






dx.doi.org/10.17488/RMIB.43.2.5

E-LOCATION ID: 1275

Secure Exchange of Medical Images Via Extended Visual Cryptography

Intercambio Seguro de Imágenes Médicas Mediante Criptografía Visual Extendida

Luis Angel Olvera-Martinez , Manuel Cedillo-Hernandez  , Carlos Adolfo Diaz-Rodriguez ,
Enrique Tonatiuh Jimenez-Borgonio 

Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME), Unidad Culhuacán

ABSTRACT

Medical image security is acquiring its importance to preserve the integrity and confidentiality of information (medical data) from malicious users given its importance in timely and successful diagnosis. In this context, several techniques have been developed to protect medical images, such as encryption, data hiding, image tagging, application of Hash algorithms, etc. This paper proposes a technique to cipher medical images by adding the metadata inside a cover image, based on extended visual cryptography as well as the inclusion of a Hash-like function to verify the integrity of the image and the metadata once they are recovered. The method proposed in this work is implemented using medical images with a grayscale resolution of $[0,4095]$ that is a depth of 12 bits/pixel and color images with 24 bits/pixel depth. Experimental results prove the effectiveness of the proposed method in the task of secure exchange of medical images by allowing higher hiding capability, lower distortion in the visual quality of the image with the hidden medical data, as well as a means to verify the integrity of the sent data, compared to state-of-the-art.

KEYWORDS: DICOM imaging, visual cryptography, information security, circular shifting, least significant bit replacement

RESUMEN

La seguridad de imágenes médicas está incrementando su importancia para preservar la integridad y la confidencialidad de la información (datos médicos), frente a usuarios malintencionados dada su importancia en el diagnóstico oportuno y acertado. En este contexto, se han desarrollado varias técnicas para proteger las imágenes médicas, como el cifrado, la ocultación de datos, el etiquetado de imágenes, la aplicación de algoritmos Hash, etc. Este trabajo propone una técnica para cifrar imágenes médicas añadiendo los metadatos dentro de una imagen de cubierta, basada en la criptografía visual extendida, así como la inclusión de una función tipo Hash para comprobar la integridad de la imagen y los metadatos una vez estos sean recuperados. El método propuesto en este trabajo se implementa utilizando imágenes médicas con una resolución en escala de grises de [0,4095] es decir una profundidad de 12 bits/píxel e imágenes en color con 24 bits/píxel de profundidad. Los resultados experimentales demuestran la eficacia del método propuesto en la tarea de transmisión segura de imágenes médicas permitiendo una mayor capacidad de ocultamiento, una menor distorsión en la calidad visual de la imagen con los datos médicos ocultos, así como un medio para comprobar la integridad de los datos enviados, en comparación con los artículos publicados.

PALABRAS CLAVE: Imágenes DICOM, criptografía visual, seguridad de la información, desplazamiento circular, sustitución de bits menos significativos

Corresponding author

TO: Manuel Cedillo-Hernandez

INSTITUTION: Instituto Politécnico Nacional,
Escuela Superior de Ingeniería Mecánica y Eléctrica
(ESIME), Unidad Culhuacán

ADDRESS: Av. Santa Ana #1000, Col. San Francisco
Culhuacán, Culhuacán CTM V, Del. Coyoacán,
C. P. 04440, Ciudad de México, CDMX, México

CORREO ELECTRÓNICO: mcedilloh@ipn.mx

Received:

4 May 2022

Accepted:

22 July 2022

INTRODUCTION

The Digital Imaging and Communications in Medicine (DICOM) file is a standard^[1] with which sundry medical equipment work to produce digital images. In general terms is the way in which the stewardship of medical files services are defined, including the electronic patient record (EPR). In this context, a DICOM file is composed by a data set of pixels with metadata at the header which relates the image with its respective EPR^{[2] [3] [4] [5]}. In this way, the enhancement in technologies like telecom have leave us the growth of services based on DICOM files for medical images transmission throughout Picture Archiving and Communication Systems (PACS), which is a technology that complies the DICOM standard, also allows the creation of different applications such as telemedicine, the remotely diagnose, among others, opening the possibility of give a better clinical analysis or treatment, in interest of the plan of patient's care. Thus, during its lifetime, a medical image can be transmitted several times inside hospitals, or even, outside of them, however, this scenario can introduce some risks regarding to the management and information security that must be mitigated because medical data are confidential^{[2] [3] [4] [5]}, and the conventional informatics security tools such as antivirus, cryptography tools or firewalls, to name a few, cannot solve all security issues of medical data. In this way, data hiding is a research field that has been widely proposed for improving the management and information security of medical imaging, concealing mainly binary data to create a trustworthy link between these data and the image.

So, it is important to ensure that the internet exchanged images correspond from their original images as a malicious user can modify considerable evidence of a patient's condition when they are sent and change the outcome of the patient's diagnosis as has been demonstrated by Yisroel Mirsky^[6]. He modified 2D and 3D medical images by means of a generative adversarial network (GAN) deep neural network. As result the altered images presented variation in tonalities.

To preserve their integrity, various methods or techniques of cryptography^{[7] [8] [9] [10] [11]}, visual cryptography and visual steganography have been developed, both of which are used to hide or protect the information in the images.

Naor and Shamir^[12], first proposed visual cryptography to allow a user to share information through N shares of the secret image and its use has been extended to several applications^[13], since it represents a simple and computationally uncomplicated way to exchange images. On the other hand, there are several techniques used for steganography of images where the information is hidden exclusively in the images, these techniques can be divided into two groups focused on the spatial or frequency domain^{[14] [15] [16] [17]}.

Cryptography differs from steganography in the sense that cryptography focuses on protecting the content of the information while steganography focuses on hiding the information. Both forms allow us to exchange information securely, however neither is perfect and information can be broken or compromised. There are several researchers who propose to implement both techniques allowing to protect and hide the information of an image to increase the security of conventional methods.

Vinothkanna^[18], proposes to implement RSA cryptography incorporated into steganography for files in multiple formats applied to images, to increase security to common stenographic methods. Thus, provides a highly secure transmission of information, to validate his proposal performs *PSNR* and *SSIM* tests, ensuring the efficiency of the method. On the other hand, Gupta Shailender and Ankur Goya^[19], explain that the use of least significant bit (LSB) as a steganography method, in which the LSB of the image is supersede by a bit of the data, is susceptible to steganalysis. However, encrypting the data and hiding it in an image increases the security of the LSB method, with their proposed method concluded that it leads to an increase in execu-

tion time, but the resulting level of security is worth it. Dhiman and Kasana ^[20], present two visual cryptography techniques, in this process the secret image, the cover image and the resulting image have the same dimensions, the pixels selected from the cover image are replaced by pixels from the secret image, this allows the recovered image is the same as the original image. Back to previous work, Richa and Ashwani ^[21], proposed to expand the cover image to make the embedded pixels as imperceptible as possible, as well as increasing the security of the method by encrypting the pixel values of the secret image (medical image), which makes the recovery process more complex.

Despite the above, there are several methods to improve security and, as mentioned above, steganography, cryptography and hashing by themselves may not solve all issues related with the information security. However, the combination of these techniques could improve security, making it more difficult to retrieve information in an unauthorized way. Therefore, the following system is proposed, which is versatile to implement in real scenarios and allows the system to be secure. Using conventional cryptographic techniques such as circular encryption and steganography techniques by substitution of the least significant bits to increase the security of both methods as proposed by Vinothkanna and Gupta.

Employing pixel replacement as proposed by Dhiman and Richa with the variant of considering a cover image, as well as an increase in information because the hidden image has grayscale bit-depth of 12 bits, averaging the replaced pixels to provide some degree of imperceptibility, and finally adding the metadata and providing a system to verify the integrity of the file received by a hash function.

Motivation and contribution

Although the DICOM file has several security standards, these standards do not guarantee that the information it contains cannot be modified. Nowadays,

visual cryptography has focused on protecting the image of the DICOM file obtaining relevant results; however, these proposals leave aside the information related to the image, therefore, a method is proposed to hide both the medical image and its respective metadata in a color cover image of the patient.

The purpose is to briefly identify the user who owns the medical image, as well to allow the medical image to be hidden within an identification image so that it can be sent as a secure transmission media protecting the integrity of the hidden image. An important contribution is related to the recovered medical image having the same bit depth as the original image, this is because the system allows working with medical images with a bit depth equal to or less than 12 bits regardless of whether the bit depth of the covered image is 24 bits/pixel.

On the other hand, the metadata contains information that may be relevant to whoever performs a study on the image, as it contains both medical information and personal information that may be of use to the medical staff, as well as to ensure again that the retrieved DICOM file belongs to the person who appears in the cover image. Including an ID image as a cover image allows both medical institutions and physicians to verify immediately that the face of the person in the image corresponds to the person receiving the studies or being diagnosed is the same, thus allowing a study-patient linkage.

MATERIALS AND METHODS

The DICOM file hiding process is shown in Figure 1, where the medical image and metadata are separated. The medical image is encrypted by the circular encryption method, two images and a key are obtained. The first image contains the four most significant bits, the second one the eight least significant bits. On the other hand, the cover image is splitted into its RGB channels, to hide the data.

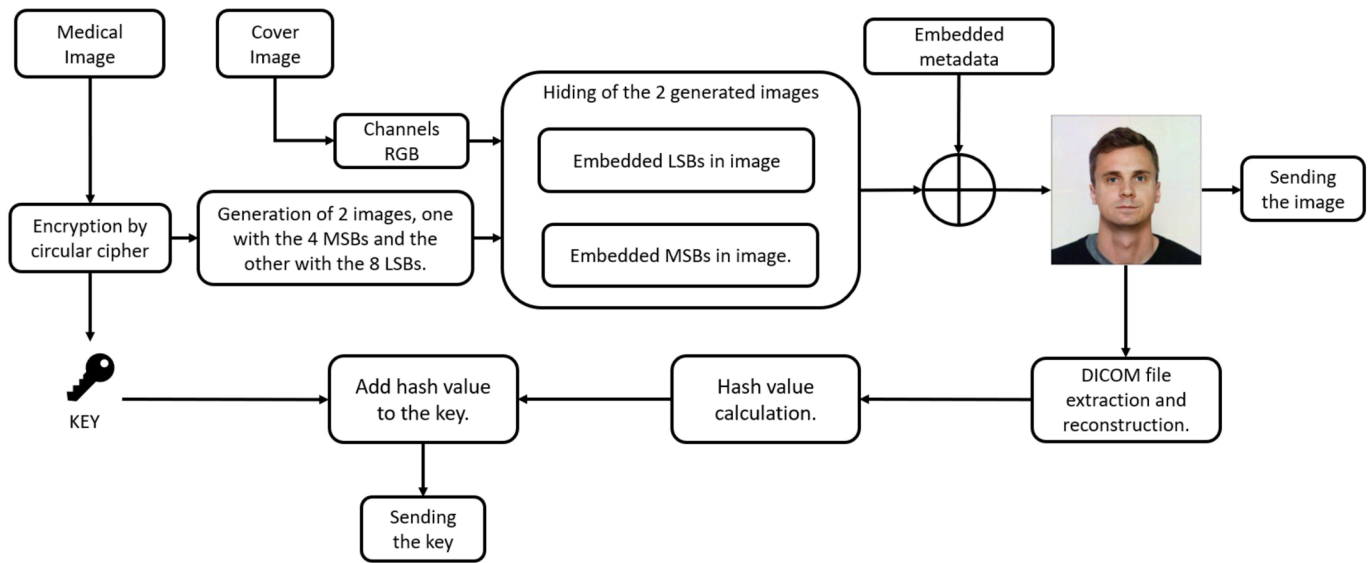


FIGURE 1. DICOM file embedding process.

The obtained two images and the metadata are hidden into the RGB channels of the cover image, resulting in the entire DICOM file embedded into the cover image. To validate the integrity of the DICOM file, it is retrieved to obtain its hash value and add it to the key.

are joined and decrypted, reconstructed DICOM file adding the metadata and then compared with their hash function. The quality of the retrieved medical image is compared with the original, the results are shown in section “Simulation, analysis and results”.

The extraction process shown in Figure 2, retrieves the metadata the Most Significant Bits (MSB's) and Least Significant Bits (LSB's) images. Then, the images

To have a better understanding of the methodology, the following subsections describe in greater detail each stage that makes up the proposal.

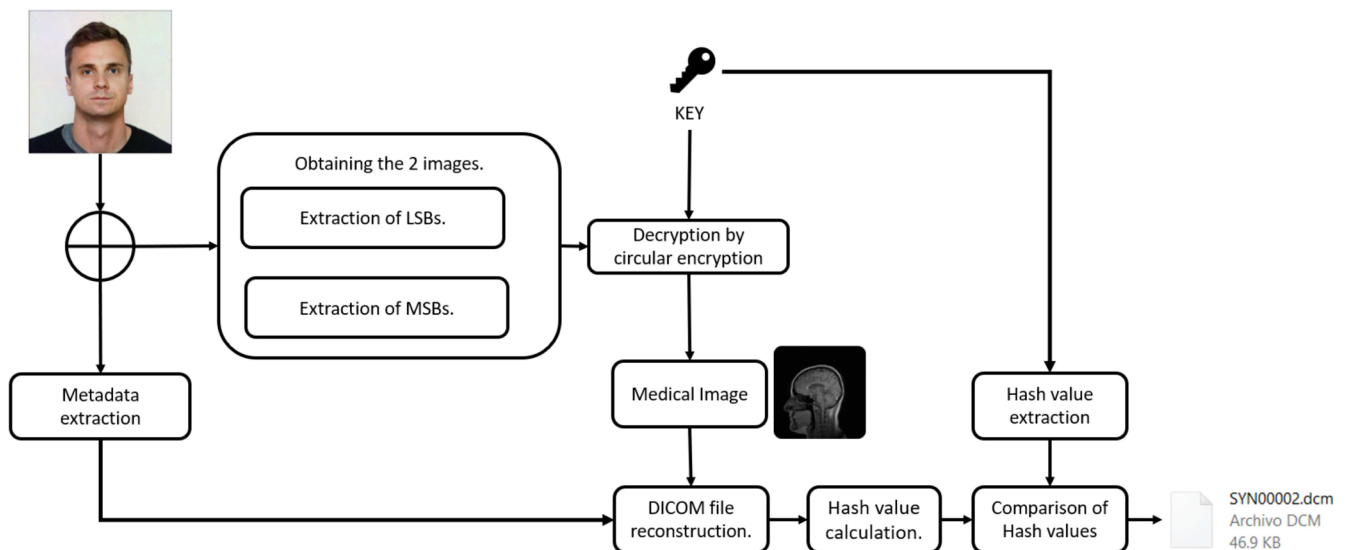


FIGURE 2. DICOM file extraction process

The encryption is described in subsection “Circular shift encryption”. The embedding of image with the remaining most significant bits is described in subsection “Embedded MSBs in cover image” and the least significant bits in subsection “Embedded LSBs in image”, the embedding of metadata information in subsection “Embedded metadata”, obtaining the SHA256 of the resulting DICOM file in subsection “Digital signature”. Finally, the extraction process of medical image and metadata information in subsection “Extraction Procedure”.

Circular shift encryption

The circular Shift Encryption process shifts the columns and rows n positions to right and down respectively [22]. The number of shifts depends on certain values contained on a previously defined key. E.g., assuming a small key, which value is (2,3,0,1) applied to an (5*5) array; the following steps are showed:

1. The first digit (2) performs a circular right shift.
2. The second digit (3) performs a circular down shift.
3. Steps 1 and 2 are looped until completing all digits
4. If the digit is zero, no shift is performed. Show Figure 3.

The key is pre-computed through a series of random numbers stored in a one-dimensional array, the length of the array corresponds to the width of the cover image, and the maximum number stored corresponds to the maximum value of the dimensions of the cover image.

It is important to assume that the maximum depth of the medical image is 12 bits, with the selected image, the circular encryption process is performed. The resulting medical image is converted into two arrays (images) one of 4 bits most significant bits (MSB) and the other of least significant bits (LSB) 8bits.

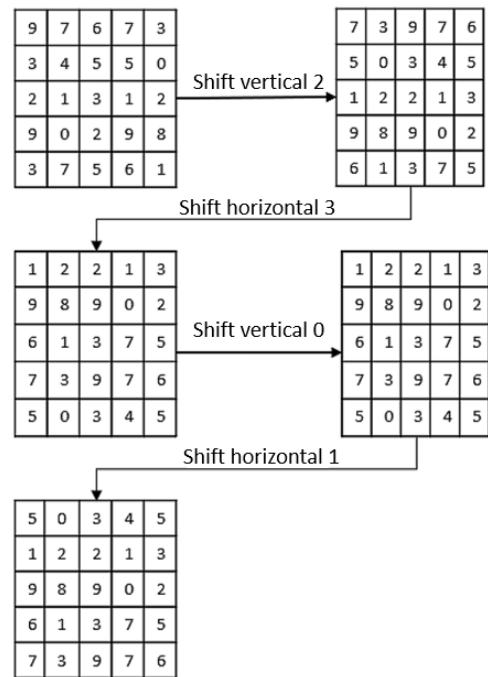


FIGURE 3. Circular Shift Encryption.

Embedded MSBs in cover image

In order to embed an MSB array, we select a 3×3 pixel array of each RGB channel from the cover image. From each RGB arrays, 3 non-deterministic selected pixels will be used to embed the values of the MSB array as shown in Figure 4.

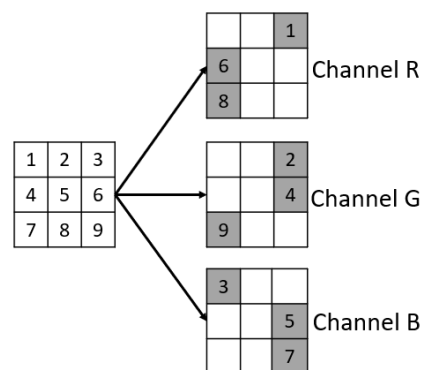


FIGURE 4. Pixel selection in channels RGB.

The pixel values in the MSB group will be embedded by modifying the last 4 bits of the selected pixels in each of the RGB channels, as shown in Figure 5, where the first row of the MSB array was selected and the last 4 bits of the selected pixels in the RGB channels were replaced.

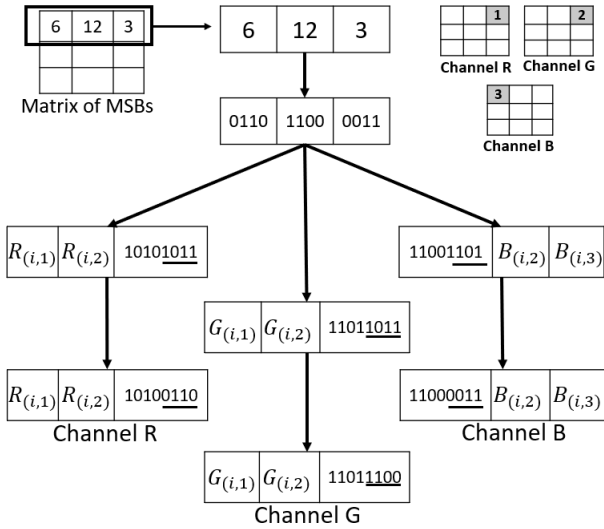


FIGURE 5. Embedded MSBs in channels RGB.

Embedded LSBs in cover image

Same as the MSB embedding process, a 3x3 pixels array is selected for the LSB group. Then 3 non-deterministically selected pixels of each RGB channels, excluding those pixels that were already modified previously, as shown in Figure 6.

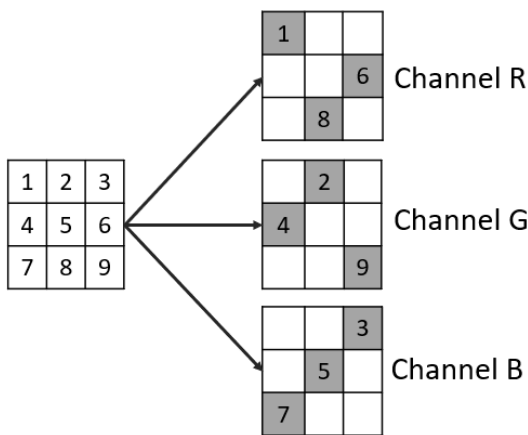


FIGURE 6. Pixel selection in channels RGB.

The values of the LSBs are embedded by replacing them with the value of the selected pixels, then each value inserted is averaged with the neighboring pixels whose values have not been modified. Considering that the embedded LSBs pixels have a value within the

range of 0 to 254, averaging makes the value be imperceptible as well as being in the range of values allowed in the 8-bit cover image, as shown in Figure 7.

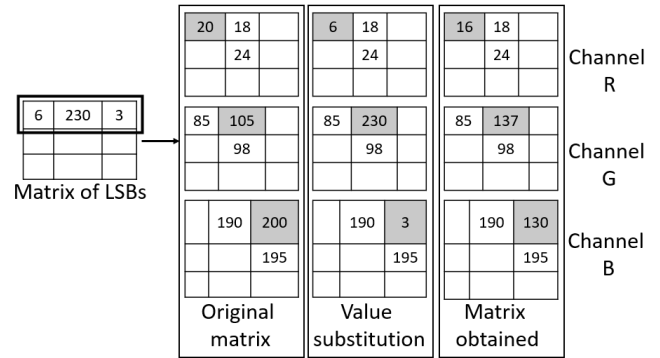


FIGURE 7. Embedded LSBs in channels RGB.

Embedded metadata

The DICOM file's metadata are relevant, since may contain patient ID information, the performed study; the medical equipment used; the medical institution information; image characteristics such as color, model, dimensions, bit resolution, etc. Therefore, it is crucial select the data that may be helpfully for the diagnosis.

For this proposal, selected data include ID data and data on the study performed, to be useful for the physician or medical institution.

Before performing the embedding, first an array of the same medical image dimensions is generated. The $n_i \times m_i$ position of the array will contain the ASCII value of each of the i -th letter information.

To embed the information, two pixels are selected at position n_i, m_j of each of the RGB channels. The selected pixels should not be those whose value has been changed during the embedding process of the medical image.

Each letter has an 8 bits assigned in the ASCII code. Therefore, the process modifies the last 4 bits of the selected pixels in the position n_i, m_j of the cover image.

There must be 2 pixels in the position n_i, m_j whose value had not been modified in the RGB channels, this ensures to hide a letter of the metadata in that position for the RGB channels. Modifying the last 4 bits of the cover image allows to preserve an imperceptibility at the moment of viewing the image.

Digital Signature

After the reconstruction of the DICOM file, it must be verified to make sure that it has not been altered. To verify the information's integrity, it is proposed to use the Secure Hash Algorithm (SHA-256) [23], of the sent file. Once the hash has been calculated, the hash is compared with hash that was received, as is shown in Figure 8.

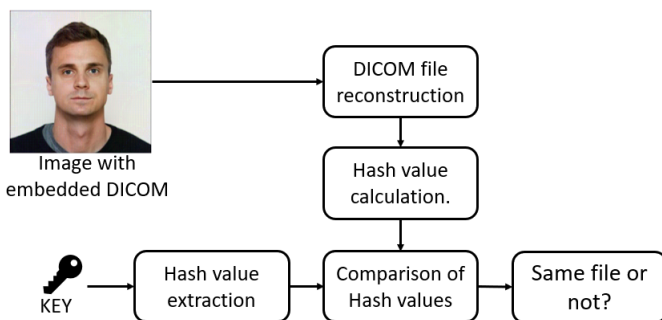


FIGURE 8. Obtaining hash value for validation.

In the process of reconstructing the DICOM file by the receiver, the SHA256 of the received file is recalculated and compared with the signature of the key file.

The objective of this process is to ensure that the reconstructed file was not modified by an external person, if the result of the comparison of both hashes match, it can be concluded that the DICOM file sent and the one obtained by the receiver are the same. In case of a function comparison mismatch, the received file should be discarded, which means that has been altered.

Extraction procedure

Once the cover image is received, the process to reconstruct the DICOM file starts. The steps for the extraction procedure are given below and show in Figure 2.

1. For every cover image's RGB channel, LSBs and MSBs images are extracted.
2. Both images are combined according to the position of the MSBs and LSBs.
3. The resulting image is decrypted with the key.
4. Metadata is extracted from the cover image.
5. The DICOM file is reconstructed with the metadata and the resulting medical image.

RESULTS AND DISCUSSION

The proposed method was tested in MATLAB, in a 16 GB RAM machine and 3Ghz processor. The tests were performed using a set of 10 MRI images consisting of 2 body parts, side view of the head and brain, with a depth of 12 bits or a maximum hue level of 4095. The images in Figure 9, constitute the set of medical images corresponds to a dataset provided by Instituto Mexicano del Seguro Social (IMSS) for research purposes.

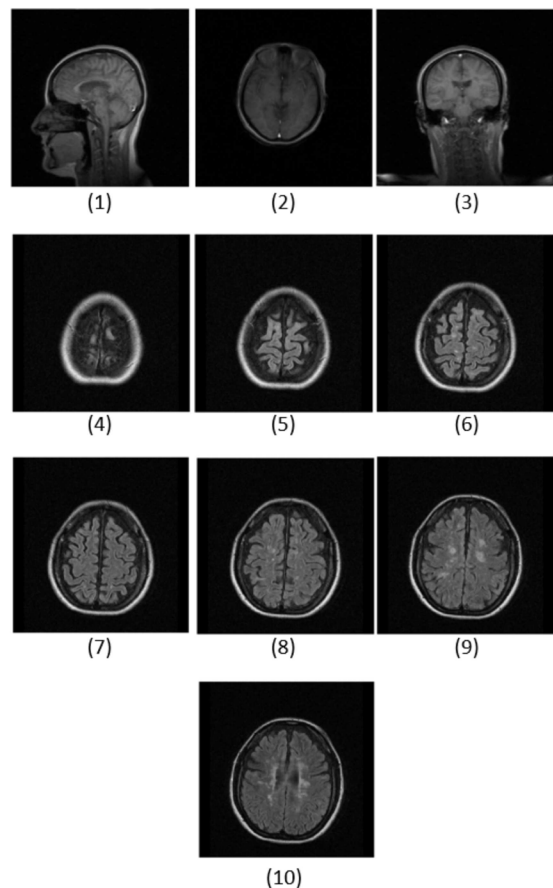


FIGURE 9. DICOM medical images used in the experiment.

On the other hand, the patient identification images used as cover images, have different background colors, clothing, as well as different skin and hair tones, shown in Figure 10 (a). The images used in this process are 255x255.

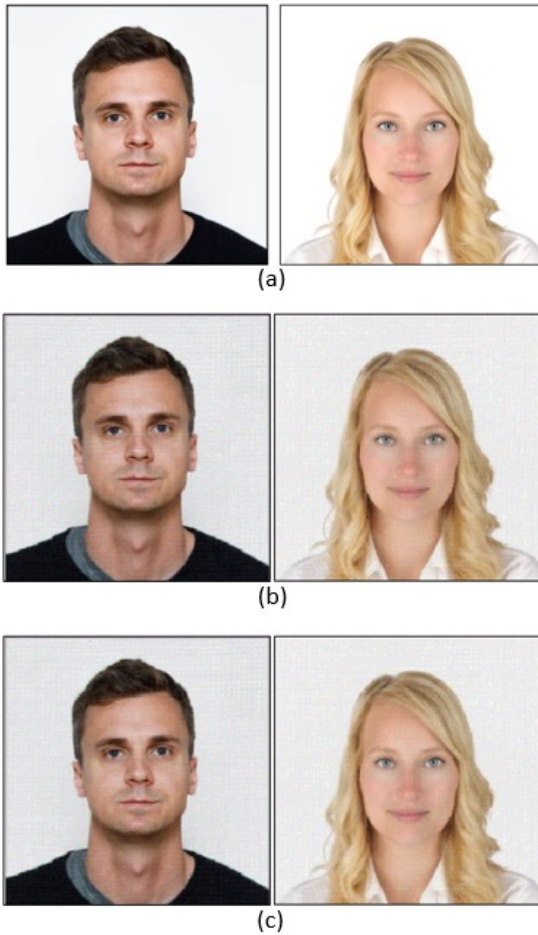


FIGURE 10. (a) Cover images, (b) Resulting cover images with only embedded DICOM image, (c) Resulting cover image with DICOM image and metadata.

The dimensions of the test images are multiples of 3, in case both images are not multiples of 3, both images are analyzed to eliminate those rows and/or columns that contain little or no relevant information in order not to distort both images.

The medical image of dimensions 255x255 with a depth of 12 bits contains approximately 780,300 bits as shown:

$$255 \times 255 \times 12 \text{ Bit depth} = 780,300 \text{ bits} \quad (1)$$

While the color cover image with the same dimensions and a depth of 8 bits in each of the RGB channels contains 1,560,600 bits as shown below:

$$255 \times 255 \times 8 \text{ Bit depth} \times 3(\text{RGB}) = 1,560,600 \text{ bits} \quad (2)$$

It can be concluded that the cover image has the capacity to store the medical image as well as the respective metadata.

From the test DICOM file, the medical image is extracted to begin the image and metadata embedding process, as is described in section “Proposed methodology”. After the encryption, the image is shown in Figure 11.

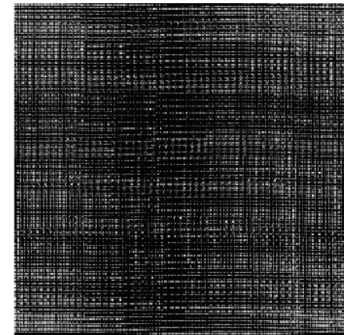


FIGURE 11. Encrypted medical image.

Then is converted to a 12-bit image and splitted into two images with a resolution of 8 bits and 4 bits the resulting images are shown in Figure 12, respectively.

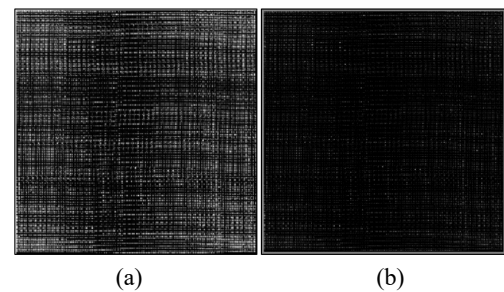


FIGURE 12. (a) Image with the 8 LSBs and (b) image with the 4 MSBs

With both resulting images, the embedding process is performed. Since in the MSB process the values of certain pixels are modified and in the LSB embedding process, the adjacent pixels of which some pixels were previously modified are considered, this order allows the hue level of the recovered pixel be like the original pixel and the changes made in the patient identification image to be less visible. The resulting image of the patient once the embedded process was performed shows in Figure 10 (b).

In the LSB embedding process, it is considered that one third of the cover image will be modified, so calculating the number of bits to be modified, the following result is obtained:

$$1,560,600 \text{ bits} / 3(\text{RGB}) = 520,200 \text{ bits} \quad (3)$$

On the other hand, if we calculate the number of bits contained in the LSB image, we obtain the following result:

$$255 \times 255 \times 8 \text{ Bit depth} = 520,200 \text{ bits} \quad (4)$$

As can be observed, the space available in the cover image coincides with the space used to hide the bits in the LSB image. From the MSB embedding process, if we calculate the number of bits in the MSB image, we obtain the following result:

$$255 \times 255 \times 4 \text{ Bit depth} = 260,100 \text{ bits} \quad (5)$$

Adding the values of (4) and (5) gives the number of bits to be hidden calculated as (1), so there is no loss of bits.

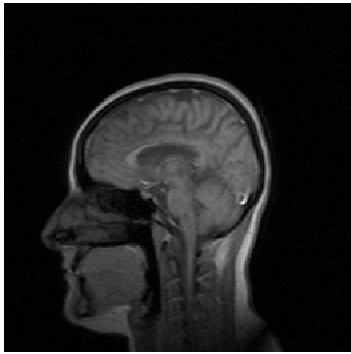
As is previously mentioned, the DICOM formats contain a diverse collection of data from which it will be select the crucial data needed a correct diagnosed, Table 1, shows the selected data in the test DICOM file.

TABLE 1. Selected data.

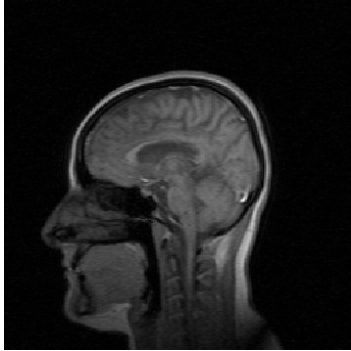
DICOM metadata field	Type
Format	CHAR
Width	INT
Height	INT
Bit Depth	INT
Color Type	CHAR
Study Date	INT
Accession Number	INT
Modality	CHAR
Study Description	CHAR
Code Meaning	CHAR
Resolution Factor	CHAR
Private Creator	CHAR
Manufacturer	INT
Institution Name	INT
Name	CHAR
Last Name	CHAR
Patient ID	INT
Patient Birthday	INT
Patient Sex	CHAR
Image Text	CHAR

With the selected data the array is generated, with $n \times m$ dimensions like the cover image where in the position n_i, m_j it will contain a character, corresponding to the data. Once the array is filled, the data is inserted in the cover image as indicated section “Embedded metadata”. The resulting image is shown in Figure 10 (c). Once the DICOM file embedding process is finished, the resulting image is sent to the receiver, who then extracts the medical image as well as the metadata and reconstructs the DICOM file, calculates its SHA256 value and extracts the one contained in the key, compares both values to verify that the file preserves its integrity and was unmodified during its sending.

After verifying the integrity of the DICOM file, the similarity as also the quality of the recovered image with respect to the original medical image is determined by Peak Signal to Noise Ratio (PSNR) and Similarity Index Metrix (SSIM) tests [24], the original medical image and the recovered image are shown in Figure 13.



(a) Original medical image.



(b) Reconstructed medical image.

FIGURE 13. Original medical image and resulting medical image.

PSNR test is measure of reconstruction quality of an image, if the calculated value for *PSNR* is high or tends to infinity it is concluded that the image recovered quality is similar compared

PSNR calculates the image quality ratio between the signal power and the distorting noise. This ratio is in decibels and the equation is expressed as ^[21]:

$$PSNR = 10 \log\left(\frac{peakval^2}{MSE}\right) \quad (6)$$

From (6) peakval (Peak Value) is the maximum pixel value of the image, if it is an 8-bit image, the maximum value is 255, and MSE is the Mean Square Error defined as follow:

$$MSE = \frac{1}{MN} \sum_{n=0}^M \sum_{m=1}^N [\hat{g}(n, m) - g(n, m)]^2 \quad (7)$$

On the other hand, the *SSIM* ^{[25] [26]} is used to measure the similarity between two images with respect to 3 factors which can be expressed as:

$$SSIM(x, y) = f(l(x, y), c(x, y), s(x, y)) \quad (8)$$

from which:

l is the brightness between two images comparison

c is the contrast distortion, which differs the brightest and darkest ranges

s is the correlation loss, it compares the pattern of local luminance

The luminescence distortion, contrast distortion and correlation loss can be expressed separately as:

$$l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (9)$$

$$c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (10)$$

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (11)$$

If the value of *SSIM* is close to 1 it is concluded that the original image and the recovered image are structurally similar.

The results obtained by implementing the proposed method are shown in Table 2.

TABLE 2. Imperceptibility results.

	PSNR	SSIM
Cover Image 1	94.6233	0.9876
Cover Image 2	94.600	0.9875

The proposed method was applied to the rest of the medical images using only the cover image 1, the *PSNR* and *SSIM* tests were performed, the values obtained are shown in Table 3.

TABLE 3. Visual quality results in terms of *PSNR* and *SSIM*.

DICOM images ID	PSNR	SSIM
1	94.6233	0.9876
2	94.5824	0.9843
3	94.5699	0.9867
4	86.5022	0.9898
5	89.7878	0.9884
6	86.4916	0.9896
7	92.3604	0.9885
8	89.7604	0.9876
9	92.3575	0.9891
10	86.9698	0.9874
Average	90.8005	0.9879
DICOM images ID	PSNR	SSIM

In the same way, Figure 14, shows some results of the tests performed, on the left the original images and on the right the reconstructed images, where at first sight they do not present any alteration now of being recovered by the receiver.

Table 4, compares the *PSNR* obtained from the original medical image and the encrypted image with the results obtained by implementing the proposal of Richa and Ashwani [16]. In this case, a minimum value of *PSNR* is expected since it ensures that the original medical image and the encrypted image are no correlated and as can be appreciated our results obtain lower values, inferring that the correlation between the two images is lower with the results previously published.

Although Richa only evaluates in terms of *PSNR*, based on the contributions presented here, it is possible to have a very detailed comparison of the processes performed, for example, Richa considers medical images with a depth of 8 bits and 3 cover images, expanding them to have a greater hiding capacity. On

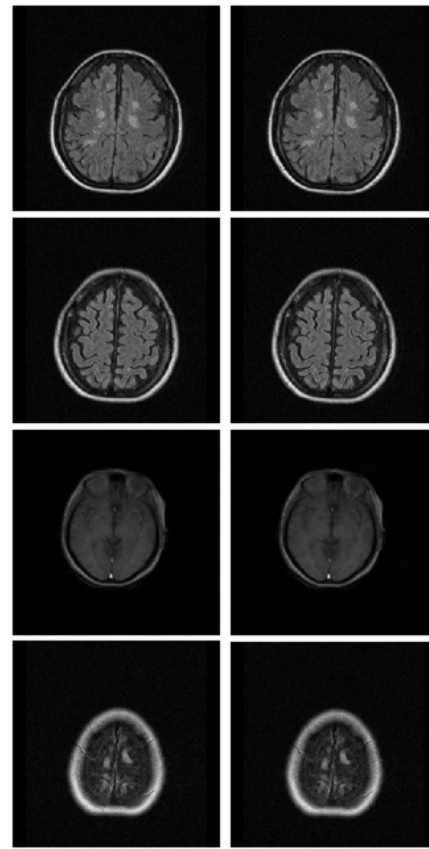


FIGURE 14. Results obtained.

the other hand, the methodology proposed in this paper allows hiding medical images up to a bit depth of 12 bits and adding the metadata, only one cover image is considered without expanding it and finally a way to verify the integrity of the file sent by a HASH function is included, adding value to the results obtained.

TABLE 4. *PSNR* (dB) of original images vs encrypted image.

DICOM Image ID	Proposed method	Richa [21]
1	56.1543	56.4547
2	56.0163	56.2816
3	56.4283	56.6693
4	52.4912	52.6509
5	52.3014	52.4326
6	51.4581	51.5942
7	51.0167	51.2845
8	50.6105	50.8029
9	50.0141	50.1966
10	50.8472	50.9351

CONCLUSIONS

The proposal provides a way to embed a medical image, as well as its respective metadata in the RGB channels in an identification patient's image. Allowing medical institutions securely share the DICOM file to preserve its integrity. For this purpose, stenographic and cryptographic techniques were combined, which proves to increase the security of conventional methods as supported in the previous research, making tough the information retrieval by malicious users.

On the other hand, the proposed method allows working with medical images with a bit-depth of more than 8 bits/pixel and incorporates the metadata, allowing a greater capacity to hide data within the color image, compared to the methods already proposed, because these methods only work with medical images with a bit-depth of 8 bits/pixel and without considering the metadata hiding.

The fact of using an ID image allows the medical institutions in responsible for delivering and evaluating the medical images to verify at a naked eye that the face of the person in the ID image corresponds to the actual patient receiving the studies, thus allowing the study-patient linkage.

Finally, experimental results prove that the proposed methodology allows the resulting image (ID image with the hidden medical data) in comparison with the original image, to have changes in tonalities that are the least perceptible to the human eye, in addition to

providing an outstanding level of medical image recovery in terms of visual quality and similarity as demonstrated in the resulting *PSNR* and *SSIM* tests.

As part of future work this methodology is proposed to be applied to other color models to increase the level of security and to make it more difficult to obtain the data embedded in the cover image as well as to improve the resulting visual quality. On the other hand, it is considered to implement it in other medical imaging modalities as well as its application to 3D medical imaging.

AUTHOR CONTRIBUTIONS

L.A.O.M. conceptualized the project, participated in the use of specialized software and developed the methodology, carried out research, formal analysis and visualization, participated in the writing of the manuscript. M.C.H. conceptualized the project, developed the methodology, participated in validation of data and/or results and data curation, carried out formal analysis and visualization, contributed providing resources and funding, oversaw the project. E.T.J.B. conceptualized the project, participated in the use of specialized software, and carried out research and visualization. C.A.D.R. conceptualized the project, participated in the development and implementation of the methodology, carried out formal analysis and data validation, carried out visualization, oversaw the project, participated in the writing, editing, and reviewing of the original manuscript. All authors reviewed and approved the final version of the manuscript.

REFERENCES

- [1] National Electrical Manufacturers Association. DICOM Security [Internet]. DICOM Digital Imaging and Communication in Medicine; 2019. Available from: <https://www.dicomstandard.org/using/security>
- [2] Coatrieux G, Quantin C, Montagner J, Fassa M, et al. Watermarking medical images with anonymous patient identification to verify authenticity. *Stud Health Technol Inform* [Internet]. 2008;136:667-672. Available from: <https://pubmed.ncbi.nlm.nih.gov/18487808/>
- [3] Qasim AF, Meziane F, Aspin R. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Comput Sci Rev* [Internet]. 2018;27:45-60. Available from: <https://doi.org/10.1016/j.cosrev.2017.11.003>
- [4] Mousavi SM, Naghsh A, Abu-Bakar SAR. Watermarking Techniques used in Medical Images: a Survey. *J Digit Imaging* [Internet]. 2014;27(6):714-729. Available from: <https://doi.org/10.1007/s10278-014-9700-5>
- [5] Cedillo-Hernandez M, Cedillo-Hernandez A, Nakano-Miyake M, Perez-Meana H. Improving the management of medical imaging by using robust and secure dual watermarking. *Biomed Signal Process Control* [Internet]. 2020;56:101695. Available from: <https://doi.org/10.1016/j.bspc.2019.101695>
- [6] Mirsky Y, Mahler T, Shelef I, Elovici Y. CT-GAN: malicious tampering of 3D medical imagery using deep learning. In: *Proceedings of the 28th USENIX Conference on Security Symposium* [Internet]. Santa Clara, CA; 2019:461-478. Available from: <https://doi.org/10.48550/arXiv.1901.03597>
- [7] Stallings W. *Cryptography and network security: Principles and practice* [Internet]. New York: Prentice Hall; 2011. 719p. Available from: <http://pozi.omsu.ru/docs/docs/stallings.pdf>
- [8] Medina Velandia LN. *Criptografía y mecanismos de seguridad* [Internet]. Bogotá: Fundación Universitaria del Área Andina; 2017. 141p. Available from: <https://digitk.areandina.edu.co/handle/areandina/1423>
- [9] Blackledge J, Bezobrazov S, Tobin P, Zamora F. Cryptography using evolutionary computing. In: *24th IET Irish Signals and Systems Conference (ISSC 2013)* [Internet]. Letterkenny: Institution of Engineering and Technology; 2013:1-8. Available from: <https://doi.org/10.1049/ic.2013.0029>
- [10] Diffie W, Hellman M. New directions in cryptography. *Secure communications and asymmetric cryptosystems*. *IEEE Trans Inf Theory* [Internet]. 1976;22(6):644-654. Available from: <https://doi.org/10.1109/TIT.1976.1055638>
- [11] Menezes AJ, van Oorschot PC, Vanstone SA. *Handbook of Applied Cryptography* [Internet]. Boca Raton: CRC press; 2018. 810p. Available from: <https://doi.org/10.1201/9780429466335>
- [12] Naor M, Shamir A. Visual cryptography. In: De Santis A (eds). *EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science, vol 950* [Internet]. Berlin: Springer; 1994:1-12. Available from: <https://doi.org/10.1007/BFb0053419>
- [13] Olvera-Martinez L, Jimenez-Borgonio T, Frias-Carmona T, Abarca-Rodríguez M, et al. First SN P visual cryptographic circuit with astrocyte control of structural plasticity for security applications. *Neurocomputing* [Internet]. 2021;457(7):67-73. Available from: <https://doi.org/10.1016/j.neucom.2021.05.057>
- [14] Morkel T, Eloff J, Olivier M. An overview of image steganography. In: Eloff JHP, Labuschagne L, Eloff MM, Venter HS (eds). *Proceedings of the ISSA 2005 New Knowledge Today Conference* [Internet]. Pretoria: ISSA; 2005. 1-11p. Available from: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/098_Article.pdf
- [15] Cox IJ, Pakura G, Sheel M. Information Transmission and Steganography. In: Barni M, Cox I, Kalker T, Kim HJ (eds). *Digital Watermarking. IWDW 2005. Lecture Notes in Computer Science, vol 3710* [Internet]. Siena, Italy: Springer; 2005. 15-17. Available from: https://doi.org/10.1007/11551492_2
- [16] Wu X, Qiao T, et al. Sign steganography revisited with robust domain selection. *Signal Process* [Internet]. 2022;196:108522. Available from: <https://doi.org/10.1016/j.sigpro.2022.108522>
- [17] Yousefi Valandar M, et al. A chaotic video steganography technique for carrying different types of secret messages. *J Inf Secur Appl* [Internet]. 2022;66:103160. Available from: <https://doi.org/10.1016/j.jisa.2022.103160>
- [18] Vinothkanna R. A secure steganography creation algorithm for multiple file formats. *J Innov Image Process* [Internet]. 2019;1(01):20-30. Available from: <https://doi.org/10.36548/jiip.2019.1.003>
- [19] Gupta A, Goyal A, Bhushan B. Information Hiding Using Least Significant Bit Steganography and Cryptography. *Int J Mod Educ Comput Sci* [Internet]. 2012;4(6):27-34. Available from: <https://doi.org/10.5815/ijmecs.2012.06.04>
- [20] Dhiman K, Kasana SS. Extended visual cryptography techniques for true color images. *Comput Electr Eng* [Internet]. 2018;70:647-658. Available from: <https://doi.org/10.1016/j.compeleceng.2017.09.017>
- [21] Maurya R, Kannojiya AK, Rajitha B. An Extended Visual Cryptography Technique for Medical Image Security. In: *2020 2nd Int Conf on Innov Mech for Ind App (ICIMIA)* [Internet]. Bangalore, India: IEEE; 2020: 415-421. Available from: <https://doi.org/10.1109/ICIMIA48430.2020.9074910>
- [22] Omari AH, Al-Kasasbeh BM, Al-Qutaish RE, Muhairat MI. A new cryptographic algorithm for the real time applications. In: Zaharim A, Mastorakis N, Gonos I (eds). *Proceedings of the 7th WSEAS international conference on Information security and privacy* [Internet]. Cairo, Egypt; World Scientific and Engineering Academy and Society (WSEAS). 2008: 33-38. Available from: <https://dl.acm.org/doi/10.5555/1576645.1576651>
- [23] Schneier B. *Applied Cryptography* [Internet]. Indianapolis: John Wiley & Sons; 1996. 784p. Available from: <https://www.schneier.com/books/applied-cryptography/>
- [24] Horé A, Ziou D. Image Quality Metrics: PSNR vs. SSIM. *20th Int Conf on Pat Rec* [Internet]. Istanbul, Turkey; IEEE. 2010: 2366-2369. Available from: <https://doi.org/10.1109/ICPR.2010.579>
- [25] Sara U, Akter M, Uddin MS. Image Quality Assessment through FSIM, SSIM, MSE and PSNR-A Comparative Study. *J Comput Commun* [Internet]. 2019;7(3):8-18. Available from: <https://doi.org/10.4236/jcc.2019.73002>
- [26] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. *IEEE Trans Image Process* [Internet]. 2004;13(4):600-612. Available from: <https://doi.org/10.1109/TIP.2003.819861>