Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi
International Journal of Engineering Research and Development

UMAGD, (2023) 15(3), s309-s317.

10.29137/umagd.1399028

Cilt/Volume:15 Sayı/Issue:3 Aralık/December 2023 Özel Sayı/Special Issue

Araştırma Makalesi / Research Article

Image Encryption Implementation by Using Memristor Based Chaotic Systems and DNA Coding

Cagri CANDAN[1], Hasan ULUTAS*

[1]*Yozgat Bozok University, Department of Computer Engineering, Yozgat, TURKIYE*

***Başvuru/Received**: 02/12/2023* ***Kabul / Accepted**: 27/12/2023* ***Çevrimiçi Basım / Published Online:** 31/12/2023*

***Son Versiyon/Final Version**: 31/12/2023*

Abstract

The rapid advancement of internet technologies has accentuated the need for robust data security mechanisms, particularly in the realm of image transmission. Addressing this, our study introduces a cutting-edge encryption system that blends arithmetic operations with DNA-inspired biological processes and the complexity of chaotic systems, presenting a significant evolution in encryption methodologies. The system employs a synergetic fusion of DNA-based encryption and XOR operations, bolstered by a memristor-based chaotic system, to heighten the security barriers of image encryption. This innovative approach not only provides a secure means to transmit images over the internet but also lays new groundwork in the field of cryptographic research. Rigorous security analyses, including correlation, histogram, and differential attack assessments, are performed, with the findings validating the robustness and efficacy of the encryption process. The findings of this research, by offering an enhanced method that could provide a distinct perspective on information protection in an increasingly digitized world, expand the discourse on data security.

Key Words

"Chaos, DNA encoding, Image encryption, Memristor, Security tests"

***Sorumlu Yazar:** hasan.ulutas@bozok.edu.tr*

1. Introduction

As internet and network technology continue to expand, the transmission of information across networks has risen, giving rise to increased security risks for users. Therefore, information security has become necessary for modern computing systems. Modern systems protect their data against security threats with cryptography applications. These currently used cryptography methods work with a lot of mathematical operations and a system of private keys. Although it seems safe, security vulnerabilities in algorithms are emerging every day. Various cryptological systems attract the attention of researchers by focusing on the randomness of chaotic systems and the rich dynamics they offer. In many of these proposed studies, it is aimed to hide data with unpredictable trajectories resulting from the sensitive dependence of chaotic systems on initial conditions and control parameters (Jakimoski and Kocarev, 2001; Amigó, Kocarev and Szczepanski, 2007; Özkaynak, Özer and Yavuz, 2013; Candan and Şahin, 2023; Sahin, 2023). The security encryption processes necessary for storing and transmitting images can be ensured. Chaotic maps are widely employed in secure communication and are considered a factor that balances data security with computational speed (Gu and Ling, 2014). For these reasons, chaotic maps have been extensively used in various image encryption applications. Image encryption applications frequently utilize chaotic systems, with approaches including one-dimensional chaotic-based algorithms (Pareek, Patidar and Sud, 2006) and two or multi-dimensional chaotic-based algorithms (Peng, Zhang and Liao, 2009). Another notable avenue involves hybrid methods, wherein encryption algorithms are craeted by integrating other encryption techniques and chaotic systems within the same framework (Chen, Mao and Chui, 2004). These methods leverage the unique properties of chaotic systems to enhance the security of image data.

DNA encoding is the modern field of cryptography with many features such as low power usage, large storage space and parallelism. They are cryptosystems with four complementary rules: addition, subtraction, XOR and XNOR DNA operations. DNA encoding represents the biological technique within DNA computation (Şahin, 2023). Encrypted images are obtained as a result of DNA encoding for the image, first of all, DNA coding is done and after the DNA processes are applied, the DNA code is decoded and converted back to its original state. There are studies using DNA coding in the literature (Chen, 2003; Tanaka, Okamoto and Saito, 2005; Amin, Saeb and El-Gindi, 2006; Şahin, 2023). Wei et al. introduced a technique for encoding images based on DNA, utilizing a hyper-chaotic system specifically designed for color images (Wei *et al.*, 2012). The suggested approach demonstrated resilience against comprehensive attacks, statistical attacks, and various other forms of attacks. Zhang et al. incorporated DNA encoding, image fusion, and a hyper-chaotic system in their method. The simulation results showcased robust encryption effects and the capability to withstand both extensive and statistical attacks (Zhang, Xue and Wei, 2012).

In this study, the simple theory of DNA sequence processing is used for image coding, and memristor chaotic map and DNA sequence are combined to implement image coding. Although the memristor element is widely used in chaotic systems, memristor-based systems in cryptology applications are not very common in the literature. In this study, using the advantages of the memristor element to chaotic systems, the usability of this element in cryptology applications is presented. The security analyses of the implemented system are presented with correlation analysis, histogram analysis and differential attack analysis. The structure of this paper is following. Section 2 provides information on chaos-based cryptosystems and DNA encoding. In Section 3, the methods used for encryption and decryption are described in detail, along with how well they perform in terms of security analysis and experimental findings. The systems' results are submitted in Section 4.

2. Material and Methods

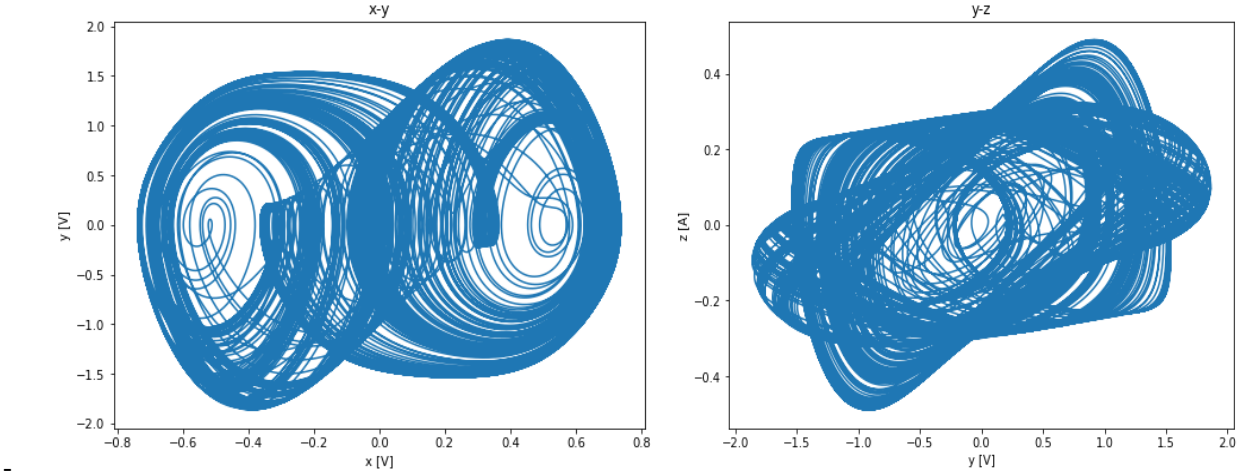
Text encryption operates under different principles compared to image encryption, primarily due to the differing nature of their data formats. As an alternative, chaos-based encryption works well with chaotic theory and maps. Details on chaotic systems and DNA encoding are provided in this section. Then, an application for image encryption is created using DNA encoding and memristor chaotic maps.

2.1. Memristor-based chaotic system

The encryption system employs a chaotic system based on memristor. The literature describes the derivation of a 4D chaotic system using a configuration involving two memristor (Lai *et al.*, 2021). The mathematical expression for the memristor based chaotic system is given in Eq. (1).

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= a[z - (-0.1 + x^2)y] \\ \dot{z} &= y - b(-0.1 + w^2)z + w \\ \dot{w} &= -cz \end{aligned} \tag{1}$$

The system parameters were chosen as follows: a = 20, b = 0.5, c = 34.84 and initial states are selected as (0, 0, 0.1, 0). The study involved 10,000 iterations conducted on the MATLAB platform. The state equations of the chaotic system are obtained, and the system's phase portraits are illustrated in Figure 1.



(*a*) (*b*)

Figure 1. Phase portraits of memristor based chaotic system (a) *x-y* plane and (b) *y-z* plane

2.2. Scheme of Encrypted System

DNA sequencing is the process of identifying the nucleic acid or nucleotide sequence in DNA. The basic building blocks of DNA are adenine, guanine, cytosine, and thymine, with guanine and cytosine pairing together, as do adenine and thymine. In digital image processing, each pixel of an image is typically represented by an eight-bit binary number. In this binary system, 0 and 1 are complementary, as are 00 and 11, and 01 and 10. Using 00, 11, 01, and 10 to represent A, T, G, and C, respectively, allows for the representation of each pixel with a nucleotide sequence. For example, a pixel value of 223, with a binary representation of 11100001, corresponds to the nucleotide sequence "TCAG" following the specified rules. While there are 24 possible combinations of these four nucleotides, the complementarity principle applies to only eight coding combinations, as outlined in Table 1. Table 1 illustrates the DNA encoding system used in our study, detailing the binary to nucleotide mappings. During coding, nucleotides are substituted using the DNA complement rule. The encryption strength can be increased by randomly selecting any rule. Rule 1 is chosen for coding in the study.

Table 1. DNA encoding system

Rule	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00	A	A	T	T	G	G	C	C
01	G	C	G	C	A	T	A	T
10	C	G	C	G	T	A	T	A
11	T	T	A	A	C	C	G	G

2.3. DNA encoding process

The pixel values are modified to ensure a significant distinction between the histograms of the encrypted image and the original image. For this, we need to do some sort of operation between pixel values. The values are encoded in the DNA sequence, so we need to do the DNA manipulations. DNA nucleotides include addition, subtraction and XOR operations. By altering the pixel values through DNA encoding, the histogram of the encrypted image significantly diverges from that of the original, enhancing encryption security. In the study, DNA XOR process is used for encryption. The XOR of all possible combinations is shown in Table 2. Table 2 showcases the DNA XOR process used for encryption, illustrating how this operation contributes to the robustness of the encryption.

Table 2. DNA and XOR process

XOR	**A**	**G**	**C**	**T**
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

3. Experimental Results

As of today, the cryptography industry is increasingly significant, with new methods emerging regularly. One of the recently developed and widely adopted approaches is DNA-based encryption, a model that simulates the four bases found in the human DNA structure within a computer environment. This innovative encryption method involves hybridizing DNA structures with chaotic systems to enhance security. The block diagram of the encrypted system, as illustrated in Figure 2, provides a visual guide through the encryption process. It begins with the original image, which undergoes confusion to increase complexity. A secret key is generated from this image using the SHA-256 hash algorithm, ensuring secure encryption. The subsequent DNA encoding translates image pixels into DNA sequences, capturing the essence of biological principles in computational form. Through DNA operations and XOR processes, the methodology effectively scrambles the information, with the DNA decoded output forming the encrypted image. The study, which leverages this intricate encryption process, is implemented on the Python platform using Google Colab, showcasing the practical application of these theoretical concepts. Figure 3 depicts the image utilized in the study, demonstrating the encryption's impact visually. The detailed steps of the system's coding procedure are provided below, illustrating how each phase Enhances the resilience of the encryption.

Step 1: Secret key generating
The input image is a 3-channel matrix in RGB format. Let this image be represented by the (M, N, O) size matrix A.
A= A(i,j,k)
i=1,2,……,M and j=1,2,….., N and k=1,2,……,O
Here A(i, j, k) represents the value of the image pixel in (i, j, k). First, the given 3-dimensional matrix is converted into a 1-dimensional array, and a secret key is generated using the SHA-256 algorithm, which converts it to 256-bit code.
Step 2: The original image (Image dimensions: 1201X801 pixels) is divided into three different matrices, red, green and blue, and these matrices are converted to binary matrices.
Step 3: By choosing one of the rules in Table 1, these matrices are encoded into the DNA sequence.
For example, for rule 1

01 11 10 00	$(120)_{10}$	G T C A
10 00 11 10	$(142)_{10}$	C A T C
00 01 11 01	$(29)_{10}$	A G T G
01 10 10 10	$(106)_{10}$	G C C C

Step 4: Similarly, the secret key generated in step 2 is converted into a 2-dimensional matrix and this matrix is encoded into the key DNA sequence.
Step 5: In this step, XOR is performed between each DNA encoded matrix and DNA encoded matrix key using the XOR operation shown in Table 2.
Step 6: Three chaotic sequences are created using the memristor chaotic system.
X1 = $\{x_1, x_2, x_3, \ldots, x_k\}$,
X2= $\{x_1, x_2, x_3, \ldots\ldots, x_k\}$ and,
X3 = $\{x_1, x_2, x_3, \ldots\ldots, x_k\}$ (The elements of each array are different from each other.)
Step 7: To mix the values of the R, G, B matrix, 3 more arrays such as X1_sort, X2_sort, X3_sort are created.
X1_sort = sort(X1);
X2_sort = sort(X2);
X3_sort = sort(X3);
Since the matrix R is a 2 dimensional array and X1 is a 1 dimensional array this matrix is converted to a 1 dimensional array and a matrix is created again after mixing. The arrays X1_sort, X2_sort, and X3_sort obtained during the sorting process represent the index values obtained when sorting chaotic values in ascending order. These index values are then used to confuse the image.
Step 8: The generated chaotic sequences are encoded using Table 1 and XOR with image pixels using Table 2.
Step 9: The three DNA encoded scrambled matrices are converted back into binary matrices and combined to get the encoded image.
Step 10: The process for decrypting the image is the reverse of the encryption process. The secret key created in step 1 is used for decryption.

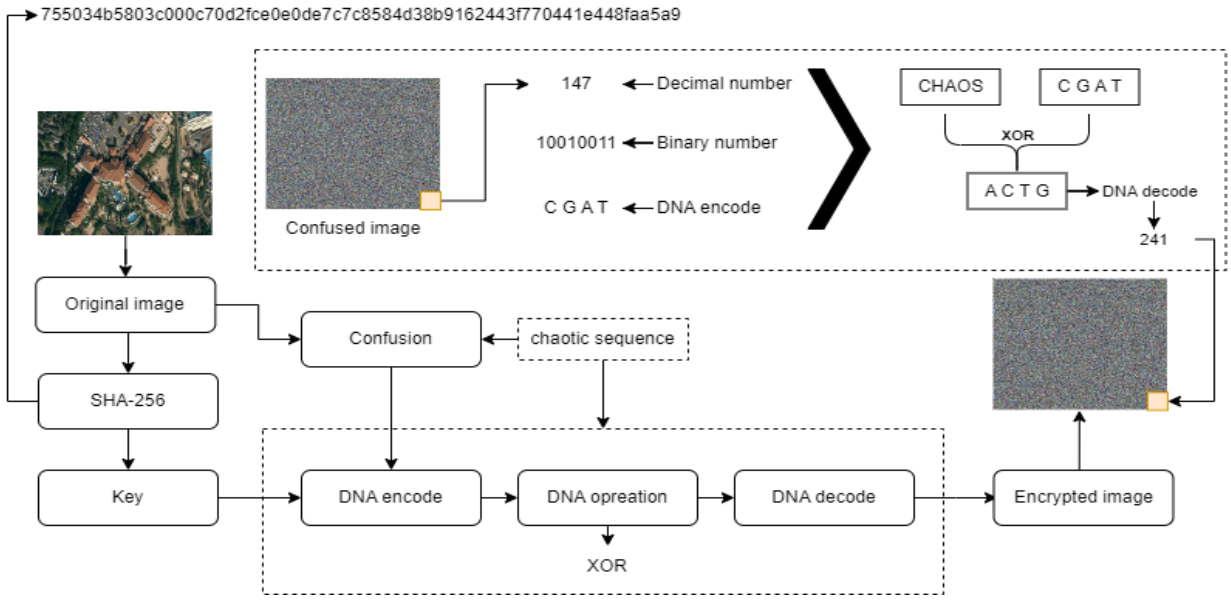
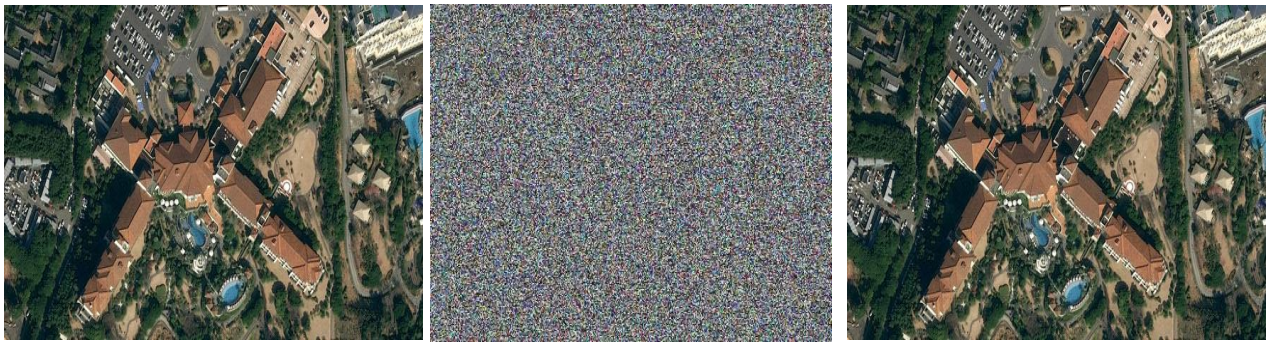


Figure 2. Block diagram of encrypted system

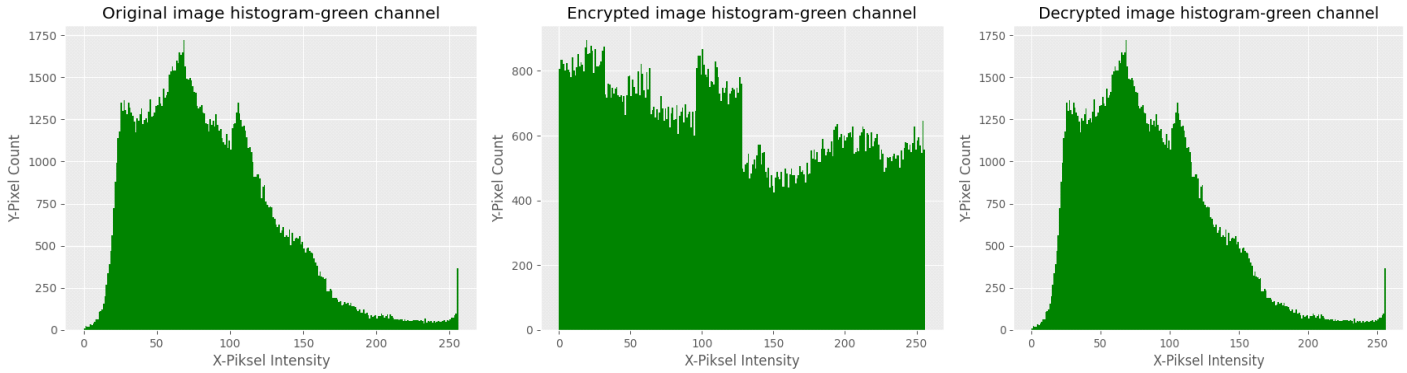


(*a*) (*b*) (*c*)

Figure 3. (*a*). Original Image (*b*). Encrypted image (*c*). Decrypted image

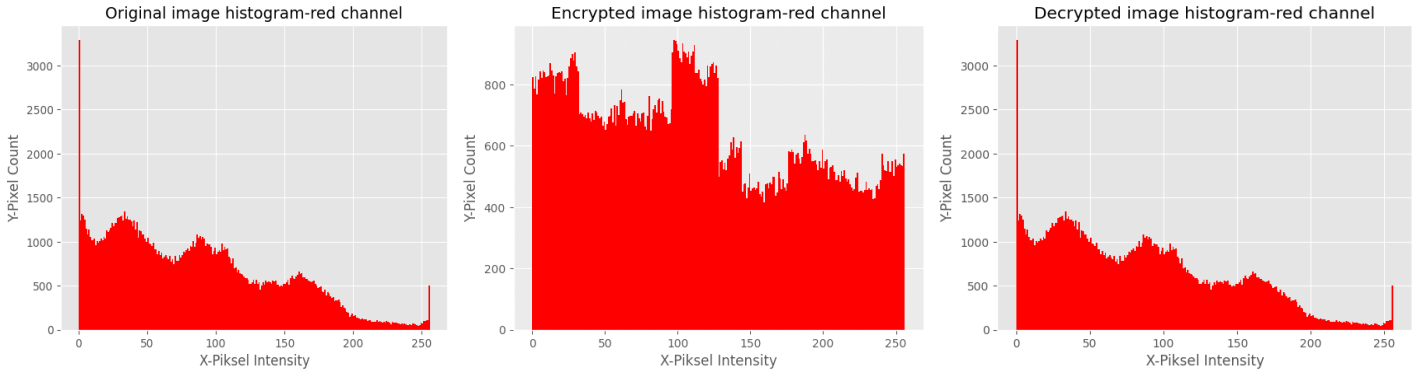
3.1. Histogram Analyses

The distribution of pixels within an image is effectively represented through histogram plots, which are critical in evaluating the efficacy of encryption processes. Histogram graphics, extracted from images, can inadvertently reveal information, hence, the histogram of an encrypted image should ideally be as uniform as possible to minimize information leakage (Wang, Teng and Qin, 2012; Alawida *et al.*, 2019). Figures 4-6 display the RGB (Red-Green-Blue) channel histogram graphs for the original, encrypted, and decrypted images, respectively. These histograms visually illustrate the differences in pixel intensity distribution across the three stages. For instance, the encrypted image's blue channel histogram (Figure 4a) shows a uniform distribution, concealing any discernible patterns and thereby reducing the potential for information leakage. In contrast, the original image's blue channel histogram (Figure 4b) exhibits peaks at certain pixel intensities, while the decrypted image's blue channel histogram (Figure 4c) mirrors the original image, confirming the restoration of the pixel distribution post-decryption. Similarly, the encrypted image histograms for the red and green channels demonstrate a flattened profile, which indicates an even distribution of pixel intensities, enhancing the randomness and security of the encryption. Conversely, the histograms of the decrypted image re-establish the original distribution, validating the effectiveness of the decryption process. Thus, the histograms presented in Figures 4-6 succinctly demonstrate the impact of the encryption and decryption processes on the pixel intensity distribution, affirming that the employed encryption method successfully obscures and subsequently recovers the image information.



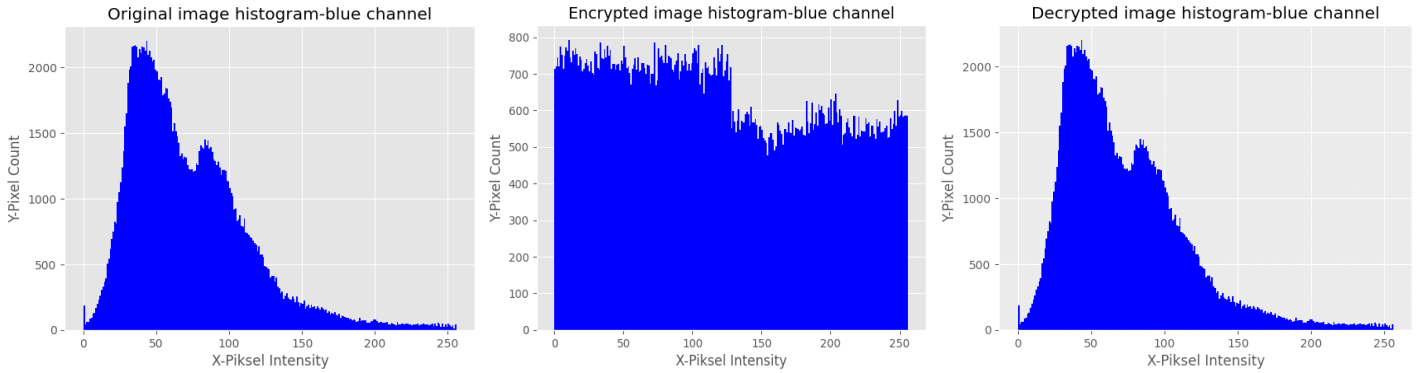
(*a*) (*b*) (*c*)

Figure 4. Green channel histogram plot of image (a) Original (b) Encrypted (c) Decrypted



(*a*) (*b*) (*c*)

Figure 5. Red channel histogram plot of image (a) Original (b) Encrypted (c) Decrypted



(*a*) (*b*) (*c*)

Figure 6. Blue channel histogram plot of image (a) Original (b) Encrypted (c) Decrypted

3.2. Correlation Analysis

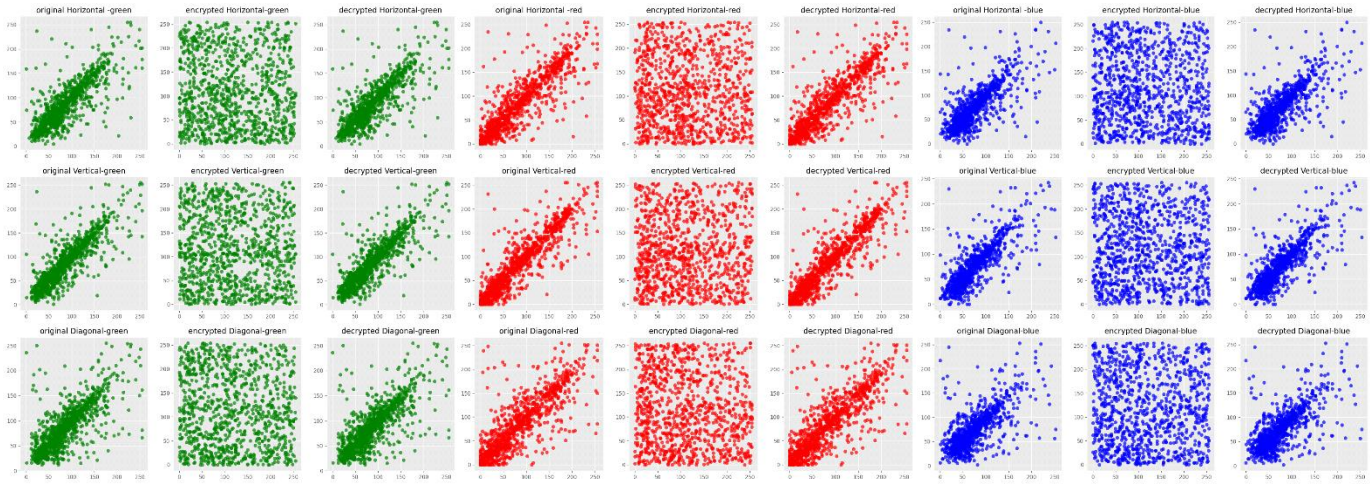
In probability theory and statistics, the concept of correlation displays the direction and size of the linear relationship between two random variables (Bandyopadhyay, Bhattacharyya and Das, 2008). High correlation between adjacent pixels is typical in a flat image. For an image that has undergone good encryption, we expect correlation values to decrease significantly, indicating a reduction of recognizable patterns in the image data. The correlation between adjacent pixels can be quantified using Eq. 2:

$$P_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{2}$$

where *x* and *y* represent the pixel values and D(x) and D(y) their respective standard deviations. Ideally, the absolute correlation value between neighboring pixels in an encrypted image should approach zero, signifying robust and efficient encryption (Yildirim, 2021). Figure 7 and the associated Table 3, which would typically show the correlation values, illustrate this principle. The depicted correlation distribution graphs for the original, encrypted, and decrypted images in the blue, red, and green channels demonstrate a substantial decrease in correlation in the encrypted images compared to the original ones, thus confirming the encryption's effectiveness in disrupting the linear relationships inherent in the unencrypted image data.

Table 3. Results of correlation analysis

Channel	Original horizontal correlation	Original vertical correlation	Original diagonal correlation	Encrypt horizontal correlation	Encrypt vertical correlation	Encrypt diagonal correlation
Red	0.8617	0.8989	0.8185	-0.0219	0.0222	-0.0817
Green	0.7968	0.8447	0.7316	-0.0586	-0.0340	-0.0499
Blue	0.7509	0.8101	0.6757	-0.0356	-0.0265	-0.0050



(*a*) (*b*) (*c*)

Figure 7. (a) Correlation graph plots of the red channel original, encrypted and decoded image (b) Correlation graph plots of the green channel original, encrypted and decoded image (c) Correlation graph plots of the blue original, encrypted and decoded image

3.3. Differential attack analysis

The combined average intensity of change (UACI) and the pixel rate of change (NPCR), two widely used metrics, are frequently used to assess how well an encryption method can fend off various attacks. While UACI shows the average difference density between two encrypted images, NPCR shows the percentage of different pixel counts between two encrypted images. An effective encryption method is characterized by high NPCR and UACI values. NPCR and UACI are defined as in the Eqs. (3)-(5):

$$D(i,j) = \begin{cases} 1, C_{o1}(i,j) \neq C_{o2}(i,j) \\ 0, C_{o1}(i,j) = C_{o2}(i,j) \end{cases} \tag{3}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_{o1}(i,j) - C_{o2}(i,j)}{255}\right] \times 100\% \tag{4}$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \tag{5}$$

In this study NPCR and UACI are obtained as 99.605 and 33.247, respectively. According to these results, it has been determined that the developed encryption algorithm has a structure resistant to differential attacks. The high NPCR and UACI values obtained in our

study suggest a strong resistance against differential attacks, indicating that even minor changes in the input lead to significant differences in the encrypted output.

4. Discussion

The incorporation of a chaotic system based on memristors, DNA encoding, and XOR operations in the suggested image encryption approach represents a noteworthy progression in cryptographic methods. This unique integration represents a significant departure from traditional cryptographic methods, introducing a novel approach to image encryption. The memristor-based chaotic system introduces a dynamic and complex element, providing a solid foundation for the subsequent encryption steps. The utilization of DNA encoding, guided by the complement rule outlined in Table 1, coupled with XOR operations, showcases a novel fusion of biological principles and computational processes. Thorough security analyses, including correlation analysis, histogram analysis, and differential attack analysis, validate the effectiveness of the encryption process. Compared to existing methods, our approach demonstrates superior performance in terms of correlation values, histogram patterns, and NPCR and UACI metrics, underscoring its robustness against various cryptographic attacks. The low correlation values, distinct histogram patterns, and high NPCR and UACI values collectively indicate the robustness of the encryption algorithm against various attacks. Looking forward, there is potential for further refinement and application of the proposed encryption model in real-world scenarios such as secure communication, data storage, and digital media protection, emphasizing the ongoing commitment to advancing encryption technologies for enhanced security and performance across diverse environments.

5. Conclusion

Chaotic systems, characterized by their inherent randomness, ergodicity, and sensitivity to initial conditions, inherently possess mixing and diffusion properties crucial for cryptographic applications. Leveraging the dynamic features of chaotic systems and introducing a DNA-XOR-based hybrid encryption algorithm, this study has successfully implemented robust, durable, and high-performance image encryption applications. The employed chaotic system utilizes a memristor-based circuit model, providing a unique perspective to the research. Comprehensive security and performance analyses of the encryption applications have been conducted, with the results disclosed. In the future, there are intentions to further enhance the practical application of encryption algorithms created through the proposed model in real-world situations. In the future, our research endeavors will be directed towards further enhancing the practical applicability of encryption algorithms developed through the proposed model in real-world scenarios. One of the primary areas of focus will be addressing the challenges associated with scalability and seamless integration of our encryption solutions into existing systems. We recognize the importance of ensuring that our cryptographic techniques can adapt to varying scales of data and diverse technological infrastructures.

Acknowledge

References

Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160, 45-58.

Amigo, J. M., Kocarev, L., & Szczepanski, J. (2007). Theory and practice of chaotic cryptography. Physics Letters A, 366(3), 211-216.

Amin, S. T., Saeb, M., & El-Gindi, S. (2006, November). A DNA-based implementation of YAEA encryption algorithm. In Computational intelligence (pp. 120-125).

Bandyopadhyay, S. K., Bhattacharyya, D., & Das, P. (2008, June). Handwritten signature recognition using departure of images from independence. In 2008 3rd IEEE Conference on Industrial Electronics and Applications (pp. 964-969). IEEE.

Candan, C., Şahin, M. E., (2023). Gömülü sistemlerde kaotik haritalar kullanılarak gerçek zamanlı görüntü şifreleme uygulaması. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 11(2), 1037-1047.

Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749-761.

Chen, J. (2003, May). A DNA-based, biomolecular cryptography design. In 2003 IEEE International Symposium on Circuits and Systems (ISCAS) (Vol. 3, pp. III-III). IEEE.

Gu, G., & Ling, J. (2014). A fast image encryption method by using chaotic 3D cat maps. Optik, 125(17), 4700-4705.

Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers based on chaotic maps. Ieee transactions on circuits and systems i: fundamental theory and applications, 48(2), 163-169.

Lai, Q., Wan, Z., Kengne, L. K., Kuate, P. D. K., & Chen, C. (2020). Two-memristor-based chaotic system with infinite coexisting attractors. IEEE Transactions on Circuits and Systems II: Express Briefs, 68(6), 2197-2201.

Özkaynak, F., Özer, A. B., & Yavuz, S. (2013, April). Security analysis of an image encryption algorithm based on chaos and DNA encoding. In 2013 21st Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and vision computing, 24(9), 926-934.

Peng, J., Zhang, D., & Liao, X. (2009). A digital image encryption algorithm based on hyper-chaotic cellular neural network. Fundamenta Informaticae, 90(3), 269-282.

Sahin, M. E. (2023). Memristive chaotic system-based hybrid image encryption application with AES and RSA algorithms. Physica Scripta, 98(7), 075216.

Şahin, M. E. (2023). Memristor-based hyperchaotic system and DNA encoding based image encryption application on LabVIEW. International Journal of Engineering Research and Development, 15(1), 269-276.

Tanaka, K., Okamoto, A., & Saito, I. (2005). Public-key system using DNA as a one-way function for key distribution. Biosystems, 81(1), 25-29.

Wang, X., Teng, L., & Qin, X. (2012). A novel colour image encryption algorithm based on chaos. Signal Processing, 92(4), 1101-1108.

Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Journal of Systems and Software, 85(2), 290-299.

Yildirim, M. (2021). A color image encryption scheme reducing the correlations between R, G, B components. Optik, 237, 166728.

Zhang, Q., Xue, X., & Wei, X. (2012). A novel image encryption algorithm based on DNA subsequence operation. The Scientific World Journal, 2012.