

# Crypto-steganographic model using chaos and coding based in deoxyribonucleic acid

Edison Andrés López Torres, Deicy Alvarado-Nieto, Isabel Amaya-Barrera,  
César Augusto Suárez Parra

Systems Engineering, Faculty of Engineering, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia

## Article Info

### Article history:

Received Dec 7, 2023

Revised Mar 22, 2024

Accepted Apr 2, 2024

### Keywords:

Chaotic attractor

Cryptography

DNA coding

Edge detection

Steganography

## ABSTRACT

Given the increase of information circulating through public channels, it is essential to create robust schemes to ensure the security of such information. The results presented here were part of the research project entitled computer security models based on mathematical tools and artificial intelligence. An algorithm focused on the encryption of images carrying steganographed texts is proposed, using chaos, artificial vision and coding based in deoxyribonucleic acid (DNA). The process consists of steganographic and cryptographic steps. In the steganographic stage, a color image was taken, the combined Canny and Sobel filters were applied to achieve its dilated edges, using Chen's chaotic attractor, the positions of the edges were selected, to hide a text in binary ASCII code using the least significant bit technique. In the encryption stage, Chen's chaotic system was used to permute the stego-image and to create a chaotic image used in the diffusion process. These two images were divided into blocks represented in DNA coding, selecting the rule to apply through the three-dimensional Logistics system, and finally applying the XOR operation by layers, obtaining a single encrypted image. To validate the proposed model, safety and performance tests were applied, obtaining comparable indicators with some current scientific references.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Deicy Alvarado-Nieto

Systems Engineering, Faculty of Engineering, Universidad Distrital Francisco José de Caldas

Bogotá, Colombia

Email: lalvarado@udistrital.edu.co

## 1. INTRODUCTION

With the advancement of technology, the amount of information circulating on the internet increases every day and so do the attacks of unauthorized individuals, trying to capture such information and take advantage of it as much as possible. Traditional information protection mechanisms are based on the prime factorization of large numbers because the computational time required to calculate them has been notably large so far. However, the emergence of more powerful computing devices, especially quantum computing, dramatically reduces the required computational time, which will increasingly facilitate the work of attackers, thus generating new challenges related to the protection of the integrity and confidentiality of information transmitted through public channels. In this context, cryptographic and steganographic algorithms contribute to ensuring that data is secure enough. In recent decades, new cryptographic and steganographic trends have emerged, incorporating tools from artificial intelligence and mathematics, such is the case of the work of [1]–[15] involving the use of quaternions, cellular automata, chaotic systems, genetic algorithms, neural networks, and deoxyribonucleic acid (DNA) encoding.

In the present article, steganography and cryptography are combined to design an algorithm focused on protecting text messages. The approach involves concealing messages within dilated edges (using Canny and Sobel techniques) of an image. Simultaneously, a chaotic image is generated using the Chen chaotic map for the permutation phase. Additionally, the logistic map is iterated to obtain a pseudo-random sequence contributing to the selection of DNA coding rules applied in the diffusion process. Subsequently, an XOR operation is performed between the permuted encoded image and the chaotic encoded image, thus obtaining the encrypted image to be sent to the receiver together with the chaotic image that plays the role of public key. The sender specifies the initial conditions and parameter values for the mentioned chaotic maps. The main contribution of this work lies in the combination of elements from various scientific references, consolidating a new steganographic cryptosystem that addresses challenges arising from technological advancements. This contribution aims to explore new mathematical strategies in creating robust schemes, a challenge that has become increasingly popular in recent decades. To validate this crypto-steganographic proposal, security and performance tests were carried out, yielding results that indicate a good performance of the algorithm compared to some current references with similar approaches.

The organization of the remaining content of this document is as follows: in section 2, related works are presented. Section 3 details the theoretical foundations. Section 4 details the method carried out to consolidate the crypto-steganographic model. Section 5 addresses the security and performance tests of the system. Finally, in section 6, the conclusions are presented.

## 2. RELATED WORK

Setiadi [10] describe a steganography technique whose purpose is to increase the useful space in the edge areas of an image through a hybrid between Canny and Sobel filters. This involves dilating the three most significant bits of the pixels and applying the least significant bit technique to embed messages. According to the tests performed by the authors, it is evident that they succeeded in increasing the payload capacity of the edges, thereby improving the imperceptibility quality in the stego-image. Likewise, the steganographic model allows the receiver to extract the original message without the need to reconstruct the original edges of the cover image.

The proposal put forward by Niyat and Moattar [16] describes a model for image encryption using the chaotic systems of Chen and three-dimensional logistics to permute the images. This process is complemented by DNA coding rules, which are selected from a pseudo-random sequence obtained through the logistic attractor. Chen's system is used to generate a chaotic image used in the permutation process and to create a key chain that becomes a chaotic image, which contributes to increase the encryption speed of his algorithm. Once the permuted and chaotic images are obtained, they are divided into blocks, which are encoded using DNA rules and then combined to obtain the encrypted image. The authors state that this model is resistant to different attacks and the entropy values are close to the ideal. Furthermore, through DNA coding rules, they achieve increased diffusion and robustness of the cryptographic model.

On the other hand, Chai *et al.* [17], report a cryptosystem for color images based on DNA code, chaos, and an external secret key of 384 bits generated by the SHA-384 hash function of the original image. This key is used to define the parameters and initial conditions of a 4-dimensional hyperchaotic attractor. To achieve this, the authors separate the image into its red, green, and blue (RGB) components and perform permutation in each layer, using the chaotic sequence. They then do the same between the components; once permuted, they are recombined into a matrix through DNA coding, which is then permuted again and subjected to a second confusion scheme, resulting in the encrypted color image. The authors claim that the algorithm is highly sensitive to small perturbations in any of the input data and can resist different attacks, especially plaintext attacks.

Likewise, steganography has been combined with cryptography to achieve better results, as exemplified in the work of Phadte and Dhanaraj [11]. In this work, the authors conceal one image within two others, and then the resulting images are encrypted using chaotic systems. Based on the previous references, a steganographic cryptosystem was designed, which also involves dilating the edges of the carrier image. This approach succeeded in improving certain security and performance indicators compared to the cited references.

## 3. BACKGROUND

### 3.1. Cryptography

New forms of communication continuously drive the development of cryptographic algorithms because it is essential to ensure the secure transmission of information, implying the ensuring of confidentiality and integrity. The objective of cryptography is to design strategies to render private information

unintelligible, preventing unauthorized individuals from fraudulently accessing such information. Information security is associated with two conditions: the robustness of cryptographic technology and the secrecy of the key.

Throughout history, several cryptographic schemes have been proposed, however, contemporary conventional schemes are slow, complex, consume a lot of energy when dealing with systems with limited resources and are not appropriate for encrypting large information such as images, videos and audios. This has prompted the scientific community to invest efforts in the search and design of new lightweight algorithms [2]. Therefore, in recent decades, new cryptographic algorithms based on the use of mathematical and artificial intelligence elements, such as chaotic attractors, neural networks, cellular automata, and DNA encoding, have been reported. According to security and performance tests, these tools indicate that they are a viable and effective alternative for proposing cryptographic schemes aimed at maintaining the security of large-sized information [1], [12], [16]–[18].

### 3.2. Chaotic attractors

Chaotic attractors arise from strange behaviors in some mathematical models that describe a dynamic system, generating patterns framed within chaos theory. In recent decades, dynamic systems exhibiting chaotic behavior have been used as a strategy to obtain pseudo-random sequences, which are employed in the context of information security. This, in turn, has spurred the proposal of new chaotic attractors, aiming to increase the level of complexity to ensure greater randomness. One advantage of pseudo-random sequences derived from chaotic functions is that the correlation between two consecutive iterations is close to zero, making them suitable for use in the confusion and diffusion processes of cryptographic schemes [1], [4], [12], [17]. In this work we particularly employed the Chen chaotic and three-dimensional logistic systems, which are described by (1) and (2) respectively [16].

$$\begin{aligned} \dot{x} &= a(y - x); \\ \dot{y} &= (c - s)x - xz + cy; \\ \dot{z} &= xy - bz \end{aligned} \quad (1)$$

where  $a$ ,  $b$  and  $c$  are the parameters of the system, which has chaotic behavior for  $a = 35$ ,  $b = 3$   $y$   $c \in [20, 28.4]$ .

$$\begin{aligned} x_{i+1} &= [\lambda \times k_1 \times y_i \times (1 - x_i) + z_i] \text{ mod } 1 \\ y_{i+1} &= \left[ \lambda \times k_2 \times y_i + z_i \times \left( \frac{1}{1 + x_{i+1}^2} \right) \right] \text{ mod } 1 \\ z_{i+1} &= [\lambda \times (x_{i+1} + y_{i+1} + k_3) \times \sin(z_i)] \text{ mod } 1 \end{aligned} \quad (2)$$

In this case the system is chaotic if  $0 < \lambda \leq 3.999$ ,  $|k_1| > 33.5$ ,  $|k_2| > 37.9$ ,  $|k_3| > 35.7$

### 3.3. Steganography

It is a mechanism to hide information in carrier media, avoiding arousing suspicion. Throughout history, carriers and techniques have evolved, and currently, carriers like images, videos, or audios are often used. This is because they provide ample space for hiding information. One of the most commonly used techniques is the least significant bit (LSB) method. However, this technique has limitations, such as being susceptible to intentional attacks or, in the case of audio, causing acoustic disturbances and consequently data loss [2], [3], [6], [8], [10].

### 3.4. Edge detection

To identify the edges of an image, it is necessary to find the points where there are strong changes in color intensity on any of its layers (red, green or blue). However, it is more common to use grayscale images in this process. Although some information is lost compared to color images, grayscale images are much more robust to variations in light. Therefore, changes in gray intensity can be easily identified, facilitating the clear delineation of the contours of objects in the image [10], [19], [20].

There are several types of algorithms for edge detection, including those that approximate the first derivative through convolution with linear filters of one or two dimensions, those that approximate the second derivative using finite differences, those that use cellular automata, those based on multi-scale features, and those using deep learning [21]. In this case, the first ones were used with a two-dimensional filter, in the approximation to the first derivative the maximum variation of the image is determined. Some of these algorithms can be consulted in [22], [23].

In general, linear filters aim to, when applied to the original image, obtain an approximation to the first derivative through the convolution operation, which is calculated for each entry in the matrix [24], [25]. It should be noted that the filters (kernels) are applied by moving them in the vertical and horizontal directions.

Subsequently, they are unified, and a thresholding is defined (post-processing operator). Some of these two-dimensional filters used for edge detection include Roberts, Prewitt, Sobel, and Canny [19], [26], [27].

Currently, new algorithms continue to be generated, aiming for more precise results in edge detection. Several of these algorithms may be a combination of existing ones, referred to as hybrid filters, to complement each other and minimize weaknesses regarding parameters like noise. Additionally, depending on the objective, once the edges are defined, it is possible to expand them by adding another pixel to each original pixel, either to the right, left, up, or down. This process is known as edge dilation [8], [9].

### 3.5. DNA coding

Deoxyribonucleic acid (DNA) is a component present in all living organisms, storing genetic information unique to each organism. Genes are responsible for producing proteins through transcription processes, where the DNA code is converted into ribonucleic acid (RNA). Both DNA and RNA consist of many small subunits called nucleotides, which are composed of a sugar molecule linked to a phosphate group and one of the four types of nucleotide bases: adenine (A), guanine (G), cytosine (C), and thymine (T). In the case of RNA, thymine is replaced by uracil (U).

In the field of information encryption, different techniques have been proposed, such as those using keys or hash algorithms. With the advancement of computer security, those interested in illicitly obtaining data by attacking communication channels have also strengthened their mechanisms. For this reason, the scientific community has been exploring alternatives to encrypt information. It is in this scenario that the use of bio-inspired techniques and/or algorithms is gaining more and more traction [16].

## 4. METHOD

The model presented in this work integrates the use of the following tools: chaotic attractors, DNA encoding, and edge detection in images. In order to facilitate the understanding of this model, two macro-stages were considered, namely: steganography and cryptography. The steps carried out in each of these macro-stages are described in detail below.

### 4.1. Steganographic process

The steganographic process employed uses the LSB technique to conceal text bits within the edges of an image. To expand the available edge space, a hybrid of Canny and Sobel filters was applied to each of the RGB layers belonging to the image. To ensure randomness, the edge positions where the bits will be hidden are selected using Chen's chaotic attractor.

- From an RGB scale image, the layers are separated, and the corresponding three numeric matrices are obtained. On each entry of these matrices, the 5 least significant bits are set to zero.
- Canny and Sobel filters are applied for edge detection on each of the RGB layers, resulting in 6 matrices, two for each layer. Every two matrices of the same color are combined through the OR operation, yielding 3 matrices. To expand the available space for hiding information, dilation is performed on each layer following the scheme proposed in [10].
- The positions of the obtained edges are stored using 3 arrays, one for each RGB layer.
- The text message to be hidden in the carrier image is converted to ASCII code and then binarized.
- Both the layer and the pixels of the dilated edges in which the text will be hidden are randomly selected by means of Chen's chaotic attractor.
- With each bit of the text to be hidden, XOR operation is performed using the least significant bit technique with the selected pixels from the previous step.

The resulting matrices are concatenated, giving rise to the stego-image.

### 4.2. Cryptographic process

Once the steganographed image is obtained, the cryptographic process is carried out. For this purpose, it is necessary to create another image formed by the results of iterating the Chen's chaotic attractor. Both images are divided into blocks and represented in DNA encoding by means of a rule selected using the iterations of the three-dimensional logistic attractor. Finally, each layer of the encrypted stego-image is obtained by combining the permuted stego-image and the chaotic image.

- New initial conditions of Chen's attractor are defined, based on values from the stego-image, in order to iterate it and obtain three pseudo-random sequences, one for each system component, from which a chaotic image is constructed and used to permute the stego-image.
- For an image of size  $M \times N$ , one-dimensional vectors are created for each layer, which are later permuted using the sequences from the Chen attractor.

- From the chaotic and permuted images, blocks of 8×8 pixels are created and encoded using 8 DNA rules [16]. The selection of the rule to use is defined by a pseudo-random sequence obtained from the three-dimensional logistic map (2) with parameters and initial conditions:  $\lambda = 3.7636$ ,  $k_1 = 35.9077$ ,  $k_2 = 41.8863$ ,  $k_3 = 45.2156$ ,  $x_0 = 0.1613$ ,  $y_0 = 0.3385$ ,  $z_0 = 0.8049$ .
- The encrypted image is constructed by performing XOR operation between the encoded blocks of the permuted image and the chaotic image.
- The developed algorithm was implemented in MATLAB and receives three inputs from the user: i) The color image in PNG, JPEG, or TIFF format; ii) The plaintext file with a .txt extension containing the text to be encrypted; and iii) Configuration parameters for the chaotic systems to be used, which configure the private key for the algorithm.

The output of the algorithm is the encrypted image, which internally contains the hidden text and the chaotic image, which takes the role of public key. The receiver, on the other hand, must enter the encrypted image, chaotic image, and the private key into the decryption algorithm to recover the original message. Figures 1(a) and 1(b) summarize the steganographic and cryptographic processes respectively, of the algorithm proposed in this paper.

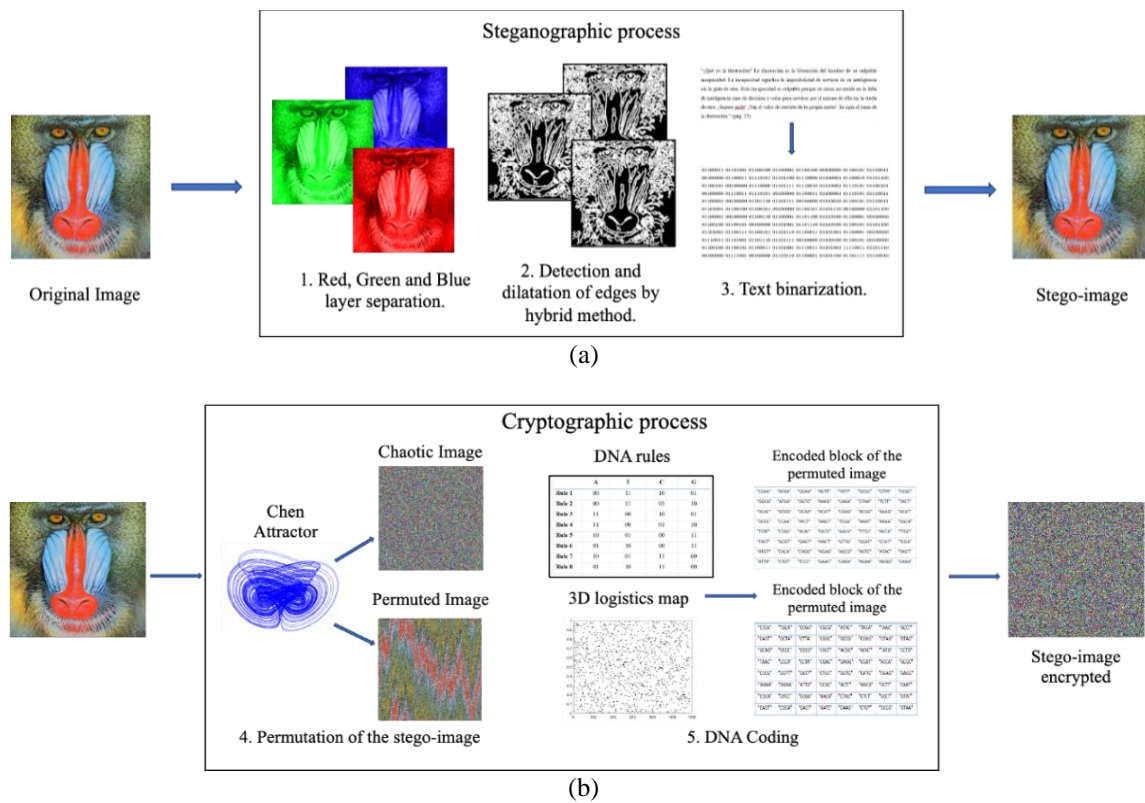


Figure 1. Stages of the proposed algorithm (a) Steganographic process and (b) Cryptographic process. Source: Own elaboration

### 5. RESULTS AND DISCUSSION

The proposed algorithm and the corresponding tests to evaluate its behavior in terms of security and performance were implemented using MATLAB R2022a, for which the images "Baboon", "Lena", "Peppers" and "F16" [28] were used in order to compare the results with various investigations presented following similar approaches. The tests were conducted on a laptop computer with Intel Core i7 vPro processor, 2.50 GHz CPU, 32 Gb RAM and 512 Gb NVMe m.2 SSD disk with Windows 10 Pro-Enterprise operating system. To validate the proposed algorithm, several security and performance indicators were considered. The indicators considered were: frequency histogram, correlation analysis, mean square error (MSE), peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), feature similarity index (FSIM), embedding capacity (bpp), pixel change rate (NPCR), unified average change intensity (UACI), and Shannon entropy. The obtained results, along with their interpretation, are described below.

Figure 2 corresponds to the layer-wise histograms of the original image in Figures 2(a), 2(b), and 2(c), stego-image in Figures 2(d), 2(e), and 2(f), and encrypted image in Figures 2(g), 2(h), and 2(i) of the Baboon. As observed, the difference between the histograms of the original image and the stego-image is imperceptible to the human eye. On the other hand, images in Figures 2(g), 2(h), and 2(i) exhibit high uniformity in the frequency distribution after the encryption process, a situation reaffirmed by the correlation diagrams presented in Figure 3 in which it is highlighted that for the original image of the “Baboon”, the evaluation graphs Figures 3(a), 3(b), and 3(c) for each color component show a high clustering on the diagonal, while in Figures 3(d), 3(e), and 3(f) which corresponds to the evaluation in the encrypted image, the distribution is homogeneous, indicating that the algorithm presents resistance to statistical attacks.

In order to contrast the results with other references in the literature and given that none of them consider all the indicators evaluated in this work, it was necessary to make comparisons with different sources to cover all indicators. Tables 1 and 2 show the comparison of the MSE, PSNR, SSIM, and FSIM indicators, considering the Baboon image as the carrier. Specifically, Table 1 presents these indicators for a 1024-bit message and an embedding capacity (bpp) corresponding to 0.0039.

It is worth noting that in the proposed algorithm, the similarity index between the carrier image and the stego-image is 1, which aligns with the expected ideal. Additionally, the mean squared error is significantly lower compared to the values reported in other references. Similarly, the obtained PSNR value is higher than 45, a desirable situation within the reported security standards [2]. Table 2 shows the same indicators for a message of 8192 bits and an embedding capacity (bpp) corresponding to 0.313.

It is worth noting that in this proposal, although the size of the text increases, the similarity index between the carrier image and the stego-image remains constant, unlike the other contrasted sources. Similarly, the mean squared error is significantly lower than those reported in the works considered as references. On the other hand, regarding the NPCR and UACI indicators, the results obtained within this work were also compared with some sources. Table 3 summarizes these results using, in this case, the image known as Lena.

As observed, the results obtained are comparable to those reported in the references considered. Similarly, as with the previous indicators, the Shannon entropy was calculated and compared with other references. Table 4 shows the results obtained for the case of the Lena image. According to the sources considered for comparing entropy, it is worth noting that the values obtained within this work are very close to those reported in those sources, and also quite close to 8, a situation consistent with the safety standards established by the scientific literature.

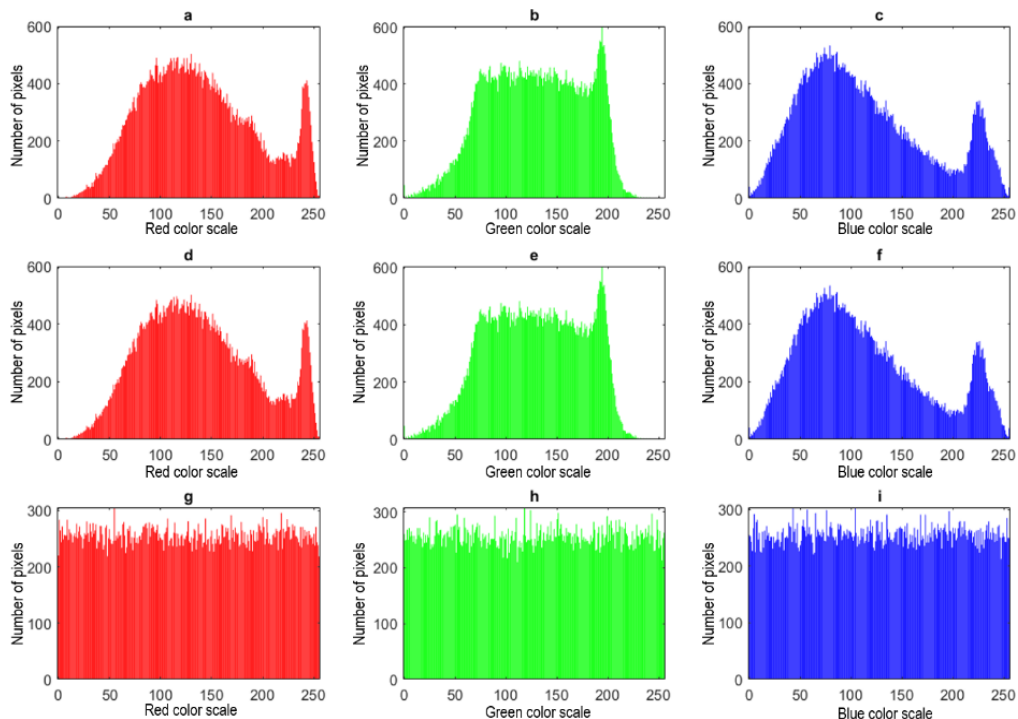


Figure 2. Histograms of the Baboon image: original (a), (b), (c); stego-image (d), (e), (f); and encrypted image (g), (h), (i) for red, green, and blue (RGB) components. Source: Taken from [29]

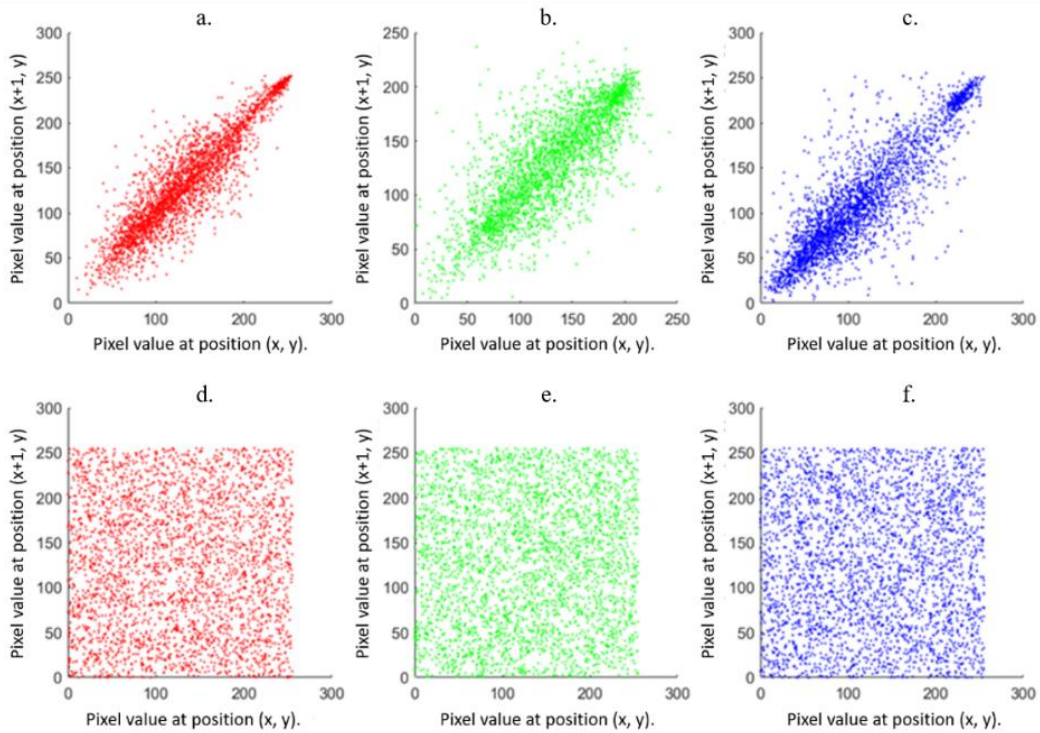


Figure 3. Baboon correlation: original image (a), (b), (c); encrypted image (d), (e), (f) for red, green, and blue (RGB) components. Source: Taken from [29]

Table 1. Indicators with a hidden message of 1,024 bits in the Baboon image

Algorithm	Border area (pixels)	MSE	PSNR (dB)	SSIM	FSIM
Proposed	400775	0.000058	64.3000	1	1
[10]	29695	0.0070	69.7156	1.00	
[8]	82944	0.2373	54.3775	0.9999	0.9997
[9]	13891	0.0108	67.8121		

Table 2. Indicators with a hidden message of 8,192 bits in the Baboon image

Algorithm	Border area (pixels)	MSE	PSNR (dB)	SSIM	FSIM
Proposed	400775	0.0046	59.7941	1.00	1.00
[10]	29695	0.0283	63.6114	0.9999	
[8]	82944	1.7027	45.8194	0.9987	0.9984
[9]	13891	0.0423	61.8675		

Table 3. Analysis of differential attacks on Lena, compared with other proposals

Algorithm	NPCR <sub>RGB</sub> (%)			UACI <sub>RGB</sub> (%)		
	Red layer	Green layer	Blue layer	Red layer	Green layer	Blue layer
Proposed	99.6567	99.6368	99.5773	33.2069	30.885	27.675
[16]	99.5693	99.5123	99.5941	33.3184	33.4127	33.4426
[17]	99.60	99.61	99.61	33.56	33.45	33.49
[4]	99.6100	99.6092	99.6099	33.4639	33.5042	33.4776

Table 4. Shannon entropy on Lena, compared with other proposals

Algorithm	Entropía			
	Red layer	Green layer	Blue layer	Average
Proposed	7.9975	7.9967	7.9971	7.9971
[16]	7.9973	7.9975	7.9975	7.9974
[17]	7.9973	7.9969	7.9971	7.9971
[4]	7.9893	7.9896	7.9903	7.9897

## 6. CONCLUSION

Based on the security and performance indicators obtained in this study, it is concluded that the developed crypto-steganographic algorithm, which merged chaos, DNA encoding, edge detection, and edge dilation, aiming to conceal a text message within the edges of a subsequently encrypted image, can be implemented for applications in real environments. It is noteworthy that even with an increase in the size of the text to be hidden, the similarity index between the original image and the stego-image remains constant. Similarly, the mean squared error remains very close to zero, a behavior that outperforms the values reported in the compared references. The results obtained in this study show that the proposed algorithm for hiding and encrypting messages in images, using indicators such as similarity index, mean squared error, PSNR, and others, has proven to be effective and comparable to other proposals in the scientific literature. Additionally, the algorithm demonstrates good resistance to differential attacks, as evidenced by NPCR and UACI indicators.

Regarding Shannon entropy, the obtained values are consistent with security standards established in scientific literature. It suggesting that the algorithm maintains a high level of randomness in the distribution of data, which is desirable in terms of security. These findings support the effectiveness and robustness of the proposed algorithm for hiding and encrypting messages in images, positioning it as a viable and competitive option in the field of information security.

## ACKNOWLEDGEMENTS

The authors express their gratitude for the support received from the Center for Research and Scientific Development (CIDC) of the Universidad Distrital Francisco José de Caldas for the execution of the research project that led to this article.

## REFERENCES




- [1] M. Luis, L. Daniel, A. Isabel, and A. Deicy, "A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic," *Multimedia Tools and Applications*, vol. 82, no. 23, pp. 35149–35181, Sep. 2023, doi: 10.1007/s11042-023-14475-1.
- [2] R. Tanwar, K. Singh, M. Zamani, A. Verma, and P. Kumar, "An optimized approach for secure data transmission using spread spectrum audio steganography, chaos theory, and social impact theory optimizer," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–10, Sep. 2019, doi: 10.1155/2019/5124364.
- [3] M. A. Hussain and P. Bora, "A highly secure digital image steganography technique using chaotic logistic map and support image," in *2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP)*, Sep. 2018, pp. 69–73, doi: 10.1109/ICICSP.2018.8549790.
- [4] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, Dec. 2015, doi: 10.1016/j.asoc.2015.08.008.
- [5] W. Zhang, H. Yu, Y. Zhao, and Z. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36–50, Jan. 2016, doi: 10.1016/j.sigpro.2015.06.008.
- [6] N. Kar, K. Mandal, and B. Bhattacharya, "Improved chaos-based video steganography using DNA alphabets," *ICT Express*, vol. 4, no. 1, pp. 6–13, Mar. 2018, doi: 10.1016/j.ict.2018.01.003.
- [7] O. A. Al-Harbi, W. E. Alahmadi, and A. O. Aljahdali, "Security analysis of DNA based steganography techniques," *SN Applied Sciences*, vol. 2, no. 2, Feb. 2020, doi: 10.1007/s42452-019-1930-1.
- [8] K. Gaurav and U. Ghanekar, "Image steganography based on Canny edge detection, dilation operator and hybrid coding," *Journal of Information Security and Applications*, vol. 41, pp. 41–51, Aug. 2018, doi: 10.1016/j.jisa.2018.05.001.
- [9] D. R. I. M. Setiadi and J. Jumanto, "An enhanced LSB-image steganography using the hybrid Canny-Sobel edge detection," *Cybernetics and Information Technologies*, vol. 18, no. 2, pp. 74–88, Jun. 2018, doi: 10.2478/cait-2018-0029.
- [10] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 104–114, Feb. 2022, doi: 10.1016/j.jksuci.2019.12.007.
- [11] R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Jul. 2017, pp. 230–235, doi: 10.1109/ICCMC.2017.8282682.
- [12] V. R. Falmari and M. Brindha, "Privacy preserving cloud based secure digital locker using Paillier based difference function and chaos based cryptosystem," *Journal of Information Security and Applications*, vol. 53, Aug. 2020, doi: 10.1016/j.jisa.2020.102513.
- [13] N. A. E.-S. Mohamed, H. El-Sayed, and A. Youssif, "Mixed multi-chaos quantum image encryption scheme based on quantum cellular automata (QCA)," *Fractal and Fractional*, vol. 7, no. 10, Oct. 2023, doi: 10.3390/fractalfract7100734.
- [14] N. A. E.-S. Mohamed, A. Youssif, and H. A.-G. El-Sayed, "Fast and robust image encryption scheme based on quantum logistic map and hyperchaotic system," *Complexity*, vol. 2022, pp. 1–20, Mar. 2022, doi: 10.1155/2022/3676265.
- [15] L. Wang, Q. Ran, and J. Ding, "Quantum color image encryption scheme based on 3D non-equilateral Arnold transform and 3D logistic chaotic map," *International Journal of Theoretical Physics*, vol. 62, no. 2, Feb. 2023, doi: 10.1007/s10773-023-05295-y.
- [16] A. Y. Niyat and M. H. Moattar, "Color image encryption based on hybrid chaotic system and DNA sequences," *Multimedia Tools and Applications*, vol. 79, no. 1–2, pp. 1497–1518, Jan. 2020, doi: 10.1007/s11042-019-08247-z.
- [17] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, Feb. 2019, doi: 10.1016/j.sigpro.2018.09.029.
- [18] A. Baalaji and R. Bevi, "Design of a novel chaotic neural network based encryption system for security applications," *Journal of the Chinese Institute of Engineers*, vol. 44, no. 5, pp. 424–439, Jul. 2021, doi: 10.1080/02533839.2021.1919558.
- [19] K. Liu, K. Xiao, and H. Xiong, "An image edge detection algorithm based on improved Canny," *Proceedings of the 2017 5th International Conference on Machinery, Materials and Computing Technology (ICMMCT 2017)*, 2017, doi: 10.2991/icmmct-17.2017.114.






- [20] P. Malathi and T. Gireeshkumar, "Relating the embedding efficiency of LSB steganography techniques in spatial and transform domains," *Procedia Computer Science*, vol. 93, pp. 878–885, 2016, doi: 10.1016/j.procs.2016.07.270.
- [21] R. Sun *et al.*, "Survey of image edge detection," *Frontiers in Signal Processing*, vol. 2, Mar. 2022, doi: 10.3389/frsip.2022.826967.
- [22] Z. Xu, X. Ji, M. Wang, and X. Sun, "Edge detection algorithm of medical image based on Canny operator," *Journal of Physics: Conference Series*, vol. 1955, no. 1, Jun. 2021, doi: 10.1088/1742-6596/1955/1/012080.
- [23] B. Patwari, U. Nandi, and S. K. Ghosal, "Image steganography based on difference of Gaussians edge detection," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 43759–43779, Nov. 2023, doi: 10.1007/s11042-023-15360-7.
- [24] H. Yin, Y. Gong, and G. Qiu, "Fast and efficient implementation of image filtering using a side window convolutional neural network," *Signal Processing*, vol. 176, Nov. 2020, doi: 10.1016/j.sigpro.2020.107717.
- [25] K. Priya, B. Rasheeda Banu, T. Umme Habiba, and A. Boosra, "Digital image processing techniques-a review," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 6, no. 9, Sep. 2019.
- [26] J. Canny, "A computational approach to edge detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. PAMI-8, no. 6, pp. 679–698, Nov. 1986, doi: 10.1109/TPAMI.1986.4767851.
- [27] I. Sobel and G. Feldman, "A 3x3 isotropic gradient operator for image processing," *a talk at the Stanford Artificial Project in*, pp. 271–272, 1968.
- [28] USC Viterbi, "The USC-SIPI image database," USC University of Southern California, Accessed: Mar. 12, 2024. [Online]. Available: <https://sipi.usc.edu/database/>
- [29] E. A. L. Torres, "Encryption of images carrying steganographed texts using chaotic systems, artificial vision and DNA coding (in Spanish)," M.S. thesis, Ingeniería de Sistemas, Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá D.C., 2022.

## BIOGRAPHIES OF AUTHORS






**Edison Andrés López Torres**    he has the systems engineer degree from Universidad Distrital Francisco José de Caldas, Bogotá Colombia. He was president of the IEEE Computer chapter at the Universidad Distrital Computer UD between 2018 and 2019. He currently is Seedbed Leader of Esri Colombia and Esri Ecuador. He can be contacted at email: [edalopezt@udistrital.edu.co](mailto:edalopezt@udistrital.edu.co).






**Deicy Alvarado-Nieto**    she has the systems engineer degree from Universidad Distrital de Bogotá Colombia, master's in systems engineering degree from Universidad Nacional de Colombia and PhD with emphasis in computer science and artificial intelligence degree from Universidad de Oviedo in Spain. She currently directs the Complexity Group at the Universidad Distrital ComplexUD. She is a titular professor at the Faculty of Engineering of the Universidad Distrital Francisco José de Caldas since 1995. She can be contacted at email: [lalvarado@udistrital.edu.co](mailto:lalvarado@udistrital.edu.co).



**Isabel Amaya-Barrera**    she has a degree in mathematics from Universidad Distrital Francisco José de Caldas, Bogotá Colombia, specialist in applied mathematics degree from Universidad Sergio Arboleda Bogotá, master's in mathematical sciences degree from Universidad Nacional de Colombia. Member of the Complexity Group of the Universidad Distrital ComplexUD, she is a titular professor at the Faculty of Engineering of the Universidad Distrital Francisco José de Caldas since 2001. She can be contacted at email: [iabaya@udistrital.edu.co](mailto:iabaya@udistrital.edu.co).



**César Augusto Suárez Parra**    he has a degree in mechanical engineering from Universidad INCCA de Bogotá Colombia. Master in materials and manufacturing processes degree from Universidad Nacional de Colombia, Member of the Complexity Group of the Universidad Distrital ComplexUD. He is an assistant professor at the Faculty of Engineering of the Universidad Distrital Francisco José de Caldas since 1999. He can be contacted at email: [casuarezp@udistrital.edu.co](mailto:casuarezp@udistrital.edu.co).