang



(a)

(b)

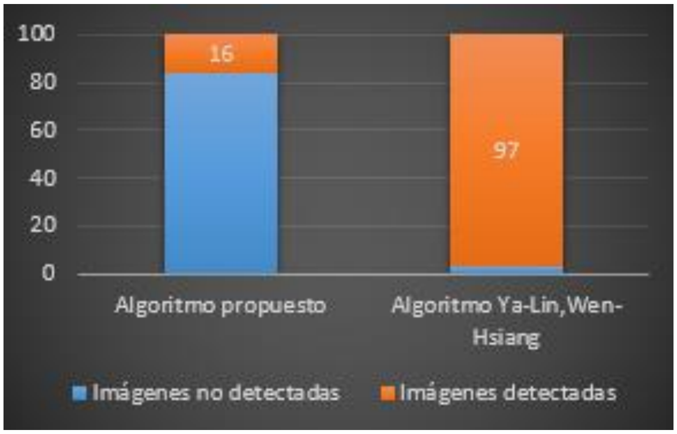
(c)

Fuente: Elaboración propia

It is evident that the histograms of the stegoimages obtained with the proposed algorithm (figure 13 [b]) have greater similarity to the histograms of the original carrier image shown (figure 13 [a]). This occurs because the proposed algorithm has a more uniform distribution of pixel values, since it has bits embedded only in the appropriate areas of the image. Meanwhile, in the histograms of the stegoimages with the algorithm of Ya-Lin and Wen-Hsiang (Figure 13 [c]), greater variations in the distribution of pixels can be noticed. This causes statistical irregularities that are more likely to be detected with statistical analysis.

Likewise, the free use Steg-Expose tool was used. This tool allows you to identify images that have hidden information. The results can be seen in figure 14.

Figura 14. Resultado del estegoanálisis por medio de la herramienta StegExpose utilizando ambos algoritmos: algoritmo propuesto y algoritmo de Ya-Lin y Wen-Hsiang



Fuente: Elaboración propia

In Figure 14, it is exposed that 84% of the 100 stegoimages obtained with the proposed algorithm were not detected by the StegExpose tool. While for the stegoimages obtained with the method of Ya-Lin and Wen-Hsiang only 3% were not detected. Finally, these results indicate that the proposed method is statistically more robust against attacks from stegoanalyzers.

Conclusions

A new algorithm for the secure transmission of images has been proposed, in which stegoimages used as camouflage to transmit secret images were created. For this, not only reversible color transformations were used, but also differential operators and filters were used to select the most suitable areas to hide the relevant information. In addition, the original secret images can be recovered almost without loss of the created images. Also, by embedding the relevant information in the most suitable areas (textures and edges), it was demonstrated that stegoimages are more difficult to detect by tools of stegoanalysis such as StegExpose. The experimental results are satisfactory and have demonstrated the viability of the proposed algorithm. Future studies could be aimed at the application of this new method in different areas, such as videography, where the images are hidden in certain frames of the video.

Acknowledgments

The present investigation was carried out with the support of the University of the Armed Forces ESPE. A special acknowledgment to the electronic engineer in telecommunications Gabriela Estefanía Onofre Concha and to Professor Julio César Larco Bravo for their collaboration in the research and writing of the article.

References

Benet, M. (2016). *Análisis de texturas de imágenes de resonancia magnética de tumores cerebrales para la caracterización y clasificación de distintas regiones de interés.* (trabajo de fin de grado). Ingeniería Biomédica. Escuela Técnica Superior Ingenieros Industriales Valencia. Universidad Politécnica de Valencia. Valencia, España. Recuperado de https://riunet.upv.es/bitstream/handle/10251/67519/35593872_TFG_146773757656651806388014303011192.pdf?sequence=2&isAllowed=y.

Coltuc, D. and Chasery, J. M. (2007). Very Fast Watermarking by Reversible Contrast Mapping. *IEEE Signal Processing Letters*, *14*(4), 255-258.

Fridrich, J., Du, R. and Meng, L. (2000). Steganalysis of LSB Encoding in Color Images. *Proceedings IEEE International Conference on Multimedia and Expo.* New York City.

Hu, X., Zhang, W., Hu, X., Yu, N. and Xianfeng, Z. (2013). Fast Estimation of Optimal Marked-Signal Distribution for Reversible Data Hiding. *IEEE Transactions on Information Forensics and Security*, 779-788.

Lerch-Hostalot, D. y Megías, D. (2014). Esteganografía en zonas ruidosas de la imagen. *RECSI*, 173-178.

Moreira, J., Vladimir, V. and Chávez, P. (2009). Implementación de un algoritmo para la detección y conteo de células en imágenes microscópicas. *Dspace*.

Nusrati, M. A. and Karimi, R. (2015). Steganography in Image Segments Using Genetic Algorithm. *ACCT*. Haryana.

Satwinder, S. and Varinder, K. (2015). State of the art Review on Steganographic Techniques. *International Journal of Signal Processing Image, Processing and Pattern Recognition, 8*(7), 161-170.

Ya-Lin, L. and Wen-Hsiang, T. (2014). A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations. *IEEE Transactions on circuits and systems for video technology, 24*(4), 695-703.

Rol de Contribución	Autor(es)
Conceptualización	**Freddy Roberto Acosta Buenaño**
Metodología	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Software	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan<<igual>> Freddy Roberto Acosta Buenaño <<que apoya>>**
Validación	**Cristian Marcelo Vasco Estupiñan**
Análisis Formal	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Investigación	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Recursos	**Freddy Roberto Acosta Buenaño**
Curación de datos	**Gabriela Estefanía Onofre Concha <<igual>> Cristian Marcelo Vasco Estupiñan <<igual>>**
Escritura - Preparación del borrador original	**Cristian Marcelo Vasco Estupiñan**
Escritura - Revisión y edición	**Cristian Marcelo Vasco Estupiñan <<principal>> Freddy Roberto Acosta Buenaño <<que apoya>>**
Visualización	**Cristian Marcelo Vasco Estupiñan**

Supervisión	**Freddy Roberto Acosta Buenaño**
Administración de Proyectos	**Freddy Roberto Acosta Buenaño**
Adquisición de fondos	**Cristian Marcelo Vasco Estupiñan <<principal>> Freddy Roberto Acosta Buenaño <<que apoya>> Gabriela Estefanía Onofre Concha <<que apoya>>**