Investigación

Steganographic Cryptosystem Based on the Use of Chaos Theory and Cellular Automata

Criptosistema esteganográfico basado en el uso de teoría del caos y autómatas celulares

Marlon Arias-Cárdenas
Universidad Distrital Francisco José de Caldas, Colombia
mariasc@udistrital.edu.co
https://orcid.org/0000-0003-1772-8199
Deicy Alvarado-Nieto
Universidad Distrital Francisco José de Caldas, Colombia
lalvarado@udistrital.edu.co
https://orcid.org/0000-0002-1305-3123
Isabel Amaya-Barrera
Universidad Distrital Francisco José de Caldas, Colombia
iamaya@udistrital.edu.co
https://orcid.org/0000-0002-8845-5901

Recepción: 06 Junio 2024
Aprobación: 18 Octubre 2024
Publicación: 12 Noviembre 2024

Acceso abierto diamante

Abstract

The exchange of large amounts of information through public channels has become an everyday occurrence, a situation that generates great risks in the case of possible cyber-attacks and motivates the academic and scientific community to develop new robust security schemes. The objective of the research was to use mathematical and artificial intelligence tools to propose new security schemes. The design and implementation of a crypto-steganographic algorithm for text is described below. The methodology employed consisted of using cellular automata to detect the edges of a carrier image, leveraging the color contrast diversity, and the Tinkerbell chaotic attractor to generate two pseudo-random sequences: one for the encryption scheme and the other to select the edge pixels of the carrier image where cryptogram bits are hidden. Additionally, a verification phase was included in which the receiver provides a code to confirm that the stegoimage was not altered. The system key is shared between the sender and the receiver using the Diffie-Hellman algorithm. The proposed algorithm was subjected to a series of steganographic and cryptographic performance tests, including entropy analysis, mean square error (MSE), correlation coefficients, key sensitivity, peak signal-to-noise ratio (PSNR), normalized root mean square error (NRMSE), and the structural similarity index (SSI). The results of PSNR, MSE and SSI test were compared with scientific benchmarks, revealing indicators that align with the standards of information security. Finally, a crypto-steganographic algorithm was consolidated as a result of an academic exercise whose indicators make it potentially applicable in real-world contexts.

Keywords: **Security, cellular automata, chaos, cryptography, image edge detection, steganography.**

Notas de autor

lalvarado@udistrital.edu.co

Resumen

El intercambio de grandes cantidades de información a través de canales públicos se ha convertido en algo cotidiano, situación que genera grandes riesgos ante posibles ciberataques y motiva a la comunidad académica y científica a desarrollar nuevos esquemas robustos de seguridad. El objetivo de la investigación fue utilizar herramientas de matemáticas e inteligencia artificial para proponer nuevos esquemas de seguridad. A continuación, se describe el diseño e implementación de un algoritmo cripto-esteganográfico para texto. La metodología empleada consistió en usar autómatas celulares para detectar los bordes de una imagen portadora, aprovechando la diversidad de contrastes de color, así como el atractor caótico Tinkerbell para generar dos secuencias pseudoaleatorias: una para el esquema de cifrado y otra para seleccionar los píxeles de los bordes de la imagen portadora, donde se ocultan los bits del criptograma. Además, se incluyó una fase de verificación, en la que el receptor proporciona un código para confirmar que la imagen stego no fue manipulada. La clave del sistema se comparte entre el emisor y el receptor mediante el algoritmo Diffie-Hellman. El algoritmo propuesto se sometió a una serie de pruebas de rendimiento esteganográfico y criptográfico, tales como el análisis de entropía, el error cuadrático medio (MSE), los coeficientes de correlación, la sensibilidad de la clave, la relación señal-ruido máxima (PSNR), el error cuadrático medio normalizado (NRMSE) y el índice de similitud estructural (SSI). Los resultados de las pruebas PSNR, MSE y SSI, se compararon con referencias científicas, revelando indicadores que se ajustan a los estándares de seguridad de la información. Finalmente, se consolidó un algoritmo criptoesteganográfico resultado de un ejercicio académico cuyos indicadores lo convierten en potencial de aplicación en contextos del mundo real.

Palabras clave: **Seguridad, autómatas celulares, caos, criptografía, detección de bordes, esteganografía.**

Highlights

Artificial Intelligence is a robust alternative for designing security schemes.
The behavior of chaotic attractors significantly impacts security schemes.
New security schemes are needed to address the challenges posed by advancing technology.
Information security is the biggest concern of the digital society.
Fraudulent access to private information can lead to global catastrophes.

Highlights

La Inteligencia Artificial es una alternativa robusta para el diseño de esquemas de seguridad.
El comportamiento de los atractores caóticos impacta significativamente los esquemas de seguridad.
Nuevos esquemas de seguridad para los desafíos generados por el avance de la tecnología.
La seguridad de la información es la mayor preocupación de la sociedad digital.
El acceso fraudulento a la información privada puede originar catástrofes a nivel mundial.

1. INTRODUCTION

Advances in telecommunications, coupled with global population growth have boosted the exponential increase in Internet-connected devices, leading to the widespread adoption of new forms of communication accessible to the majority of the population. This growth was further accelerated by the spread of the SARS-CoV-2 virus. This trend is highlighted in the annual reports published by the International Telecommunication Union (ITU), the United Nations agency responsible for providing official statistics on information and communication technologies [1]. This has strengthened the search for strategies for the secure exchange of information, reason why it is imperative to join academic efforts to propose increasingly robust security schemes, in line with the development of next generation devices. In this regard, cryptography and steganography have played a leading role throughout history in safeguarding information, preventing intruders from gaining illegal access to it [2] - [7]. Their strategies have evolved in parallel with technology and advances in mathematics and artificial intelligence, promoting the emergence of academic communities interested in proposing secure algorithms with new approaches [8] - [17].

In recent decades, due to the intrinsic properties of dynamical systems that exhibit chaos, a line of research called chaotic cryptography has been conceived, with increasingly promising results, which in parallel has meant progress in the study and definition of new dynamical systems, all this looking for more complex behaviors, a favorable condition to use a chaotic attractor in order to define cryptographic schemes with high security and performance indicators [14], [18] - [24].

On the other hand, cellular automata have been applied in different contexts, particularly in the field of cryptography, where security schemes can be designed based on their evolution [11], [25]. Similarly, in the field of steganography, it is usual to use the edges of an image to hide information [26], [27], automata are an alternative in this process of edge detection [13], [28], [29], as well as fuzzy logic.

In summary, this paper describes the application of chaos theory and cellular automata, with the objective of designing a text encryption algorithm complemented with a steganographic scheme, a process that involved the selection of a chaotic attractor and the implementation of an edge detection method with cellular automata to hide a ciphertext. Some references found in the scientific literature, used to support the achievement of the results shown in this article, are presented below.

In [25] they describe a set of linear rules that are applied to evolve two-dimensional automata to find the edges of an image. Likewise, in [11] the authors present a model for encrypting videos from security cameras,

by means of the evolution of composed cellular automata, which are defined based on Wolfram automata and are applied by arranging each frame as a set of eight layers generated from the bit values.

In relation to the use of chaotic attractors, there is the work of [14] which propose a mechanism for generating pseudo-random numbers by means of the Tinkerbell attractor. On the other hand, in steganography, the contribution of [13] stands out, they use the three most significant bits belonging to the pixels of the edges of an image, in order to increase the space for information hiding.

Another work to remark is the one proposed in [18], the authors combine steganography and cryptography to hide an image inside another one, the stegoimage is later encrypted using a chaotic attractor. Likewise, in [30], combining chaos with DNA code, they present a steganographic proposal applied to videos, they assert that the stegoimage presents a minimum of degradation with respect to the frames of the original video, that is, the difference is imperceptible to the human eye.

The model described throughout this article is part of the results of the research project entitled "Encryption models based on chaotic attractors" developed within the Faculty of Engineering of the Universidad Distrital Francisco José de Caldas, which gave rise to the development of undergraduate thesis, such is the case of [31], which involve cellular automata for edge detection, the Tinkerbell attractor for the generation of two pseudorandom sequences used in the encryption and steganography processes respectively, and finally recurring to the least significant bit technique to hide, in the carrier image, the encrypted text. It is important to note that in the proposed model, the Tinkerbell attractor can be replaced by another attractor with more than one dimension that exhibits complex chaotic behavior, whether discrete or continuous. Examples include the Rössler or Lorenz attractors. To validate the proposed scheme, security and performance tests were carried out, which showed consistent results in the context of security.

2. METHODOLOGY

To achieve the objectives proposed in this work, the basic elements for the construction of the crypto-steganographic model are presented below, following a deductive, correlational, and mixed methodology. Based on general principles of mathematics and artificial intelligence, the design of cryptographic and steganographic schemes focused on large information is carried out, emphasizing that although cause-effect relationships are considered, it is not possible to control all the factors involved, since chaotic systems have a high sensitivity to the initial conditions and their parameters, which leads to both qualitative analysis to characterize the level of complexity of the security model, and quantitative analysis to validate the security and performance of the model. Figure 1 shows a synthesis of the process proposed in this work, which is described in sections 2.1 - 2.7.

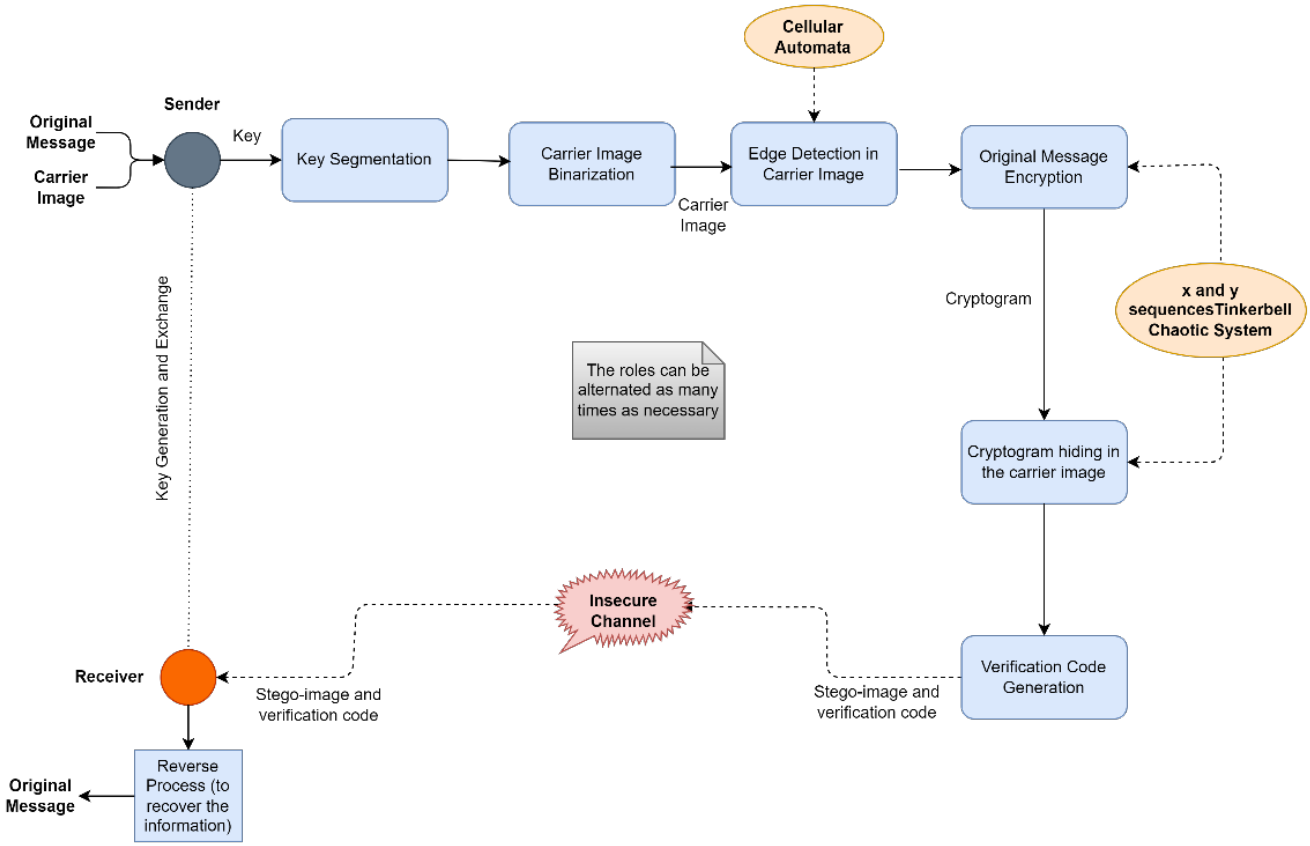

Figure 1.
Encryption scheme diagram
Source: own elaboration based on [31]

2.1 Creation and secure exchange of keys

The OpenSSL [32] cryptographic library is used to obtain a prime number of 2048 bits in length and a generator number, which are represented in hexadecimal format, considered as public parameters of the Diffie-Hellman key exchange algorithm [33], and needed by the sender and receiver to generate their own keys using the same library, thus obtaining secure parameters for the exchange of these keys.

The hashlib library, included in the Python installation [34], allows to calculate secure hash functions for an input data, in this case the SHA3-256 hash function was applied on the matching private keys, previously obtained to generate the key used in the system input data.

Part of the 32-byte string is used to define the initial conditions of the Tinkerbell chaotic attractor, which in addition to being two-dimensional is discrete and is modeled by means of the System of Equations given in expression (1)

$$\begin{cases} x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} = 2x_n y_n + cx_n + dy_n \end{cases} \quad (1)$$

This system displays complex behaviors in its trajectories in phase space, presenting both periodic and chaotic orbits depending on the choice of parameters, such as in [35] where, using Quasi-Newton methods for the values a=0.9, b=-0.6, c=2, d=0.5; 64 unstable periodic orbits and a strange attractor with a fractal structure were found, as illustrated in Figure 2, with initial conditions x_0 = -0.72 y y_0 = -0.64.

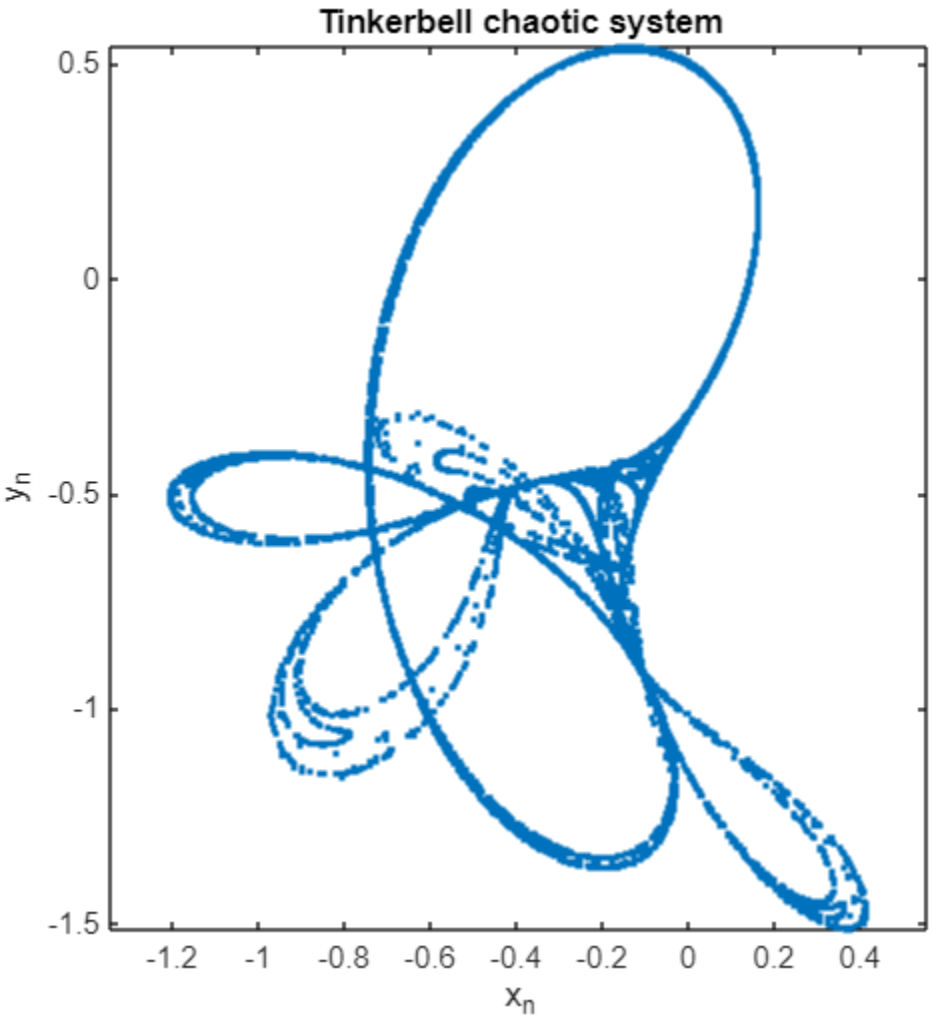

Figure 2.
Tinkerbell chaotic system
Source: own elaboration.

Similarly, the Tinkerbell attractor, which is used throughout this work to generate pseudo-random sequences, employed for both processes, namely: steganographic and cryptographic, exhibits high sensitivity to initial conditions, which can be verified by calculating Lyapunov exponents. For the particular case where b oscillates between -0.6 and -0.5, it can be seen that there are both positive and negative exponents, as shown in Figure 3.

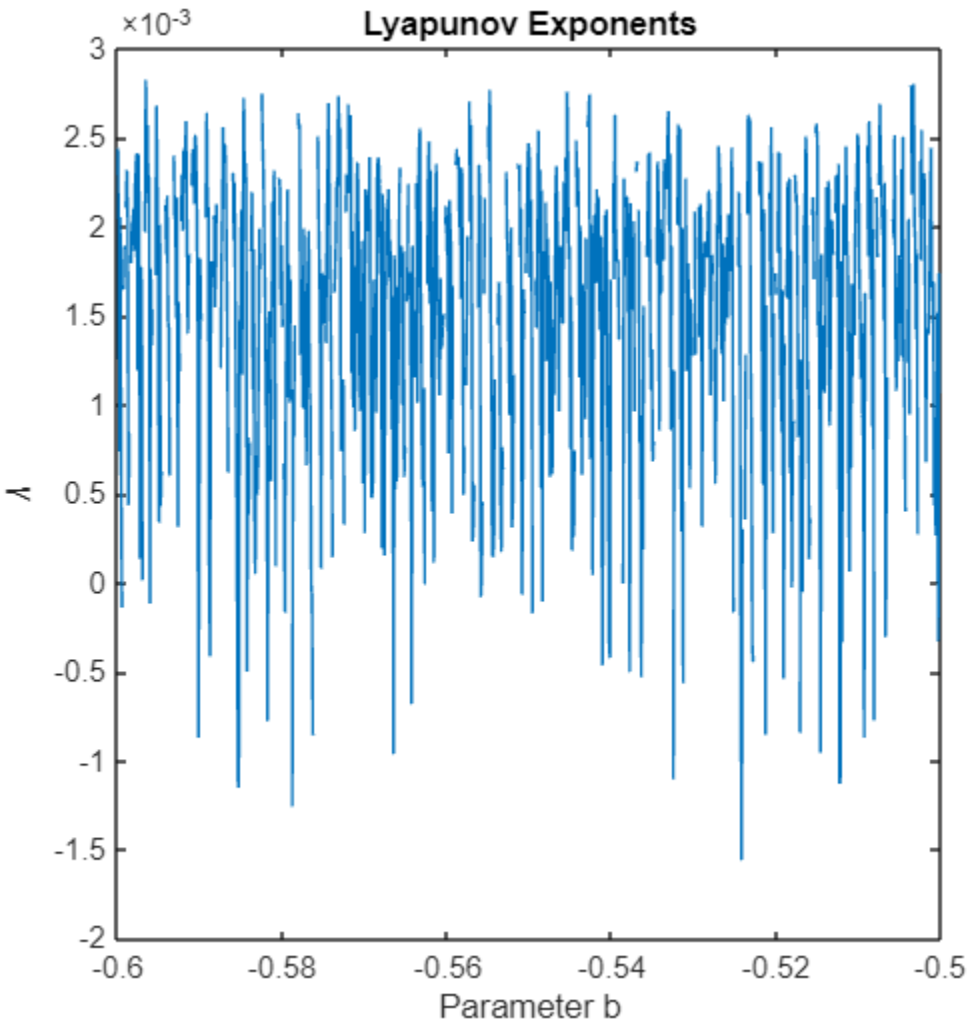

Figure 3.
Lyapunov Exponents
Source: own elaboration.

2.2 Key segmentation

The 32-byte string obtained in the previous step are used as follows: the first 12 bytes as initial conditions of the Tinkerbell attractor (6 for X and 6 for Y) generating a pseudo-random sequence for the encryption process. In order to increases the confusion and diffusion properties in the cryptosystem and since both the cipher sequence and the cryptogram are stored in one-dimensional arrays, the next 4 bytes are used to define shiftings, 2 in the cipher sequence and 2 in the cryptogram.

Likewise, for the steganographic process, the other 16 bytes are divided into 4 groups used as shown in Figure 4. Initial conditions of the Tinkerbell chaotic system are given by the bytes from 16 to 27, which is evolved to randomly choose several pixels belonging to the edges of the carrier image in which the cryptogram will be embedded, this number is determined by the length of the cryptogram. For a cryptogram of n characters, i.e., 8n bits, ideally, n edge pixels are required, as 8 bits will be hidden in each pixel. However, it is highly recommended that the number of edge pixels in the image significantly exceeds n, to avoid modifying all of them.

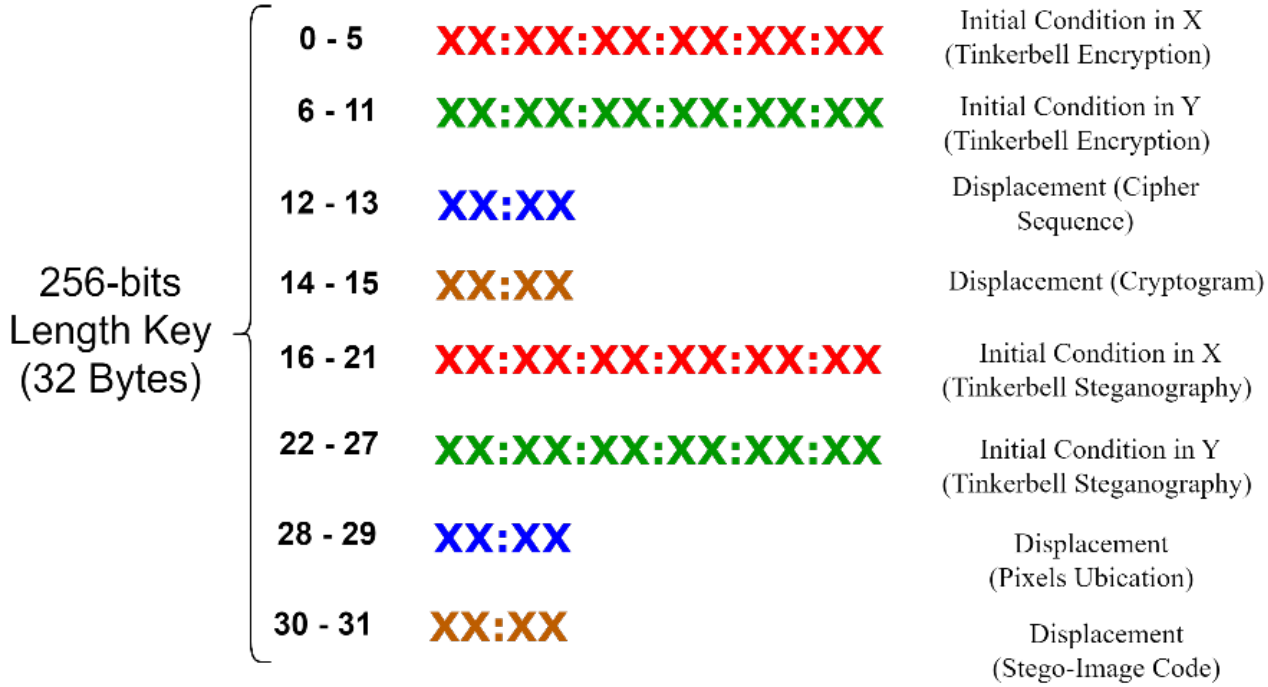

Figure 4.
Key segmentation
Source: own elaboration based on [31].

To increase the dispersion of the data to be hidden in the selected pixels and to make the integrity verification code more sensitive to key variations, the last 4 bytes of Figure 4 are used to define shiftings, two for the arrays containing the coordinates of the pixels chosen in the steganographic process and the other two for the stegoimage verification code.

2.3 Binarization of the carrier imagine and edge detection

For this process, it was necessary to transform the original image to gray scale in order to avoid independent manipulation of each RGB layer. Subsequently, the resulting image is binarized by applying a Gaussian filter with reflective edges, for which neighborhoods of 9 x 91 pixels were taken as a basis to generate the reference threshold.

Since the use of cellular automata in edge detection, whose behavior is described in [25], reduces processing times with respect to other filters found in the literature, it was decided to use them on the binarized image, where each cell corresponds to a pixel, and the states depend on its color (black or white), as presented in Figure 5.

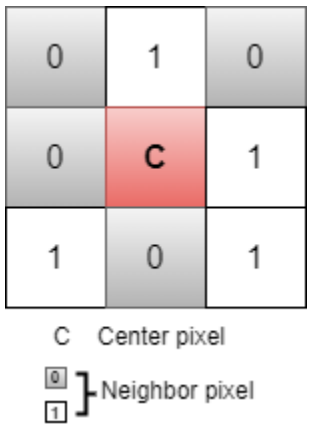

Figure 5.
Pixel neighborhoods
Source: own elaboration based on [25].

In this case, the cellular automaton is rectangular, the states correspond to zero or one, in [25] they assign an identifier to each of the 9 cells. More neighborhoods with radius equal to one are used, with adiabatic or reflective boundary condition and linear transition rules, as shown in Figure 6.

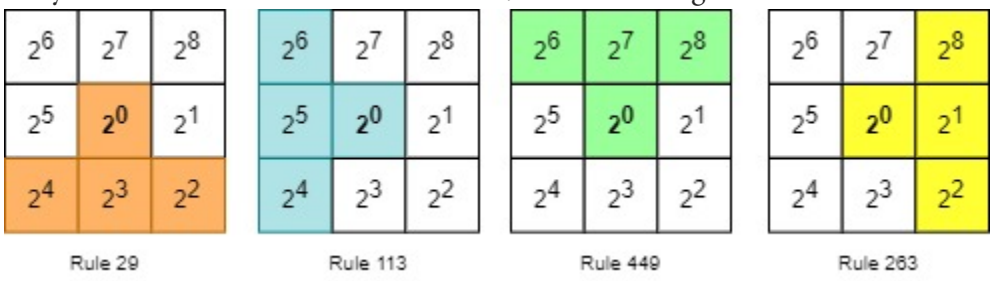

Figure 6.
Rules identifiers
Source: own elaboration based on [25].

Based on the identifiers shown in Figure 6, in [23] they define 4 evolution rules noted as:
Rule 29 (bottom edge): P29=P16⊕P8⊕P4⊕P1
Rule 113 (left edge): P113=P64⊕P32⊕P16⊕P1
Rule 263 (right edge): P263=P256⊕P2⊕P4⊕P1
Rule 449 (upper edge): P449=P64⊕P128⊕P256⊕P1

The entries corresponding to each of the identifiers involved in a given rule are all equal to 1 and the other ones are equal to 0. The symbol ⊕ denotes the XOR operation and Pj corresponds to the input position associated with the identifier j. The edge detection process begins by selecting one of these 4 rules and overlaying the table from Figure 6 to iteratively match the entries of the identifiers that are part of the rule with each of the pixels to be evolved, as illustrated in Figure 7.In this case, rule 29 is selected, and the pixel to be evolved is shaded in pink.

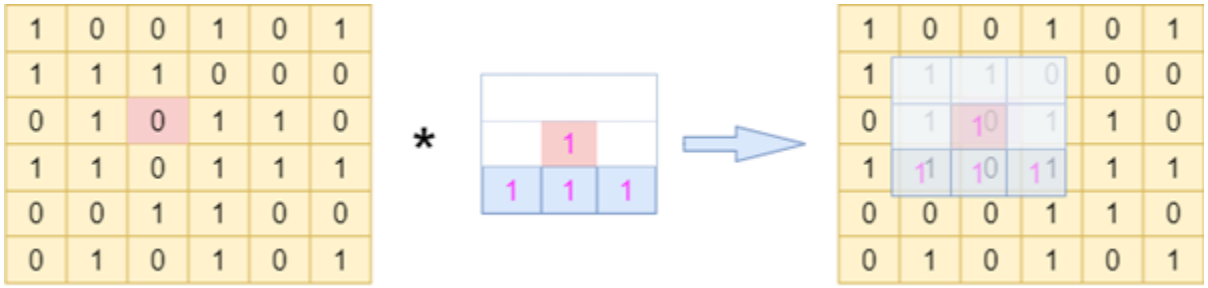

Figure 7.
Convolution process for a cell, using rule 29
Source: own elaboration.

Subsequently, an XOR operation is performed on the 4 obtained results. This output replaces the value of the pixel shaded in pink in the original binarized matrix, as shown in Figure 8.

$$(0 \oplus 1) \oplus (1 \oplus 1) \oplus (0 \oplus 1) \oplus (1 \oplus 1)$$

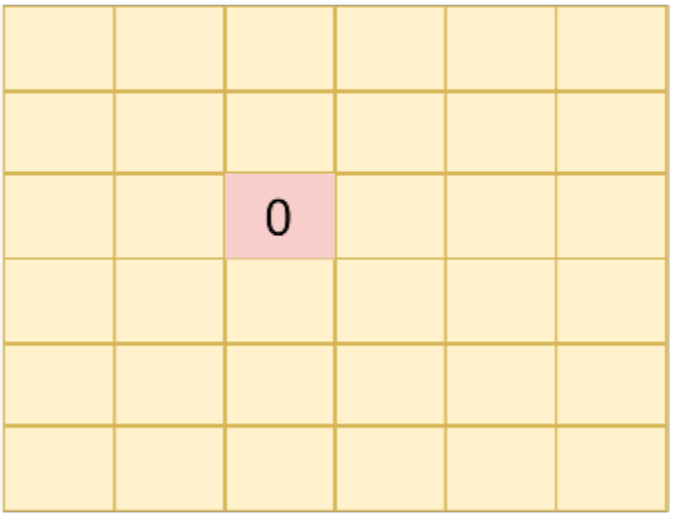

Figure 8.
Result of applying rule 29 to the pixel shaded in pink
Source: own elaboration.

After completing the previous process, the edges of the image are obtained for each of the pixels in the binarized image.

2.4 Encryption strategy

The model presented in this paper is applied to text files with n characters, encoded in binary. The Tinkerbell system is then iterated 4n times, generating two sequences, corresponding to the X and Y axes of the system's phase space. Each of the 8n entries is used to encrypt one bit of the text. The initial conditions are given as part of the user's key.

In order to store the result of the iterations of the X and Y components, two one-dimensional arrays are generated using the single precision format provided by the IEEE 754 standard, which allows storing numbers

with more than 38 decimal digits. Subsequently, the eighth decimal digit of each entry of the X array and the sixth of the entries in Y are selected, in order to apply to each of these two digits the module 2 operation, obtaining a cipher sequence of zeros and ones, with the same length of the text message expressed in binary.

To introduce confusion and diffusion in the cryptosystem and make it more robust against cryptanalysis attempts, both the encrypting sequence and the binary text are shifted several positions, as defined in the key segmentation section, schematized in Figure 4, this shift is determined according to the key and the length of the original message.

Subsequently, to obtain the cryptogram, further hide the relationship between the ciphertext and the original text and distribute the redundancy of the language, minimizing the risk of differential and statistical attacks, a bitwise XOR is performed between the ciphertext and binary sequences, then a shifted is applied to the result.

2.5 Hiding the cryptogram

Once the length of the cryptogram and the list of edge pixels of the image chosen by the user have been obtained, those where the cryptogram bits will be hidden are selected, for which the Tinkerbell attractor is iterated again with other initial conditions until a sequence of the same length of the cryptogram is obtained, this sequence is reordered from smallest to largest by executing in parallel the same changes of position in the list of edge pixels.

Subsequently, according to the length of the cryptogram, using the Permuted Congruential Generator (PCG) pseudo-random number generator, a finite number of pixels is selected from the reordered list of edge coordinates where the cryptogram will be embedded. The coordinates are stored in two one-dimensional arrays corresponding to the indices i, j that allow to determine the position of any pixel in the image, indicating height and width, respectively.

With the sequence used to reorder the pixels of the edges, another sequence composed of ones and zeros is obtained, taking the same position in each decimal value generated. If an odd number appears in the selected position, a one is assigned, otherwise a zero is assigned.

Since the arrays and the random sequence have the same length, the sequence is traversed from the initial position i = 0, and if there is a zero, the coordinate at that position, in the two arrays, is left untouched, but if in the sequence there is a one this coordinate is passed to the end of the list.

On the previously selected and processed pixels, the Least Significant Bit (LSB) technique is applied to hide the cryptogram bits, three in each of the red and green layers and two in the blue layer. This makes it difficult to carry out a successful steganalysis process.

2.6 Stegoimage verification code

In order to ensure the integrity of the stegoimage during the communication process, a Verification Code mechanism has been implemented. The Verification Code is designed to be corroborated by the receiver and involves a series of steps: (i) *XOR Operation on RGB Layers*: Initially, an XOR operation is performed on the pixels belonging to the three RGB layers of the stegoimage. This operation results in a two-dimensional matrix. (ii) *Consecutive XOR Operations*: Subsequently, consecutive XOR operations are applied within the obtained matrix, both horizontally (between the rows) and vertically (between the columns). This process generates two one-dimensional arrays. (iii) *Array Concatenation*: The first 32 values of each of the generated one-dimensional arrays are concatenated, resulting in a final Verification Code with a length of 64 bits. This Verification Code, once generated, serves as a checksum mechanism, ensuring the integrity of the stegoimage during transmission and reception.

2.7 Information recovery process

Due to the symmetric nature of the steganographic cryptosystem, the process of recovering the original message is the reverse of the sender's operation, using the same key at both ends and ensuring the integrity of the information through the verification code. If these last two conditions are not complied with, it will be impossible to recover the original message. Figure 9 illustrates the processes of encryption, steganography, and recovery of the original information, proposed in this document.

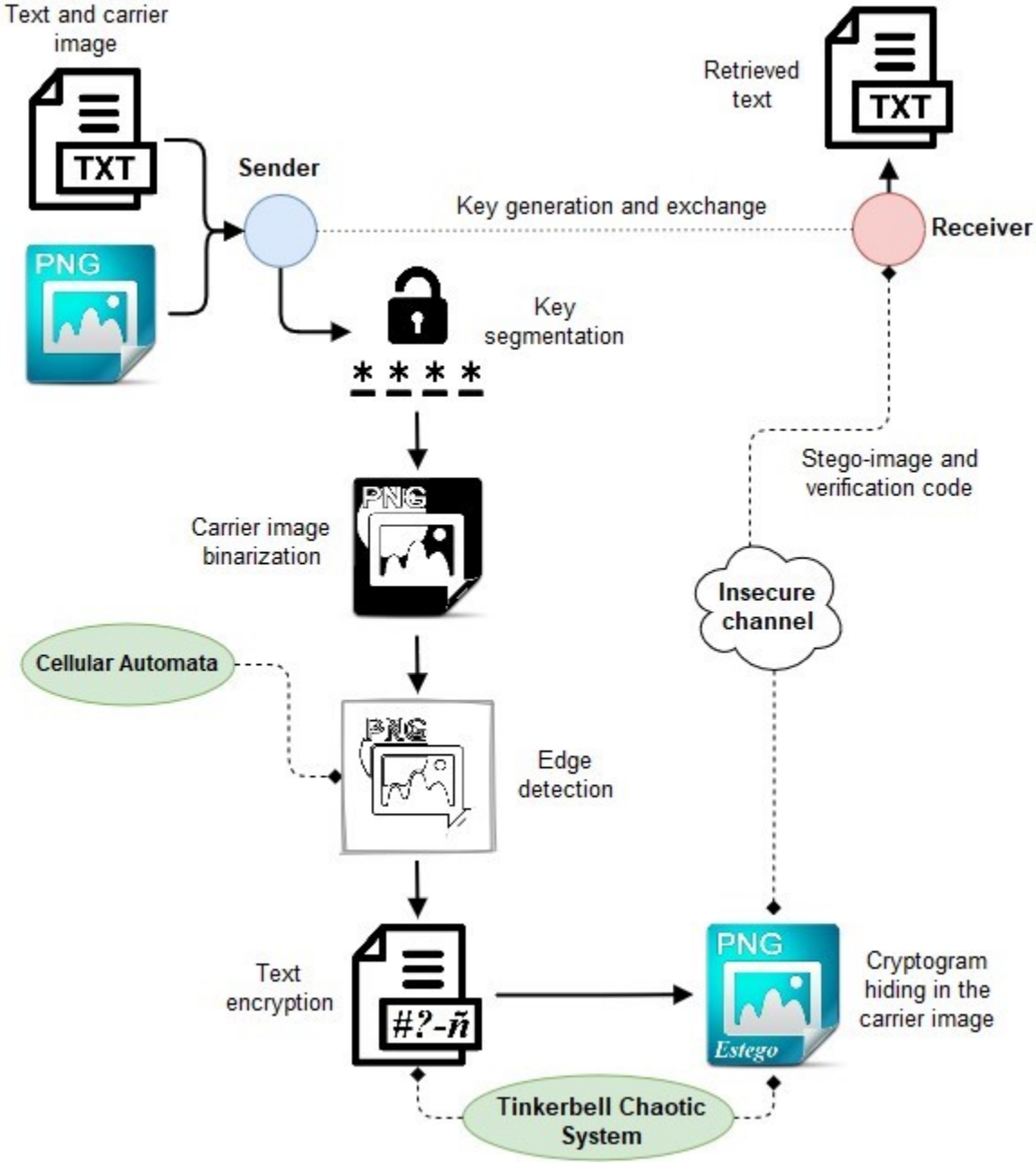

Figure 9.
Complete sequence of the proposed process
Source: own elaboration.

3. RESULTS AND DISCUSSION

The algorithm presented in this work is summarized in Figure 10, emphasizing that each of the stages carried out in the proposed crypto-steganographic process is schematized there. Security and performance tests were applied on texts of different lengths and different carrier images, to validate this proposal, finding in all cases indicators consistent with the standards found in current scientific literature on security.

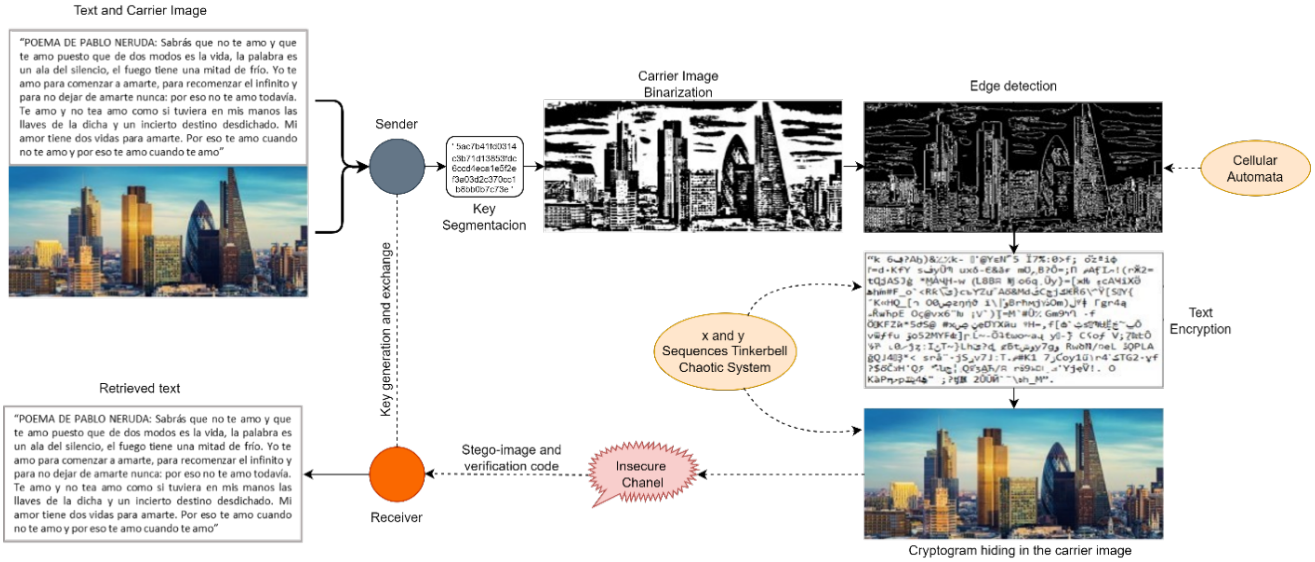

Figure 10.
Stages of the proposed algorithm
Source: own elaboration based on [31].

As a case study, we present the results using the key 5J*`;`ltsd;hwRf%e%.mqQ, to encrypt a text message of 2979 characters and hide it in the carrier image Baboon (Figure 11(a)). Figure 11(b) shows the stegoimage with the encrypted text, highlighting that changes are not evident to the human eye.

Figure 11.
Cryptosteganographic result
Source: taken from [36]; Source: own elaboration

Despite the above, when generating and visualizing the grayscale frequency histograms of the two images, slight differences are found, however, the cumulative frequency histograms seem to be identical, which reduces the risk of arousing suspicion that hidden information is stored on the image. Figures 12(a) and 12 (b) show

the histograms corresponding to the original image and the stegoimage, respectively, while the cumulative frequency histograms of these images are presented in Figures 12(c) and 12(d).

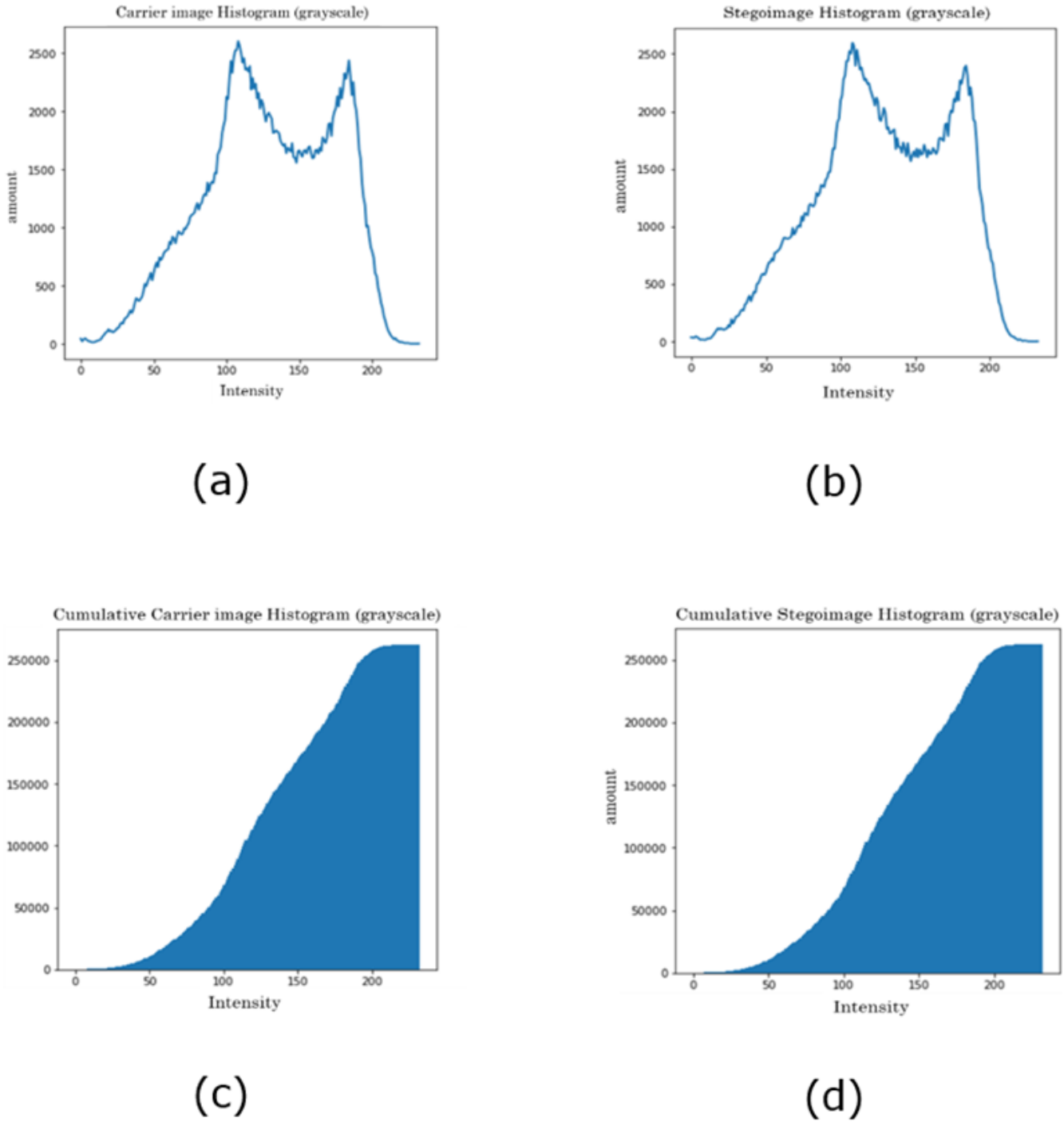

Figure 12.
Grayscale histograms original image and stegoimage
Source: own elaboration.

Additionally, histograms of the original Baboon vs Baboon stegoimage (Figure 11) were obtained for each RGB layer, which are presented in Figure 13, showing high similarity between these histograms, a favorable situation in the context of steganography.

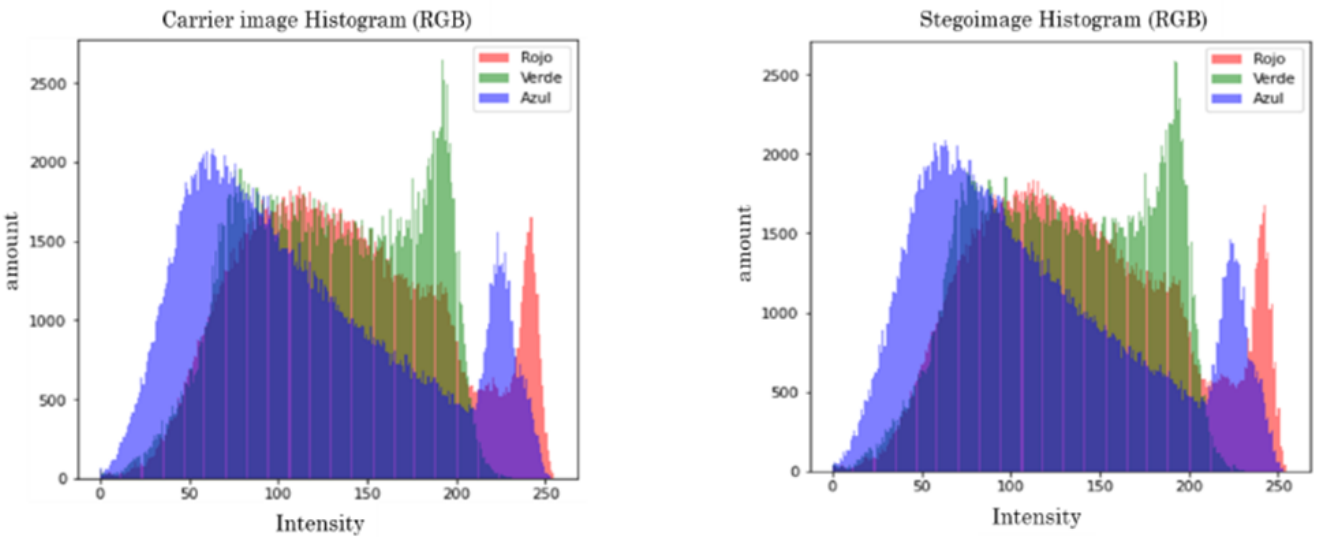

Figure 13.
RGB histograms original image and stegoimage
Source: own elaboration.

Another indicator considered to evaluate the differences between the carrier image and the stegoimage, in grayscale, was the calculation of the local entropy, which measures precisely the level of randomness of the pixels of an image [37], [38], as shown in Figure 14, generating, in this case, two identical images to the human perception, a desirable situation in the field of steganography.

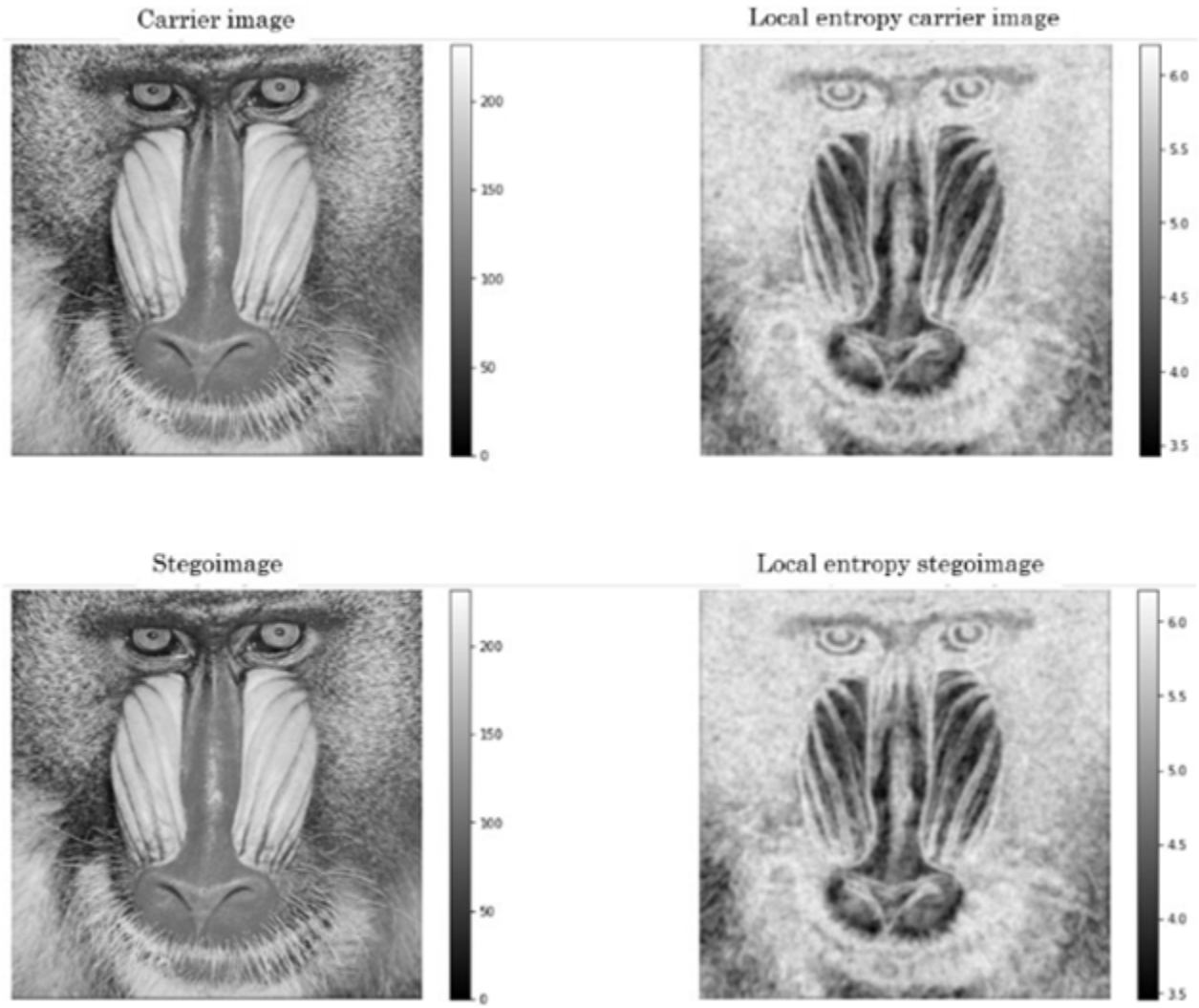

Figure 14.
Local entropy of the original and the stegoimage
Source: own elaboration.

The Shannon entropy values for the carrier image and for the stegoimage were respectively 7.380353762612659 and 7.380578390214877, finding a minimum difference of about 0.00022, which allows us to ensure that the level of disorder in the pixels of both images is almost identical, a scenario that is pursued in any steganographic process.

The Peak signal to noise ratio (PSNR), Mean Square Error (MSE), Normalized Root Mean Square Error (NRMSE), Structural Similarity Index (SSI) indicators presented in Table 1 were also calculated, the values obtained allow us to affirm that the differences between the original image and the stegoimage are really minimal, a fact that supports the security level of the proposed algorithm.

Table 1
Similarity Indicators

Indicator	Value obtained
PSNR	51.147060
MSE	$7.678X10^{-6}$
NRMSE	0.0051064
SSI	0.9986450

Source: own elaboration.

A reference for the development of this proposal was the work of Setiadi [13], who used a greater number of bits in the pixels to hide the information, which leads to significant modifications in the stegoimage, additionally, by dilating the edges of the image, he obtained areas with low entropy, which implies that the modifications made in them are easier to identify, such drawback was corrected in this proposal where an almost identical entropy value was achieved for the original image and its corresponding stegoimage, as shown in Table 2.

Table 2
Entropy values for original image and stegoimage

Imagen	Original Entropy	Stegoimage Entropy
Lena	7.49899	7.49957
Baboon	7.38035	7.38057
Airplane	6.73475	6.73082

Source: own elaboration.

However, [13], obtained very good indicators of similarity, which were slightly improved in this work, as shown in Table 3.

Table 3
Comparison with Setiadi's work

Algorithm used	Message length	MSE	PSNR	SSI
Proposed in [13]	16384 bits	0.0554	60.697	0.9997
Proposed in this work	23832 bits	$7.678x10^{-6}$	51.147	0.9986

Source: own elaboration.

Another fact to highlight in the proposed model, which results in good indicators, is related to the use of the Tinkerbell chaotic attractor in the pseudorandom reordering of the list of pixel coordinates that can be used to embed information, so that the values variations are distributed throughout the image, minimizing the possibility of finding a relationship between these values.

Regarding the sensitivity analysis of the key and Pearson's key space, Figure 15 shows the result of encrypting a text of 488 characters with two keys that differ only in one digit, obtaining completely different cryptograms, which indicates that small changes in the key generate completely different results, a situation desired in the field of cryptography.

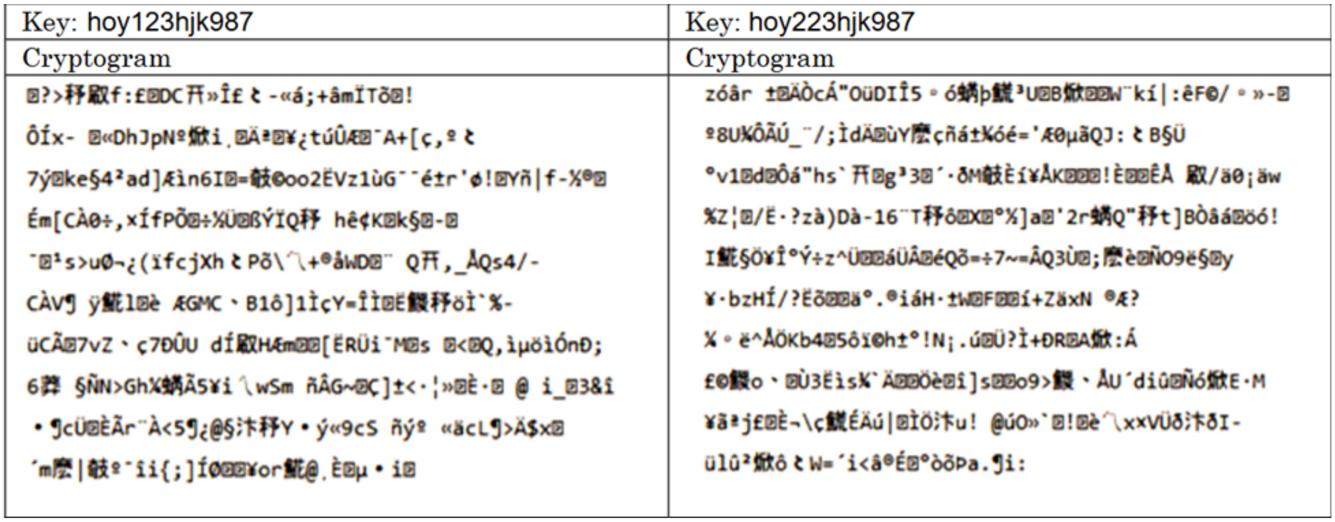

Figure 15.

Key Sensitivity

Source: own elaboration based on [31].

Since the SHA3-256 hash function is used for key generation, the key space is larger than the obtained in [13] by Stoyanov and Kordov. In general, for the tests performed, the correlation coefficients found in this work are slightly below those reported in [14] as shown in the Table 4.

Table 4.

Comparison space and key sensitivity comparison

Algorithm	Key space	Correlation coefficient
Proposed in [14]	2^{183}	-0.0014 – 0.00043
Proposed in this work	2^{256}	0.0039789– 0.001112719

Source: own elaboration.

These results show that the proposal presented here is resistant to brute force attacks.

However, the steganographic process carried out with the two cryptograms obtained in Figure 15, leads to obtain stegoimages identical to the human eye, as shown in Figure 16 and as corroborated through the calculation of Pearson's correlation coefficients.

Figure 16.
Stegoimages with slight key variation
Source: own elaboration.

In turn, to evaluate the randomness of the pseudorandom cipher sequences generated by the Tinkerbell chaotic attractor, the statistical tests proposed by the National Institute of Standards and Technologies (NIST) were used, finding that almost all of these 15 tests were passed, a favorable situation for the purpose of the validation performed. The results, for a string of 60.000 bits obtained from the Tinkerbell attractor, are shown in Figure 17.

```
    Length: 60000 bits / 750 bytes
    Runs: 30

    Statistical Test of Randomness (NIST sp800)
    TEST: monobit_test
    Number of ones = 30032
    Number of zeros = 29968
    Pass
    P = 0.793877432390982

    RESULTS
    --------
    monobit_test                            0.7938774623909824  PASS
    frequency_within_block_test             0.8379213646094826  PASS
    runs_test                               0.9351468689731612  PASS
    longest_run_ones_in_a_block_test        0.3030992899687981  PASS
    binary_matrix_rank_test                 0.2932651425138177  PASS
    dft_test                                0.8808800176244775  PASS
    non_overlapping_template_matching_test  0.9999999847086102  PASS
    overlapping_template_matching_test      0.0                 NO DATA*
    maurers_universal_test                  0.0                 NO DATA**
    linear_complexity_test                  0.0                 NO
DATA***
    serial test                             0.6078154427748813  PASS
    approximate_entopy_test                 0.9091921669706351  PASS
    cumulative_sums_test                    0.9318746883859528  PASS
    random_excursion_test                   0.0830309371331871  PASS
    random_excursion_variant_test           0.0615996076976977  PASS
    --------
    * - At least 128512 bytes required
    ** - At least 48480 bytes required
    *** - At least 10^6 bits required
```

Figure 17.
NIST tests for a 60,000-bit string generated with the Tinkerbell attractor
Source: own elaboration.

4. CONCLUSIONS

The main contribution of this work is the combination of chaotic attractors and cellular automata in both encryption and text hiding within an image. By means of the Tinkerbell chaotic attractor and the use of cellular automata, a scheme for encrypting and hiding text on the edges of an image was designed, which, according to the performance tests carried out, can be classified as highly secure and reliable for use in real environments.

The work presented here highlights the strengths provided using multiple mathematical foundations combined in the process of encryption and hiding of information, a requirement that has taken on greater relevance due to massification of new forms of communication accessible to the vast majority of the population, increase of devices connected to the Internet, advances in telecommunications and population growth worldwide as well as the pandemic caused by COVID19, which increased the need for secure exchange of large information through public channels.

It is important to note that in the proposed scheme images with different color contrasts must be used, the algorithm works independently of the size of the text to be hidden. If the text exceeds the capacity of pixels belonging to the edges of the carrier image, it is possible to carry out the steganography process using more than one image.

REFERENCES

[1] United Nation, "International Telecomunication Union," sdgs.un.org. Accessed: Jun. 5, 2024. [Online]. Available: https://sdgs.un.org/un-system-sdg-implementation/international-telecommunication-union-itu-54247

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[3] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Labs Technical Journal,* vol. 27, no. 3, pp. 379-423, Jul. 1948. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[4] J. Von Neumann, "First draft of a report on the EDVAC," in *IEEE Annals of the History of Computing,* vol. 15, no. 4, pp. 27-75, Dec. 1993. https://doi.org/10.1109/85.238389

[5] S. Singh, *The Code Book: The Secrets Behind Codebreaking,* New York, NY, USA: Penguin random, 2002. https://www.penguinrandomhouse.com/books/168003/the-code-book-the-secrets-behind-codebreaking-by-simon-singh/9780375890123/

[6] K M. M. de Leeuw, and J. Bergstra, Eds, "Computer Security" in *The history of Information Security: A comprehensive handbook*. Londres, Inglaterra: Elsevier Science, 2007. https://shop.elsevier.com/books/the-history-of-information-security/de-leeuw/978-0-444-51608-4

[7] Y. Yu, "Preface to special topic on lattice-based cryptography," *National Science Review,* vol. 8, no. 9, Sep. 2021. https://doi.org/10.1093/nsr/nwab154

[8] M. J. Lucena López, *Criptografía y Seguridad en Computadores*, Jaen: Universidad de Jaén, 2022. https://ccia.esei.uvigo.es/docencia/SSI/cripto.pdf

[9] A. Yaghouti Niyat, and M. H. Moattar, "Color image encryption based on hybrid chaotic system and DNA sequences," *Multimedia Tools and Applications,* vol. 79, p. 1497–1518, Jan. 2020. https://doi.org/10.1007/s11042-019-08247-z

[10] M. M. Savchuk, and A. V. Fesenko, "Quantum Computing: Survey and Analysis," *Cybernetics and Systems Analysis,* vol. 55, pp. 10-21, Jan. 2019. https://doi.org/10.1007/s10559-019-00107-w

[11] L. M. Cortés Martinez, L. D. Alvarado Nieto, and E. I. Amaya Barrera, "Composite cellular automata based encryption method applied to surveillance videos," *Dyna (Medellin)*, vol. 87, no. 213, pp. 212–221, Apr. 2020. https://doi.org/10.15446/dyna.v87n213.81859

[12] M. Hussain, A. W. Abdul Wahab, Y. I. Bin Idris, A. T. S. Ho, and J. Ki-Hyun, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46-66, Jul. 2018. https://doi.org/10.1016/j.image.2018.03.012

[13] 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. https://doi.org/10.1016/j.jksuci.2019.12.007

[14] B. Stoyanov, and K. Kordov, "Novel secure pseudo-random number generation scheme based on two Tinkerbell maps," *Adv. Stud. Theor. Phys.*, vol. 9, no. 9, pp. 411–421, 2015. https://www.m-hikari.com/astp/astp2015/astp9-12-2015/p/stoyanovASTP9-12-2015.pdf

[15] F. Y. Shih, *Digital Watermarking and Steganography,* Boca Ratón: CRC Press, 2017. https://doi.org/10.1201/9781315121109

[16] M. Hassaballah, *Digital media steganography: Principles, algorithms, and advances*. San Diego, CA, Estados Unidos de América: Academic Press, 2020. https://doi.org/10.1016/C2018-0-04865-3

[17] V. Lyubashevsky, "Lattice-based digital signatures," *National Science Review*, vol. 8, no. 9, Sep. 2021. https://doi.org/10.1093/nsr/nwab077

[18] R. S. Phadte, and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," in *2017 International Conference on Computing Methodologies and Communication (ICCMC),* Erode, India, 2017, pp. 230-235. https://doi.org/10.1109/ICCMC.2017.8282682

[19] T. Saha, S. Sengupta and T. Dasgupta, "Chaotic cipher based spatial domain steganography with strong resistance against statistical attacks," in *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Kolkata, India, 2017, pp. 365-370. https://doi.org/10.1109/ICRCICN.2017.8234536

[20] A. Flores-Vergara *et al.*, "Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 497–516, 2019. https://doi.org/10.1007/s11071-019-04802-3

[21] I. Cherkaoui, and F. Zinoun, "On the use of Egyptian fractions for stream ciphers," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 1, pp. 139-152, Nov. 2021. https://doi.org/10.1080/09720529.2021.1923921

[22] Y. Satria, M. T. Suryadi and D. J. Cahyadi, "Digital text and digital image encryption and steganography method based on SIYu map and least significant bit," *Journal of Physics Conference Series,* vol. 1821, no. 1, p. 012035, Mar. 2021. https://doi.org/10.1088/1742-6596/1821/1/012035

[23] S. Kumar, P. K. Srivastava, G. K. Srivastava, P. Singhal, D. Singh, and D. Goyal, "Chaos based image encryption security in cloud computing," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 25, no. 4, pp. 1041-1051, Jun. 2022. https://doi.org/10.1080/09720529.2022.2075085

[24] H. El Bourakkadi, A. Chemlal, H. Tabti, M. Kattass, A. Jarjar, and A. Benazzi, "Improved Vigenere approach incorporating pseudorandom affine functions for encrypting color images," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 14, no. 3, pp. 2684-2694, Jun. 2024. https://doi.org/10.11591/ijece.v14i3

[25] J. Mohammed and D. R. Nayak, "An efficient edge detection technique by two dimensional rectangular cellular automata," in *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, India, 2014, pp. 1-4. https://doi.org/10.1109/ICICES.2014.7033847

[26] S. Kumar, A. Singh, and M. Kumar, "Information hiding with adaptive steganography based on novel fuzzy edge identification," *Defence Technology,* vol. 15, no. 2, pp. 162-169, Apr. 2019. https://doi.org/10.1016/j.dt.2018.08.003

[27] B. Lakshmi Sirisha, and B. Chandra Mohan, "Review on spatial domain image steganography techniques," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 24, no. 6, pp. 1873-1883, Sep. 2021. https://doi.org/10.1080/09720529.2021.1962025

[28] S. Amrogowicz, Y. Zhao, and Y. Zhao, "An edge detection method using outer Totalistic Cellular Automata," *Neurocomputing,* vol. 214, pp. 643-653, Nov. 2016. https://doi.org/10.1016/j.neucom.2016.05.092

[29] A. Kumar, and S. K. Sharma, "Information cryptography using cellular automata and digital image processing," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 25, no. 4, pp. 1105-1111, 2022. https://doi.org/10.1080/09720529.2022.2072437

[30] 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. https://doi.org/10.1016/j.icte.2018.01.003

[31] M. Arias Cárdenas, "Criptosistema Esteganográfico a través de Imágenes Digitales para el Cifrado de Texto Usando Teoría del Caos y Autómatas Celulares," Tesis de grado, Universidad Distrital Francisco

José de Caldas, Bogotá, 2020. https://repository.udistrital.edu.co/items/a34dbf52-d2c1-40f9-a1dc-a6d9ec463ab4

[32] OpenSSL Corporation, "OpenSSL Cryptography and SSL/TLS Toolkit," openssl.org. Accessed: [Online]. Available: https://www.openssl.org/. https://www.openssl.org/

[33] W. Diffie, and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976. https://doi.org/10.1109/TIT.1976.1055638

[34] G. Van Rossum. *Python Software.* V3.13, (2024). Centrum Wiskunde & Informatica (CWI). Netherlands. [Online]. Available: http://www.Python.org

[35] S. Yuan, T. Jiang, and Z. Jing, "Bifurcation and Chaos in the Tinkerbell Map," *International Journal of Bifurcation and Chaos,* vol. 21, no. 11, pp. 3137-3156, 2011. https://doi.org/10.1142/S0218127411030581

[36] USC Viterbi School of Engineering, "Signal and Image Processing Institute," sipi.usc.edu. Accessed: Jun. 5, 2009. [Online]. Available: https://sipi.usc.edu/database/database.php

[37] L. Pardo LLorente, "Teoría de la información estadística," *Estadística Española,* vol. 35, no. 133, pp. 195-268, 1993. https://halweb.uc3m.es/esp/Personal/personas/dpena/publications/castellano/1993EE_pardo _ coment.pdf

[38] A. Saha, N. Manna, and S. Mandal, "India," in *Information theory, coding and cryptography:* Pearson Education, 2013. https://books.google.com.co/books/about/Information_Theory_Coding_and_Cryptograp.html?id=iUI8BAAAQBAJ&redir_esc=y

Notes

5. 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.

CONFLICTS OF INTEREST The authors declare that there is no conflict of interest.

AUTHOR CONTRIBUTIONS

Marlon Arias-Cárdenas: Conceptualization, Software, Validation, Data Curation, Writing Original Draft.
Deicy Alvarado-Nieto: Conceptualization, Formal analysis, Investigation, Formal, Writing -Review & Editing, Supervision, Project administration.
Isabel Amaya-Barrera: Conceptualization, Formal analysis, Investigation, Formal, Writing -Review & Editing, Supervision, Project administration.
All authors have read and agreed to the published version of the manuscript.

Información adicional

How to cite / Cómo citar: M. Arias-Cárdenas, D. Alvarado-Nieto, and I. Amaya-Barrera, "Steganographic Cryptosystem Based on the Use of Chaos Theory and Cellular Automata," *TecnoLógicas*, vol. 27, no. 61, e3132, 2024. https://doi.org/10.22430/22565337.3132

Enlace alternativo

https://revistas.itm.edu.co/index.php/tecnologicas/issue/view/142 (html)

Marlon Arias-Cárdenas, Deicy Alvarado-Nieto,
Isabel Amaya-Barrera

Steganographic Cryptosystem Based on the Use of Chaos Theory and Cellular Automata
Criptosistema esteganográfico basado en el uso de teoría del caos y autómatas celulares

TecnoLógicas
vol. 27, núm. 61, e3132, 2024
Instituto Tecnológico Metropolitano, Colombia
tecnologicas@itm.edu.co

ISSN: 0123-7799
ISSN-E: 2256-5337

DOI: https://doi.org/10.22430/22565337.3132