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

UMAGD, (2023) 15(1), 269-276.

10.29137/umagd.1239725

Cilt/Volume:15 Sayı/Issue:1 Ocak/January 2023

Araştırma Makalesi / Research Article

Memristor-Based Hyperchaotic System and DNA Encoding Based Image Encryption Application on LabVIEW

Muhammet Emin Şahin[1*]

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

***Başvuru/Received**: 20/01/2023* ***Kabul / Accepted**: 29/01/2023* ***Çevrimiçi Basım / Published Online:** 31/01/2023*

***Son Versiyon/Final Version**: 31/01/2023*

Abstract

The growth of multimedia and communication tools has sped up the data transfer thanks to technological advancements, and ensuring image security has become a crucial doubt, particularly during the transmission and storage of the images. So, when images are sent via a public network, they should be encrypted before being sent to the receiving part. In this study, a memristor-based encryption system with Deoxyribonucleic acid (DNA) coding is proposed on the LabVIEW platform to ensure information security. Firstly, memrsitor based hyperchaotic system is used for chaotic sequence. The images are encrypted using the DNA and XOR arithmetic process on the LabVIEW platform. A memristor-based hyperchaotic system and the combination of techniques used aim to encrypt the image securely. Additionally, security tests; histogram analysis, correlation analysis, differential attack, and entropy analysis, are performed on the proposed system and the results are presented. The aforementioned methods are thoroughly examined and tested to determine their efficacy. It has been determined that the proposed encryption schemes are effective and can therefore be used in real-time applications.

Key Words

"chaos, DNA coding, image encryption, memristor, security tests"

Sorumlu Yazar: emin.sahin@bozok.edu.tr

1. Introduction

Encryption is one of the most important techniques that ensure the secure transmission of digital images and videos transmitted via the network. The unique properties of image or video such as bulk data capacity, strong correlation of adjacent pixels and high data redundancy require encryption algorithms that can address fundamental issues like data storage, speed and security.

Chaotic systems are extremely sensitive to input parameters; a small change in these factors might result in an entirely different output for chaotic maps. Various image encryption applications utilizing chaotic systems are mentioned in the literature (H. Li et al., 2019; Z. Li et al., 2021; Maazouz et al., 2022). This is because chaotic signals have favourable pseudorandom, initial-value sensitive, and long-term unpredictability features, which increase the confusion and dissemination of encrypted data. When studies in the literature are examined; Wenwu Yu and Cao suggested a novel encryption technique based on a chaotic Hopfield neural network with variable delay time (W. Yu and Cao, 2006). Patidar et. al. presented a specially designed symmetric encryption system for color images based on the substitution-diffusion model obtained utilizing chaotic standard maps and chaotic logistic maps (Patidar et al., 2010). Zhi Liang Zhu came up with another chaos-based encryption scheme that uses bitwise permutations of the image to encrypt it (Zhu vd., 2011).

It comes from the concept of DNA cryptography with the evolution of DNA computation. DNA computing provides tremendous parallelism and consumes minimal energy. DNA encryption is a type of encryption that has been created in recent years by considering the completion feature of DNA, its double helix feature and, its ability to be synthesized and transported in different environments (biological, digital). Based on current technology, it is used as an extra step in encryption algorithms that are already in use.

It is not true in encryption processes that the more difficult the encrypted text is to decrypt, the better. In addition, encryption, data transmission, and decryption processes each consume processing energy on existing computers. The better the hard decryption/complexity of the encryption is compared to other algorithms with the current number of transactions, the more useful this encryption algorithm is. A number of image coding techniques using DNA techniques have been proposed in the literature (Chen et al., 2020; Gasimov and Mammadov, 2020; Guesmi et al., 2016; Zhang et al., 2010).

X. Lai et al. proposed asymmetric encryption and signature cryptography based on DNA computation and traditional public key cryptography (Lai et al., 2010). H. Liu et al. proposed an image coding scheme using DNA complement rules and chaotic maps Liu et al., 2012). Q. Zhang et al. described a way for encrypting images using DNA-XOR processes (Zhang and Wei, 2013). An image encryption application is proposed for a chaotic system based on memristors by Zhang et al. (Zhang et al., 2022). Combining the DNA algorithm with an image encoding algorithm, the new system is used to encode the chaotic sequence images, and the results are presented. Using the memristive chaotic system proposed in the study by L. Luo et al., a color image encryption scheme based on DNA coding was proposed, and the scheme's security was tested using statistical analyses and various attacks (L. Luo et al., 2022). In addition, DNA coding and a color image encryption scheme are implemented on the chaotic system ARM platform.

In this paper, a memristor-based encryption system with DNA coding is proposed on the LabVIEW platform to ensure information security. Memristor-based hyperchaotic system is used to construct the algorithm. The images are finally encrypted using DNA and XOR arithmetic on the LabVIEW platform. The security tests (histogram analysis, correlation analysis and NPCR and UACI test and entropy analysis) of the obtained study are performed and the results are presented.

2. Material and Methods

2.1. Memristor-based hyperchaotic system

The memristor is an element whose resistance is characterized by a non-linear relationship between load and flux, presented by L.Chua (Chua, 1971). Memristor-based chaotic systems have attracted the attention of many researchers due to their rich dynamic behavior and therefore they have been widely used in the literature in recent years (Sun et al., 2018; Sahin et al., 2021; Sahin et al., 2021). In this study, a memristor-based chaotic system is preferred for the encryption part. 5D memristive hyperchaotic system has been obtained in the literature (F. Yu et al., 2020). Equation 1 provides the mathematical expression of the utilized hyperchaotic system based on memristor.

$$\begin{aligned} x &= -ax + yz \\ y &= by - xz \\ z &= xy - cz + dw(f + 3gu^2) \\ w &= xy - ew \\ u &= -z \end{aligned} \tag{1}$$

The system parameters of the memristor-based hyperchaotic circuit are selected as a=10, b=12, c=30, d= 2, e=4, f=0.1, g=0.01, and initial states (2, 1, 1, 2, 2). Phase portraits of the circuit are obtained on the LabVIEW platform and are given in Figure 1. Phase portraits of the memristor-based chaotic circuit is shown in Figure 2.

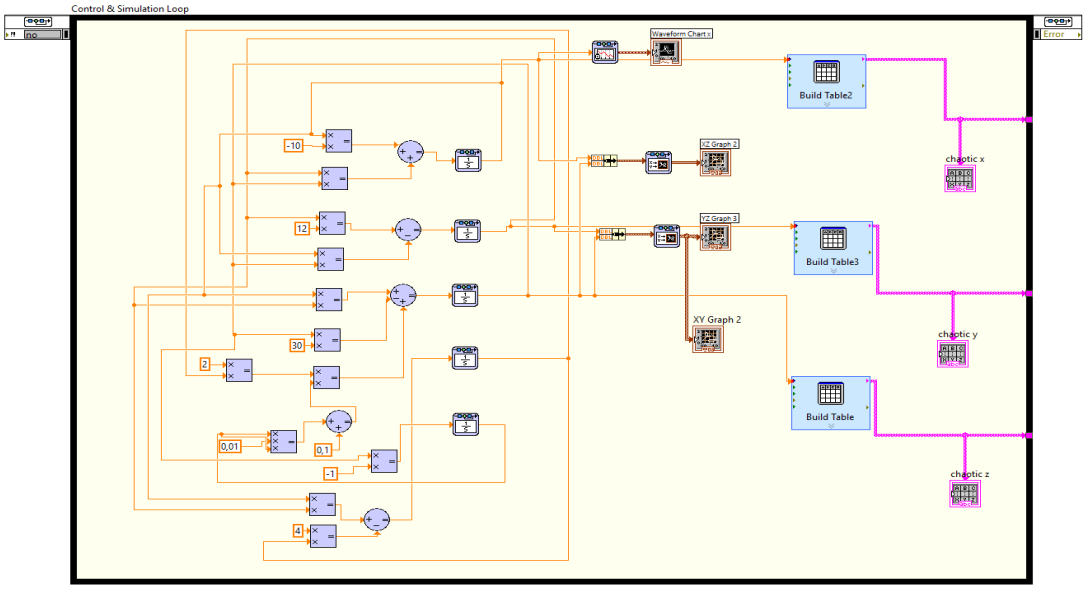
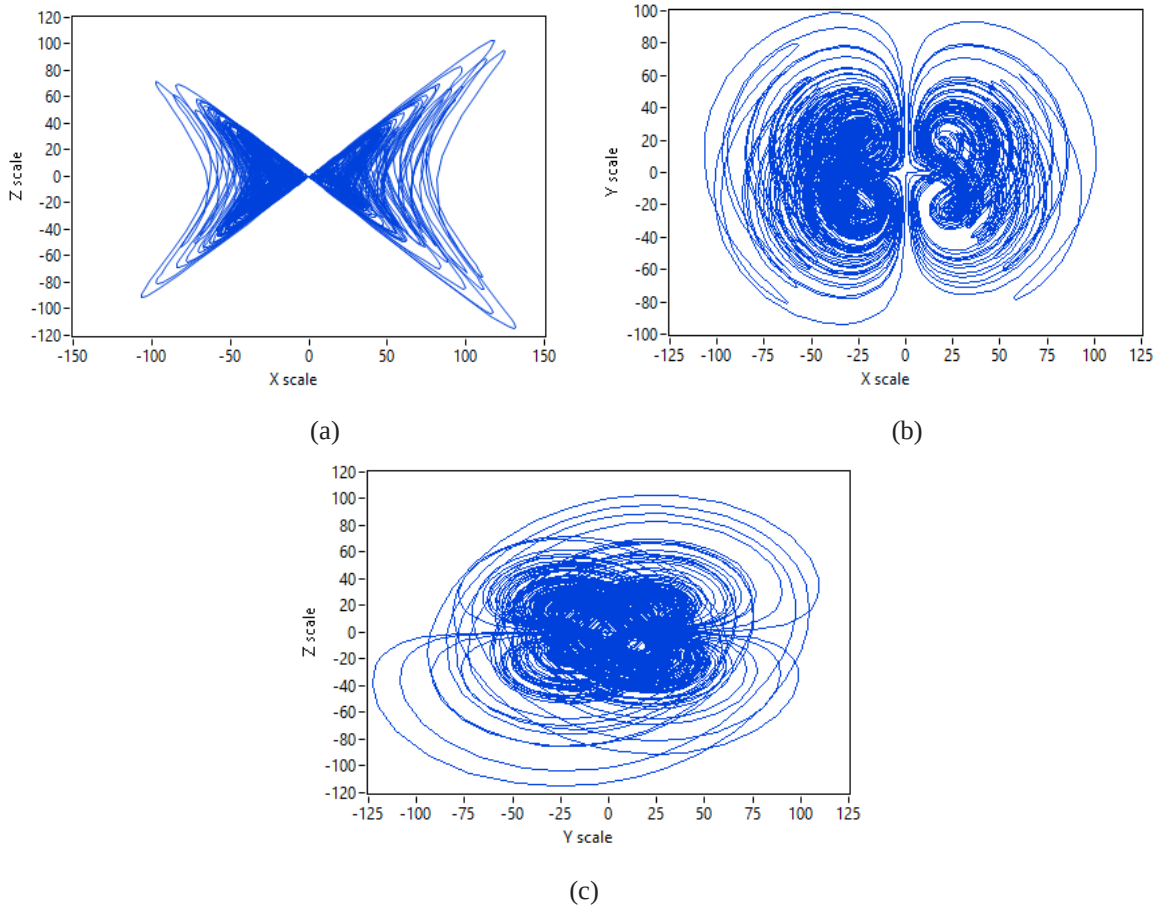


Figure 1. Memristor-based hyperchaotic circuit design on the LabVIEW



(a) (b)

(c)

Figure 2. Phase portraits of the memristor-based hyperchaotic circuit (a) *x-z* plane, (b) *x-y* plane and (c) *y-z* plane

2.2. Scheme of Encrypted System

Deoxyribonucleic acid (DNA) is a genetically encoded nucleic acid. It is a genetic trait necessary for the vitality and biological development of all unicellular or multicellular organisms. The most important role of DNA is to ensure that the genetic characteristics of organisms are passed down from generation to generation (Çelik, 2016).

DNA contains the information necessary to build other components of the cell (such as proteins and Ribonucleic acid). The deoxyribonucleic acid that carries the biological genetic information is called a gene. Deoxyribonucleic acid sequences have functional properties such as defining the shape of chromosomes and regulating how genetic information is used in which cells and under what conditions. There are four types of nucleic acid bases in a DNA sequence: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) (Wen et al., 2019). However, when only four bases are treated according to the principle of complementary base pairs, only eight kinds of coding combinations emerge. A and T, as well as C and G, are essentially complementary to one another. Table 1 presents DNA coding rules.

Table 1. DNA coding rules

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

3. Experimental Results

There are two important situations in image encryption, which are diffusion and permutation. When the pixel values in an image are close to one another, an image emerges. Figure 3 depicts a block diagram of an encrypted system, whereas Figure 4 shows the corresponding images.

The closer the pixel-to-pixel correlation is to zero, the more meaningless the image is. The encryption process specifies this meaningless image. Thanks to features such as complexity found in chaotic systems, the mixing and diffusion steps in the encryption process can be easily completed. First, the *x*, *y* and *z* memristor base chaotic sequences are taken from the hyperchaotic circuit. Then the chaotic sequence x from these taken sequences is used for image mixing. Then, the y-chaotic sequence is used as an XOR, and the z-chaotic sequence is used as the key for the DNA-based encryption process. In this way, our images are encrypted as a result of the structure that goes through three processes.

Step 1 The image from the LabVIEW environment is loaded in *M**N size.

Step 2 Obtaining chaotic sequence values from a memristor-based hyeprchaotic system.

Step 3 Normalizing the *x*, *y* and *z* chaotic sequence values in the designed memristor-based chaotic circuit model (between 0-255). Here *x*', *y*' and *z*' contain normalized chaotic sequences these are our keys.

Step 4 The generated *x*' sequence is used for the confusion step (confusion refers to making the relationship between the key and the cipher text as complex as possible).

To mix the image pixels, X1_sort array is created from the *x*' array.

X1_sort = sort(x');

The image matrix is mixed using the X1_sort array. For example, chaotic array x' = {x1, x2, …. xk} is replaced by the position of x1 in X1_sort and taking a pixel from the image matrix whose position in the array x' is the same as x', this pixel is replaced using the position equal to the position of *x*' in the array X1_sort.

In this way, the mixing step is done.

Step 5 Use the generated *y*' array for the diffusion step (diffusion refers to the property, that redundancy in the statistics of the plain text is dissipated in the statistics of the cipher text), the diffusion step process is created by XOR method the generated chaotic array with the image pixels.

Step 6 The generated *z*' chaotic sequence is used for DNA encoding. During the DNA process, the chaotic values obtained from the *z*' chaotic sequence and the image pixels are coded with DNA and then subjected to the XOR method using the procedures in Table 2. The encoded sequence is DNA decoded using the rules in Table 1. After this step, the encrypted image is obtained.

Table 2. DNA-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

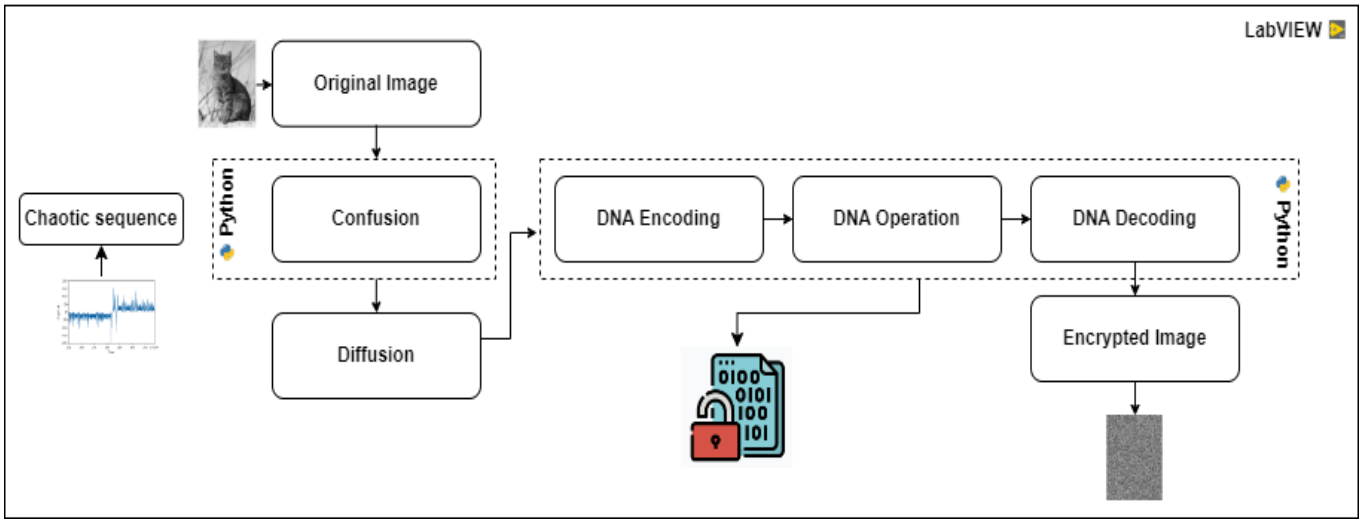
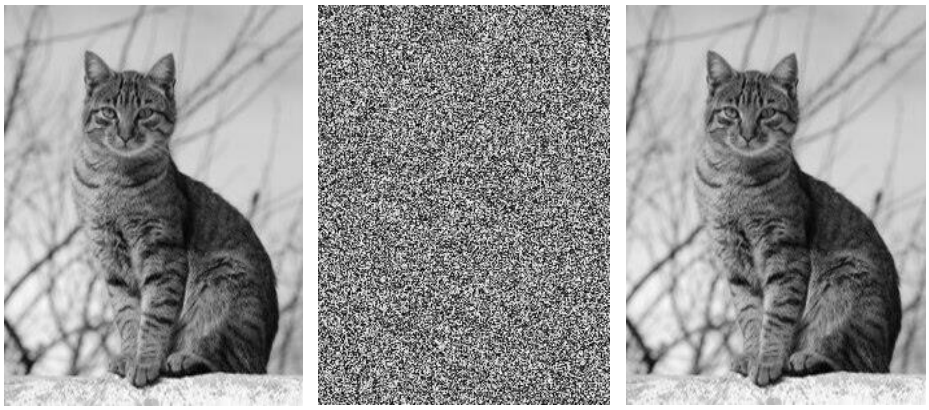


Figure 3. Block diagram of encrypted system



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

Figure 4. (a) Original image (b) Encrypted image (c) decrypted image

3.1. Security Analysis

Histogram Analyses

The image histogram demonstrates the distribution of pixel values in the image. When the histogram of an encrypted image is uniform, each grayscale has the same probability, the encryption technique is more resistant to statistical attacks. Therefore, the optimal histogram plot of an obtained encrypted picture should be in a format that is fully distinct from the original plain image (Chen et al., 2018; Wang et al., 2012).

Figure 5. (a) shows the histogram distribution graph of the original image. Histogram distribution graphs of the encrypted images in Figure 5. (b) and the decoded images are shown in Figure 5. (c). It has been determined that the original images histogram graph in Figure 5. (a) and the histogram graphs of the solved image in Figure 5. (c) are the same. Examining the histogram graphs obtained by the study reveals a balanced distribution of encryption techniques and a suitable histogram distribution for the system.

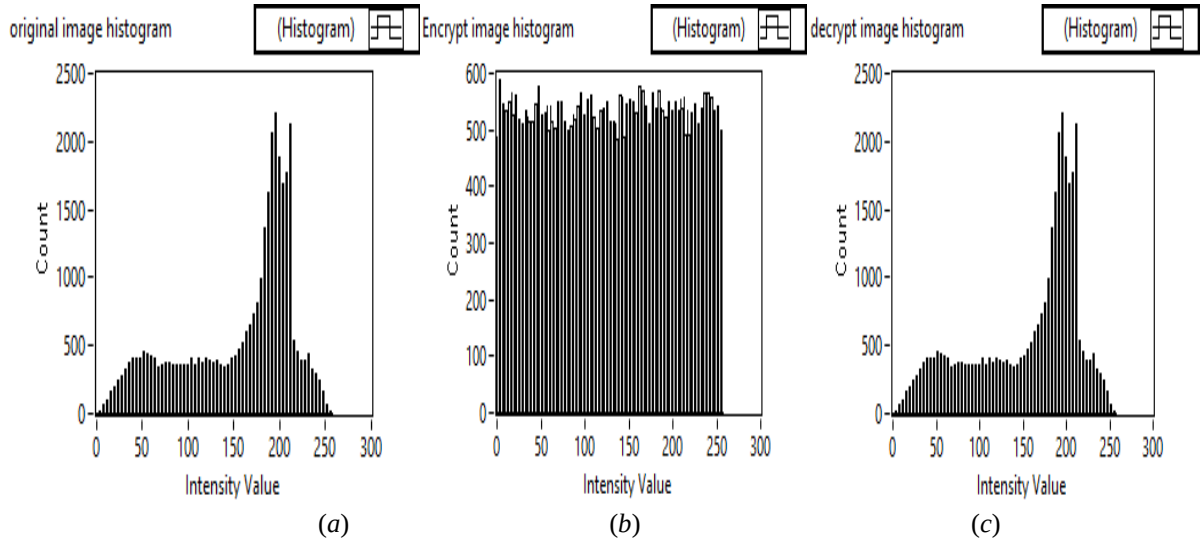


Figure 5. Histogram plot of (a) original image (b) encrypted image and (c) decrypted image

Correlation Analysis

In a plain image, the values of adjacent pixels (horizontal-vertical and diagonal) are very close to each other and the correlation coefficient between them is very high. Therefore, when creating an image encryption algorithm, it is crucial to remove as much correlation as possible between adjacent pixels (Yang et al., 2021). Correlation between adjacent pixels is high in a flat image. In a good encryption, correlation values are expected to decrease to a certain level. The correlation graphs of the original image, the encrypted image and the decoded images for the encryption operations performed are given in Figure 6. Table 3 demonstrates the correlation results of the proposed system.

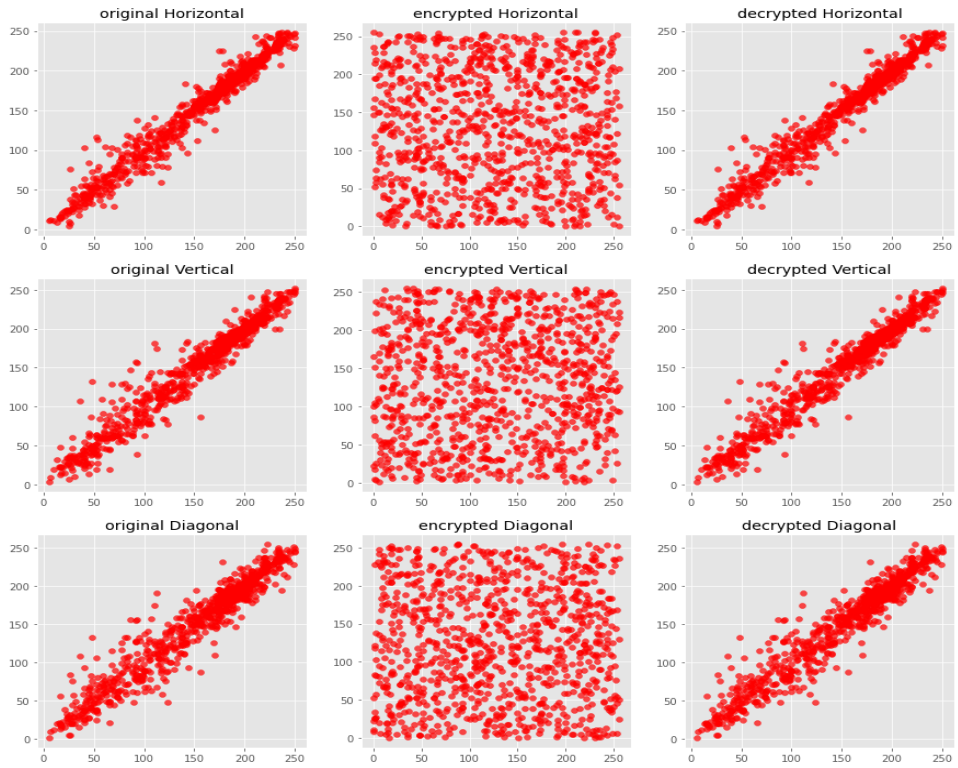


Figure 6. Horizontal, vertical and diagonal correlation scatter plots of the original encrypted and decrypted image

NPCR and UACI test and entropy analysis

Differential cryptanalysis, which was introduced by Biham and Shamir, examines how small modifications to the original image affect the encrypted images (Biham and Shamir, 1991). Table 4 shows the NPCR and UACI test results calculated as a result of the differential attack tests of the developed encryption algorithms.

Table 4. NPCR and UACI values

NPCR	UACI
0.99631	0.31885

The information entropy analysis value of the designed system is very close to the optimum value of eight. The entropy value of the analysed encryption algorithm is observed to be satisfactory. Information entropy analysis results of encryption algorithms are shown in Table 5.

Table 5. The entropy values of the original, encrypted and decrypted image

Original Image	Encrypted Image	Decrypted Image
7.52625	7.99722	7.52625

4. Discussion

The hyperchaotic system used is extremely dependent on the encryption key because of the great sensitivity of chaotic functions. A hyperchaotic memristor-based system is used to perform image encryption in this study. In this regard, it is appropriate for image encryption. The findings demonstrate that the suggested system has adequate security against intrusions and the usage of encrypted photos without authorization. The increasing amount of data being published in widely used digital media makes the need to create new encryption solutions urgently necessary. The established methods will become less credible when hackers and unauthorized users research and examine the old and existing approaches. Therefore, exploiting common surroundings and creating new, attack-resistant approaches might boost confidence.

5. Conclusion

Chaotic systems, due to their randomness and sensitive dependence on initial conditions, provide permutation and diffusion features, which are the basic requirements of cryptological applications. In this study, the memristor-based chaotic system, become increasingly popular in recent years, is favoured. It has been shown in the literature that encryption applications performed only with chaotic systems have some vulnerabilities and are not sufficiently resistant to attacks. LabVIEW is used to implement a chaotic system and a DNA-based encryption application for the purposes of this study. On the implemented encryption applications, histogram analysis, correlation analysis, differential attack (NPCR and UACI tests) and entropy analysis are performed as security analysis. When the security analysis results are evaluated, it has been determined that the proposed encryption algorithm provides a very good correlation distribution, the NPCR value is close to a hundred and the entropy value is close to eight.

Acknowledgment

This work is part of a research project supported by TUBITAK 3501 (Grant number: 122E004).

References

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1), 3-72.

Chen, J., Chen, L., & Zhou, Y. (2020). Cryptanalysis of a DNA-based image encryption scheme. Information Sciences, 520, 130-141.

Chen, J., Zhu, Z. L., Zhang, L. B., Zhang, Y., & Yang, B. Q. (2018). Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing, 142, 340-353.

Çelik, Y. (2016). Nükleobazlar ve nükleositlerde tautomer kararlılığının moleküler modelleme yöntemleriyle belirlenmesi ve mutasyon etkisinin araştırılması (Master's thesis, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü).

Gasimov, V. A., & Mammadov, J. I. (2020). DNA-based image encryption algorithm. In IOP conference series: materials science and engineering (Vol. 734, No. 1, p. 012162). IOP Publishing.

Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dynamics, 83(3), 1123-1136.

Lai, X., Lu, M., Qin, L., Han, J., & Fang, X. (2010). Asymmetric encryption and signature method with DNA technology. Science China Information Sciences, 53(3), 506-514.

Li, H., Wang, Y., & Zuo, Z. (2019). Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. Optics and Lasers in Engineering, 115, 197-207.

Li, Z., Peng, C., Tan, W., & Li, L. (2021). An effective chaos-based image encryption scheme using imitating jigsaw method. Complexity,

Liu, H., & Wang, X. (2012). Image encryption using DNA complementary rule and chaotic maps. Applied Soft Computing, 12(5), 1457-1466.

Luo, H. L., et al. "Coexisting behaviors of chaotic system with tri-stable locally active memristor and its application in color image encryption." *The European Physical Journal Plus* 137.5 (2022): 1-22.

Maazouz, M., Toubal, A., Bengherbia, B., Houhou, O., & Batel, N. (2022). FPGA implementation of a chaos-based image encryption algorithm. Journal of King Saud University-Computer and Information Sciences.

Patidar, V., Pareek, N. K., Purohit, G., & Sud, K. K. (2010). Modified substitution–diffusion image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 15(10), 2755-2765.

Sun, Junwei, et al. "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization." *Nonlinear Dynamics* 94.4 (2018): 2879-2887.

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

Wen, H., Yu, S., & Lü, J. (2019). Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos. Entropy, 21(3), 246.

Yang, Y., Wang, L., Duan, S., & Luo, L. (2021). Dynamical analysis and image encryption application of a novel memristive hyperchaotic system. Optics & Laser Technology, 133, 106553.

Yu, F., Liu, L., Qian, S., Li, L., Huang, Y., Shi, C., ... & Wan, Q. (2020). Chaos-based application of a novel multistable 5D memristive hyperchaotic system with coexisting multiple attractors. Complexity, 2020.

Yu, W., & Cao, J. (2006). Cryptography based on delayed chaotic neural networks. Physics Letters A, 356(4-5), 333-338.

Zhang, Jie, et al. "Hyperchaotic circuit design based on memristor and its application in image encryption." *Microelectronic Engineering* 265 (2022): 111872.

Zhang, Q., & Wei, X. (2013). A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik, 124(23), 6276-6281.

Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11-12), 2028-2035.

Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 181(6), 1171-1186.