Islamic Azad University

Journal of
Optoelectronical Nanostructures

Summer 2023 / Vol. 8, No. 3

Research Paper

A New Image Encryption Algorithm Using a Hyperchaotic Lorenz System to Produce Efficient and Sufficiently Swift Responses to Different Security Needs of Clients

Zahra Kaviyani[1], Mahnaz Mohammadi*[,2], Abbas Kamali[3]

[1, 2] Department of Electrical Engineering Telecommunications, Faculty of Engineering Sciences, Shiraz Branch, Islamic Azad University, Shiraz, Iran

[3] Department of Electrical Engineering, Faculty of Engineering Sciences, Fasa Branch, Islamic Azad University, Fasa, Iran

Received: 10 Jul. 2023
Revised: 16 Aug. 2023
Accepted: 4 Sep. 2023
Published: 15 Sep. 2023

Use your device to scan and read the article online

Keywords:
Hyperchaotic Sequences, Image Decryption, Image Encryption, Symmetric

Abstract

This paper proposes a new plaintext-related mechanism based on plaintext encryption. For simplicity, PCODE was proposed as the image encryption code. The original picture was encoded to get the proposed encryption and plaintext encryption with a chaotic sequence to control the PCODE rules. Another chaotic sequence was encoded into a PCODE sequence for the PCODE XOR operation. The remaining two chaotic sequences were then processed with the proposed scheme to get two key streams for the permutation phase. The cipher image was obtained after the conventional permutation and PCODE XOR operations. The use of the proposed plaintext encryption leads to the correlation between the keystreams used in the displacement phase and both the secret key and the plaintext image. This correlation increases the sensitivity and security of the encryption system with respect to the plaintext. The experimental findings from simulation show that the proposed encryption system shows significant efficiency and security.

Citation: Kaviyani Z, Mohammadi M, Kamali A. A New Image Encryption Algorithm Using a Hyperchaotic Lorenz System to Produce Efficient and Sufficiently Swift Responses to Different Security Needs of Clients **Journal of Optoelectronical Nanostructures.** 2023; 8 (3): 1-18. **DOI: 10.30495/JOPN.2023.30554.1267**

***Corresponding author:** Mahnaz Mohammadi
Address: Department of Electrical engineering telecommunications, Faculty of Engineering Sciences, Shiraz Branch, Islamic Azad University, Shiraz, Iran. **Tell:** 00989177135548 **Email:** mahnazlm53@gmail.com

1. INTRODUCTION

Cryptography reduces maintaining the confidentiality of a message of large and arbitrary length to maintaining the confidentiality of a short key. The foremost criterion that determines the robustness of an encryption algorithm has nothing to do with the possibility of cracking it: if sufficient plaintext-ciphertext pairs are available, any encryption algorithm will eventually crack [1-2- 3].

The greatest strength of an encryption algorithm is the ability to run it in a reasonable time window. The text that takes years to crack, let alone with a network of supercomputers, is actually extremely secure [4]. Early cryptographic systems substantially depended on maintaining the confidentiality of the encryption algorithm to ensure security. Gradually, these algorithms evolved to resolve the problem of key length dependence and confidentiality [5]. Today, the most reliable encryption algorithms have no choice but to successfully pass multiple rounds of scrutinized and non-confidential investigation to gain the trust of enterprises and customers. Naturally, it is intractable to develop reliable encryption algorithms and test them publicly rather than confidentially [5-6-7-8-9]. Choosing weak or poorly protected keys is a sincere invitation to penetrators. If an intruder gains access to an encryption key, even the most robust encryption algorithms will fail to protect the data [8-9-10].

Modern encryption algorithms fall into symmetric and asymmetric groups. Symmetric encryption schemes can be divided into direct, partial, and compression-encryption designs. Each method can encrypt a different volume of data from an image. They also provide different levels of security and efficiency [11-12-17]. In direct encryption, the entire contents of the image are directly encrypted using a new or standard method, while in partial encryption, only some specific parts of an image are encrypted and the rest remains unencrypted. In a compression-encryption scheme, compression is combined with encryption. Since direct encryption encrypts a large portion of the image data, it provides improved security at the expense of slower speed. Instead, the volume of encrypted data decreases in partial and compression-encryption, and the amount of encrypted data decreases, thus enabling higher rates at the cost of lower security [18-19]. This study aims to achieve high security and reasonable image encryption speed efficiency. Therefore, direct symmetric encryption is used to ensure sufficient security.

This paper provides a systemic perspective on image encryption, a subject that has a significant research gap. While AES is the preferred method for symmetric encryption of text documents, it is not well-suited for image encryption due to its low-speed performance and the reflection of correlation and pixel redundancy in the encrypted image [13]. Therefore, image cryptography requires encryption algorithms that preserve the unique properties of the image during encryption. Most studies that do not systematically address image encryption are mainly concerned with confidentiality, an element that can be achieved by a comprehensive image encryption scheme. Multimedia data communications have become very important due to the openness and sharing of networks, especially for digital images related to the military, medicine, and other disciplines dealing with sensitive information. The development of a secure digital image encryption technique has become a critical research focus. Nonetheless, with the inherent properties of digital images - massive data capacity, the strong correlation between adjacent pixels, and high redundancy - common text cryptography systems, such as data encryption standard (DES), advanced encryption standard (AES), and similar systems, are unsuitable for image encryption [1]. Many plaintext or non-plaintext algorithms for image encryption based on chaotic systems are insecure and inefficient against chosen-plaintext attacks (CPAs).

2. The Theory of the Proposed Algorithm

The proposed design implements encryption using a four-dimensional hyperchaotic Lorenz system [10]. Eq. (1) describes the theory:

$$
\begin{aligned}
x &= a(y-x)+w\\
y &= cx-y-xz\\
z &= xy-bz\\
w &= -yz+rw
\end{aligned}
\tag{1}
$$

where a = 10, b = 8/3, c = 28, etc. $-1.52 \leq r \leq -0.06$ are the parameters of the hyperchaotic Lorenz system. Using the Lyapunov exponents spectrum on the differential system proposed in [9], if the parameter is set to r = -1, four Lyapunov exponents are obtained: $\lambda1=0.3381$, $\lambda2=0.1586$, $\lambda3=0$, and $\lambda4=-15.1752$. Furthermore, Fig. 1 shows the hyperchaotic attractors.

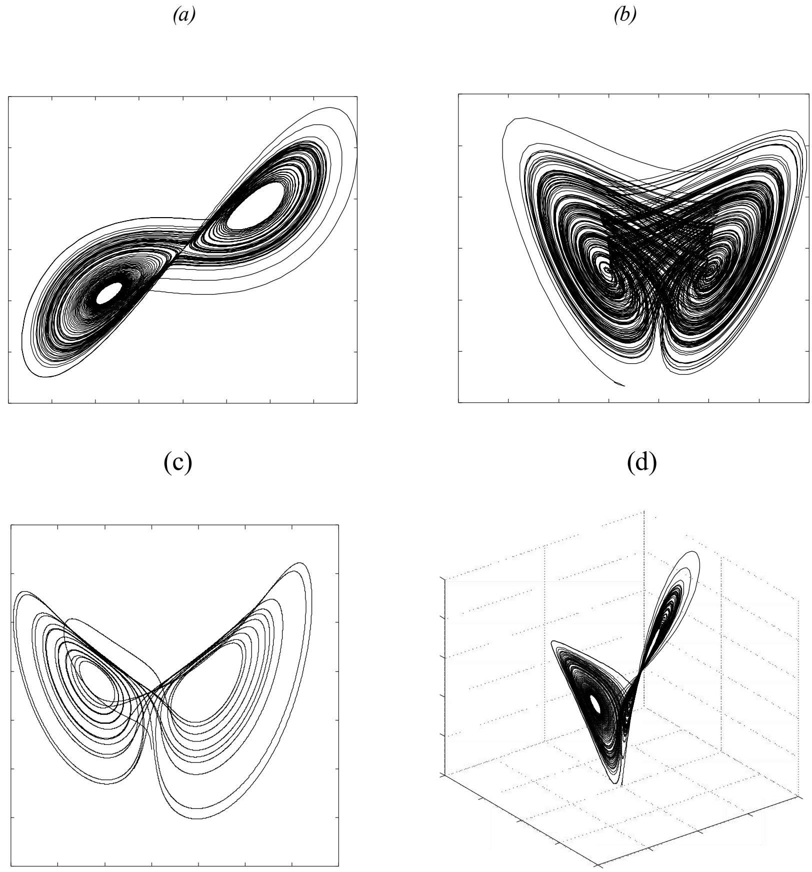


Fig. 1. The hyperchaotic Lorenz system, (a) a = 10 ،b = 8/3 ،c = 28 ،(b) a = 1 ،b = 8/3 ،c = 28 ،(c) a = 10 ،b = 1/3 ،c = 28 ،(d) a = 10 ،b = 8/3 ،c = 2

As you can see in Fig. 1, compared to low-scale systems, a hyperchaotic system has complicated attractors.

Where a = 10, b = 8/3, c = 28, etc. $-1.52 \leq r \leq -0.06$ are the parameters of the hyperchaotic Lorenz system. Using the Lyapunov exponents spectrum on the differential system proposed in [9], if the parameter is set to r = -1, four Lyapunov exponents are obtained: $\lambda 1=0.3381$, $\lambda 2=0.1586$, $\lambda 3=0$, and $\lambda 4=-15.1752$. Furthermore, Fig. 1 shows the hyperchaotic attractors.

3. THE PERFORMANCE OF THE PROPOSED CODE

In the context of the binary system, it can be seen that the binary data represented by the digits 00 and 01 are correspond to the corresponding 11's and 10's complements. Hence, by assigning the four operands, X, Y, Z, and W to represent the binary numbers 00, 01, 10, 11, respectively a total of 24 distinct encoding rules can be formulated. However, only eight encoding rules correspond to the complementary base pairing principle. The rules are listed in Table 1.

TABLE I
THE ENCODING RULES OF THE PROPOSED CODING SEQUENCE

	X	Y	Z	W
Rul 1	00	11	10	01
Rul 2	00	11	01	10
Rul 3	11	00	10	01
Rul 4	11	00	01	10
Rul 5	10	01	00	11
Rul 6	01	10	00	11
Rul 7	10	01	11	00
Rul 8	01	10	11	00

The image encoding process involves the initial conversion of pixel values into binary numbers, which are subsequently encoded into the designated PCODE encoding sequence. In contrast, the PCODE sequence can be decoded using the same coding rule to extract the corresponding pixel value. For instance, A pixel with a value of 188, which corresponds to the binary representation of "10111100", can be encoded as a PCODE sequence of "YWWZ" according to Rule 3, and as "WXXY" according to Rule 7. Various binary sequences can be derived from the same PCODE sequence using distinct PCODE. the PCODE sequence "WXYZ" can be decoded as "10001101" and "11100100" by applying rules 1 and 5. Table 2 shows the performance of XOR operation on PCODE, which is used in the dissemination stage.

TABLE II
THE XOR PERFORMANCE OF PCODE SEQUENCES

XOR	X	Y	Z	W
X	X	Y	B	W
Y	Y	X	W	W
Z	Z	W	X	Y
W	DW	Z	Y	X

4. A GENERAL DESCRIPTION OF THE PROPOSED ALGORITHM

Fig. 2 illustrate the flow diagram of the suggested algorithm.

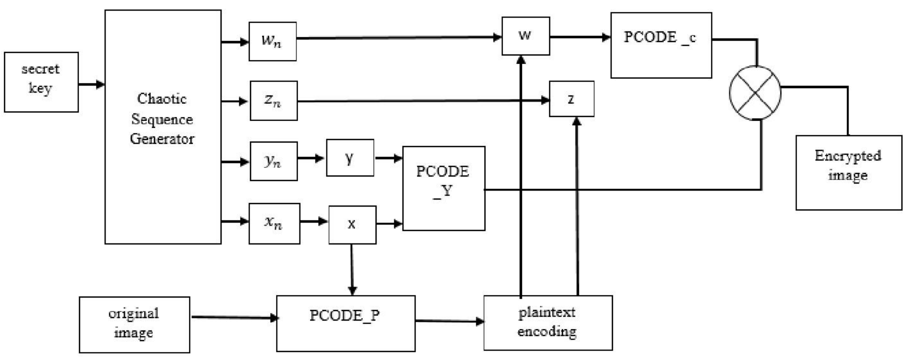


Fig. 2. The flow diagram of the suggested algorithm

Without undermining the totality, it is assumed that we have an original image named I with M × N dimensions. First, I is changed into the one-dimensional array P with M × N dimensions. In the proposed design, four secret keys, including fx0, y0, z0, w0g, have been selected as the primary values of the four-dimensional hyperchaotic Lorenz system. They are resolved using the fourth-order Runge-Kutta algorithm as much as the h=0.002 stage. In order to generate four random sequences xn, yn, zn, and wn, all of which have the same size r = M * N, equation (2) is used, which leads to the elimination of the previous N0 iteration values.

$$x_n = \{x_1, x_2, x_3, \dots, x_r\}$$
$$y_n = \{y_1, y_2, y_3, \dots, y_r\}$$
$$z_n = \{z_1, z_2, z_3, \dots, z_r\}$$
$$w_n = \{w_1, w_2, w_3, \dots, w_r\} \tag{2}$$
$$x_n = \{x_1, x_2, x_3, \dots, x_r\} y_n = \{y_1, y_2, y_3, \dots, y_r\} z_n = \{z_1, z_2, z_3, \dots, z_r\} w_n = \{w_1, w_2, w_3, \dots, w_r\}$$

Then, Eq. (3) is run on x_n and y_n sequences to obtain X and Y sequences.

$$X = f\,loor\left(mod(xn(i) \times 10^{15}, 8)\right) + 1$$
$$Y = f\,lppr(mod(yn(j) \times 10^{15}, 256)) \tag{3}$$

Where

I, j=1, 2, …, r

In the next stage, Array P and Sequence Y are converted into Pb and Yb binary arrays. Then, using Sequence X as an encryption rule, the binary Pb and Yb are encoded to obtain PCODE_P and PCODE_Y. Note that any PCODE_Pi or PCODE_Yi consists of the four elements represented by "X" ،"Y" ،"Z" and "W".

This paper introduces a new plaintext-related mechanism based on PCODE plaintext encryption (PPPC). First, the numbers X, Y, Z, and W in PCODE_P are calculated. They are respectively named numX ،numY ،numZ and numW. Then, their values are used in Eqs. [2] to calculate the plaintext encryption. Unquestionably, invaders cannot be aware of the value of X elements; thus, it is impossible to obtain the amount of the plaintext encoding and select or create special images to break the proposed algorithm.

$$num1 = mod(numX \times 1015/(M \times N \times 4), 32768) \tag{4}$$
$$num2 = mod(numY \times 1015/(M \times N \times 4), 32768) \tag{5}$$
$$num3 = mod(numZ \times 1015/(M \times N \times 4), 32768) \tag{6}$$
$$num4 = mod(numW \times 1015/(M \times N \times 4), 32768) \tag{7}$$
$$PPPC = num1 \times num2 \times num3 \times num4 \tag{8}$$

Finally, the PPPC, which is used to process the zn and wn chaotic sequences, is employed with the following equation to produce two Z and W sequences in the permutation stage of the PCODE level. Algorithm 4-1 involves the precise permutation process.

$$\begin{cases} Z = floor\Big(mod\big((z_n(k) \times PPPC), M\big)\Big) + 1 \\ W = floor\Big(mod\big((w_n(l) \times PPPC), 4 \times N\big)\Big) + 1 \end{cases} \tag{9}$$

Fig. 3 shows the stream flowchart of the encryption-decryption system to encrypt a 3×3 image. In this flowchart, the original image and a secret key are used along with the scrambled sequence, which provides an encrypted image after two stages of coding. More details of this method are provided below.

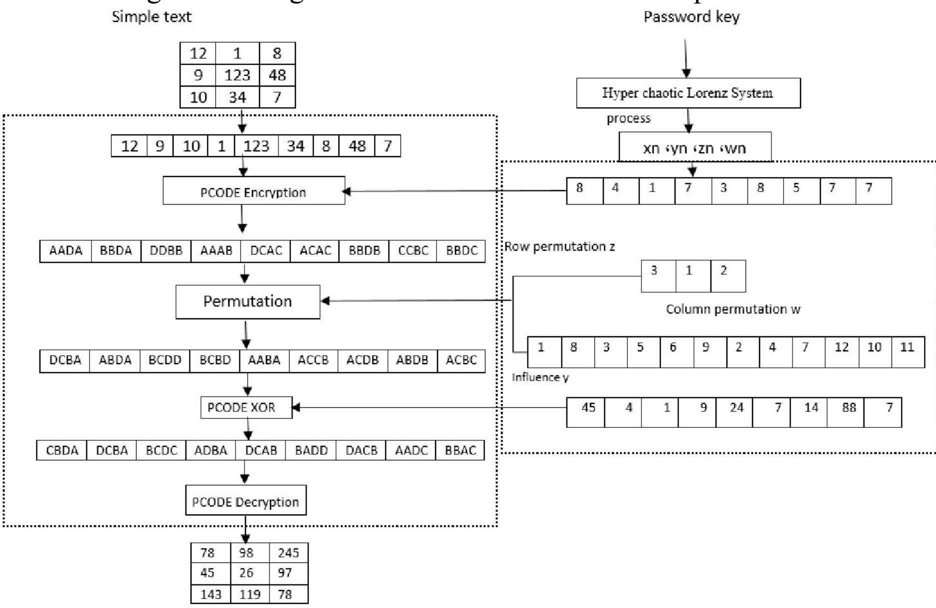


Fig. 3. displays an example of an encryption scheme.

Figure 3 shows the flow diagram of the proposed algorithm for encoding a 3x3 image. In this figure, the process of transforming the image into a one-dimensional array P, generating random sequences, converting the sequences xn and yn into sequences X and Y, converting the arrays P and Y into binary arrays Pb and Yb, encoding the binary arrays using the sequence X and Simple text computation is shown to generate the Z and W sequences. The innovative method proposed in the proposed algorithm is to use plain text to maintain security and prevent various attacks. Also, using random sequences and combining random data in the proposed algorithm has an advantage for security and increasing the randomness of information.

5. IMPLEMENTATION OF THE PROPOSED METHOD

In the proposed method, confidential information is encrypted using the proposed algorithm. The encrypted information is then encoded into the host images. The data volume that can be stored in a host depends on the nature of the host and to what extent the data can be concealed without seriously compromising transparency .

Here, encryption is performed first on text information and then on digital images. To that end, standard, common images were used. After encryption, the encrypted data into different images is then encrypted to compare the quality of the encrypted images. The performance and efficiency of the design were also compared to previous works. The proposed method was implemented in MATLAB. The proposed method's output image was better than the image outputs of other algorithms. Many functions were expressed through this implementation. In this section, image simulation was carried out in standard conditions key_x0 = 1.1, etc. key_y0 = 2.2, etc. key_z0 = 3.3, etc. key_w0 = 4.4, and N0 = 2000. Figs. (4) and (7) show the original and encrypted images, respectively. The simulation results indicate that the plaintext image information cannot be identified from the cipher image. Fig. 5 displays the decrypted image, which fully retrieves the plaintext image information. Fig. 7 shows the image decrypted with the wrong key _x0 = 1.10000000000001, key_y0 = 2.2, key_z0 = 3.3, key_w0 = 4.4, and N0 = 2000. As shown, the wrong key fails to retrieve the original key.

(a) (b) (c)

Fig. 4. The image of the host used in encryption, (a) nature image, (b) airplane (c)

Lena

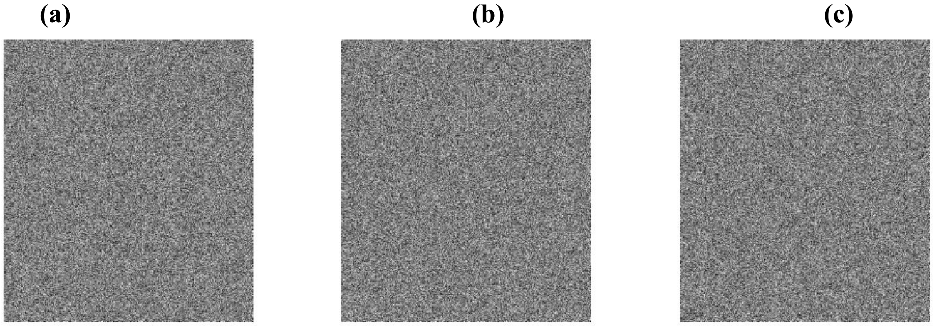


Fig. 5. The encrypted images, (a) Encrypted nature image, (b) Encrypted airplane (c) Lena encrypted

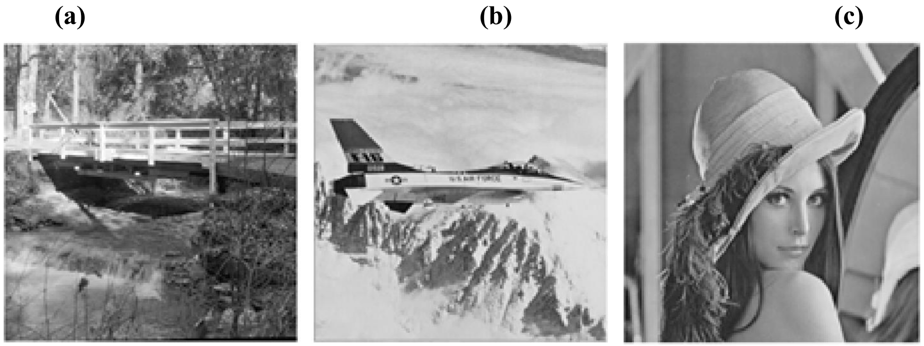


Fig. 6. The decrypted images, (a) decrypted nature image, (b) decrypted airplane (c) Lena decrypted

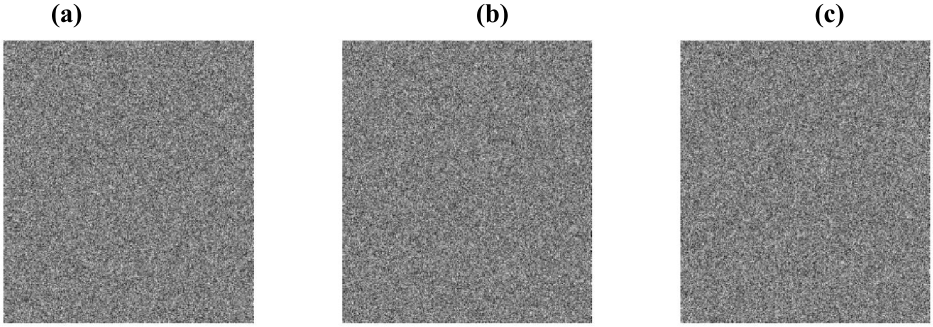


Fig. 7. The images were decrypted with the wrong key, (a) Wrong key decrypted nature image, (b) Wrong key decrypted airplane (c) Wrong key decrypted Lena

There is generally a strong correlation between adjacent pixels in the plaintext image. This correlation should be reduced to near zero after encryption with a secure encryption system (note that the theoretical value is zero). In the experiment, the correlation coefficients of all adjacent pixels in four directions of the unencrypted and encrypted images (See Table 3). Table 4 compares the proposed algorithm's results with other algorithms in detail.

TABLE III
CORRELATION COEFFICIENTS OF RELATED UNENCRYPTED AND ENCRYPTED IMAGES

direction	Simple image	Proposed algorithm	[3]	[4]	[5]	[6]	[7]	[8]
Horizontal	0.959	0.0018	0.0032	0.0011	-0.0045	0.0024	0.0029	0.0035
Vertical	0.968	0.0007	-0.0003	-0.0021	-0.0001	0.0009	0.0033	0.0023
diagonal	0.986	0.0039	-0.00034	0.0016	0.0053	-0.0033	0.0062	-0.0012

TABLE IV
THE CORRELATION COEFFICIENTS OF THE IMAGE OF LENNA, ENCRYPTED WITH DIFFERENT ENCRYPTION SCHEMES

		Horizontal	Vertical	diagonal	Anti-diameter
Lenna	original image	0.96	0.9345	0.98	0.987
	encrypted images	0.024	-0.002	-0.002	0.0011
Jet	original image	0.98	0.9567	0.945	0.93
	encrypted images	00.18	0.00129	0.0033	0.0013
prospect	original image	0.987	0.985	0.987	0.9509
	encrypted images	0.0001	-0.0018	0.0013	0.0014

(a) **(b)**

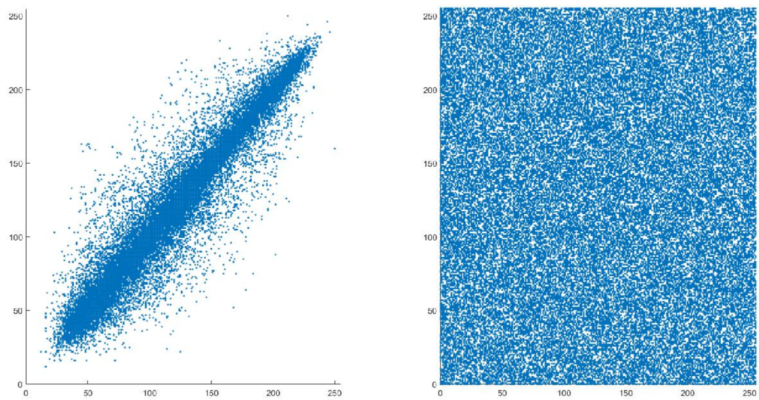
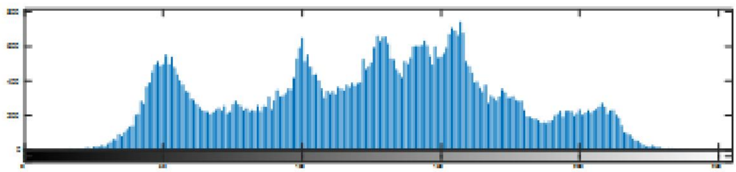


FIG. 8. The images decrypted with the wrong key, (a) Original image correlation (b) Encrypted image correlation

(a)



(b)

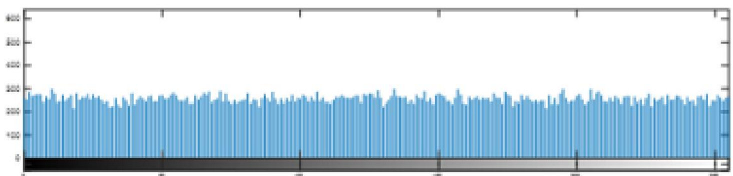


Fig. 8. The histogram diagram of the original and encrypted images of Lenna at a higher resolution, (a) Original image correlation (b) Encrypted image correlation

Table 5 presents the results of the histogram variance of the image encrypted by various encoding algorithms. Compared to similar algorithms, our proposed design's histogram of the encrypted image is flatter.

TABLE V
THE HISTOGRAM VARIANCE OF THE GRAY IMAGE ENCRYPTED BY VARIOUS

	Proposed algorithm	[3]	[4]	[5]	[6]	[7]	[8]
Lenna	957.2	1104.711	1043.214	977.02	973.2578	1027.593	5118.094

6. ENCRYPTION TIME ANALYSIS

In practical applications, the speed at which the system runs the encryption is also a critical indicator in addition to the security function. This section evaluates the running time in seconds. Table 6 illustrate the implementation time of the image encryption system proposed. As shown, the proposed design performs better at encryption speed. Moreover, time complexity (represented by Q) is demonstrated and analyzed. In our proposed design, time consumption mainly involves stages of generating key streams, encoding/decoding of PCODE, permutation, and dissemination. For a gray-scale image with a dimension of $M \times N$, the time complexity of encryption and decryption is $Q(8 \times M \times N)$. At the stage of permutations and dissemination, the modified object is the PCODE sequence with a complexity of $Q(4\times M\times N)$. Moreover, the hyperchaotic Lorenz system is solved to obtain chaotic sequences in which time complexity is $Q(M \times N)$. Therefore, the proposed design's time complexity is $Q(8\times M\times N)$. The proposed method's encryption and decryption have higher time complexity through time complexity analysis.

TABLE VI
THE PROPOSED ALGORITHM'S ENCRYPTION SPEED AND OTHER ENCRYPTION SCHEMES (TIME)

Image	Proposed algorithm	[3]	[4]	[5]	[6]
512×512	0.743	2.6379	3.6208	1.3857	1.2843
256×256	0.181	0.2985	0.9317	0.4397	0.2985

7. CONCLUSION

This paper proposes a new mechanism involves encoding the original image to obtain PCODE encryption and PPPC encoding. The PPPC encoding is then utilized to process chaotic sequences, which generates key streams to be used in the permutation phase. This approach for generating key streams is different from the methods used in previous PCODE-based chaotic image encryption algorithms. The main strength of any encryption algorithm is the possibility of executing it at an acceptable time. A text that can be broken after years with a network of supercomputers is actually very secure [14-15-16-20]. Early encryption systems were very dependent on the confidentiality of the encryption algorithm to maintain security; gradually, encryption algorithms based on key length and confidentiality have prevailed [21]. Today, the most reliable cryptographic algorithms have to pass several rounds of rigorous and non-confidential research in order to win the trust of organizations and customers [17-18]. Naturally, it is very difficult to create reliable encryption algorithms and test them publicly and non-confidentially [22-23-24-25].

Choosing a weak key or protecting it improperly opens the way for intruders to enter, if an intruder gets access to an encryption key, even the strongest encryption algorithms are not able to protect the desired data [14]. In this article, the most important thing is the system view of the image encryption category, which has been neglected until now. In image encryption, algorithms are needed to consider the special features of the image during encryption. In this article, the main concern is the aspect of confidentiality in security, which is provided by a comprehensive system design. This article presents a fuzzy adaptive model based on user needs for image encryption using AES, chaotic function and genetic operators.

References

[1] Ning, H., Liu, H., Ma, J., Yang, L. T., & Huang, R.. *Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology. Future generation computer systems*, 56, (2016) 504-522.

Available:https://www.sciencedirect.com/science/article/abs/pii/S0167739X15002356

[2] Amor, A. B., Abid, M., & Medb, A. *Secure blockchain-based e-learning scheme*. IEEE Access, 8, (2020) 31920-31933.

Available:https://ieeexplore.ieee.org/ielaam/6287639/8600701/8917991-aam.pdf

[3] Ding, S., Li, C., & Li, H. *A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT*. IEEE Access, 6, (2018) 27336-27345.

Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8359407

[4] Zhang, Y., Li, J., & Yan, H. *Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure*. IEEE Access, 7, (2019) 47982-47990.

Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8681522

[5] Ning, J., Cao, Z., Dong, X., & Wei, L. *White-box traceable CP-ABE for cloud storage service: how to catch people leaking their access credentials effectively*. IEEE Transactions on Dependable and Secure Computing, 15(5), (2016) 883-897.

Available:https://www.scinapse.io/papers/2520342609

[6] Chuman, T., Sirichotedumrong, W., & Kiya, H. *Encryption-then-compression systems using grayscale-based image encryption for jpeg images*. IEEE Transactions on Information Forensics and security, 14(6), (2018)1515-1525. Available: https://ieeexplore.ieee.org/document/8537968

[7] Yang, Y. G., Zou, L., Zhou, Y. H., & Shi, W. M. *Visually meaningful encryption for color images by using Qi hyper-chaotic system and singular value decomposition in YCbCr color space*. Optik, 213, (2020) 16442 Available:https://www.sciencedirect.com/science/article/abs/pii/S0030402620302564

[8] Ghadirli, H. M., Nodehi, A., & Enayatifar, R. *An overview of encryption algorithms in color images*. Signal Processing, 164, (2019)163-185.

Available:https://www.sciencedirect.com/science/article/abs/pii/S016516841930218X

[9] Farah, M. B., Farah, A., & Farah, T. *An image encryption scheme based on a new hybrid chaotic map and optimized substitution box*. Nonlinear Dynamics, (2019) 1-24.

Available:https://www.hindawi.com/journals/complexity/2020/9597619/

[10] Khan, P. W., & Byun, Y. *A blockchain-based secure image encryption scheme for the industrial Internet of Things.* Entropy, 22(2), (2020) 175.

Available: https://www.mdpi.com/1099-4300/22/2/175

[11] Mondal, B., Kumar, P., & Singh, S. *A chaotic permutation and diffusion based image encryption algorithm for secure communications*. Multimedia Tools and Applications, 77(23), (2018) 31177-31198.

Available: https://link.springer.com/article/10.1007/s11042-018-6214-z

[12] Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. *Analytical study of hybrid techniques for image encryption and decryption*. Sensors, 20(18), (2020) 5162.

Available: https://www.mdpi.com/1424-8220/20/18/5162

[13] Wang, J., Zhi, X., Chai, X., & Lu, Y. *Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion*. Multimedia Tools and Applications, 1-36. (2021)

Available: https://link.springer.com/article/10.1007/s11042-020-10413-7

[14] Bashier, E., & Jabeur, T. B. *An Efficient Secure Image Encryption Algorithm Based on Total Shuffling, Integer Chaotic Maps and Median Filter* (No. 5028). (2021) EasyChair.

Available: https://jisis.org/article/jisis-2021-vol11-no2-04/69464/

[15] Zhang, L., Liang, P., & Mu, Y. *Improving privacy-preserving and security for decentralized key-policy attributed-based encryption*. IEEE Access, 6, (2018) 12736-12745.

Available :https://ro.uow.edu.au/cgi/viewcontent.cgi?article=228

[16] Alshehri, M., & Panda, B. *Minimizing Data Breach by a Malicious Blockchain Node within a Blockchain Federation*. 7th IEEE International Conference on Cyber Security and Cloud Computing (2020, August) (pp. 36-43). Available :https://www.researchgate.net/publication/343756473

[17] Ismail, S. M., Said, L. A., Radwan, A. G., Madian, A. H., & Abu-ElYazeed, M. F. *A novel image encryption system merging fractional-order edge detection and generalized chaotic maps.* Signal Processing, 167, (2020) 107280.

Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9387309

[18] Ahmad, M., Al Solami, E., Wang, X. Y., Doja, M. N., Beg, M. M., & Alzaidi, A. *Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos*. Symmetry, 10(7), (2018) 266.

Available:https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9465166R

[19] Yahyazadeh , Z.Hashempour , *Effect of Hydrostatic Pressure on Optical Absorption Coefficient of InGaN/GaN of Multiple Quantum Well Solar Cells* , (Spring 2021). Vol. 6, No. 2.

Available: https://jopn.marvdasht.iau.ir/article_4768.html

[20] M. Mohammadi , A.Zolghadr , M. Pourmina , *Comparison of two Public Key Cryptosystems*, Summer 2018 / Vol. 3, No. 3.

Available: https://jopn.marvdasht.iau.ir/article_3045.html

[21] M.Momeni , M Javadian Sarraf , F.Khatib ,*Design of high sensitivity and high FoM refractive index biosensor based on 2D-photonic crystal,* Winter 2021 / Vol. 6, No. 1.

Available: https://jopn.marvdasht.iau.ir/article_5040.html

[22] M.Rajaee, S. Rabiee , *Analysis and Implementation of a New Method to Increase the Efficiency of Photovoltaic Cells by Applying a Dual Axis Sun Tracking System and Fresnel Lens Array,* Summer 2021 / Vol. 6, No. 3.

Avalable: https://jopn.marvdasht.iau.ir/article_4981.html

[23] Sh.Shahi, P. Momayezan , M. Ranjbaran, S. Wadi Harun, *Observation of Raman Gain in Reduced Length of Bismuth Erbium Doped Fiber*, Summer 2020 / Vol. 5, No. 3.

Avalable: https://jopn.marvdasht.iau.ir/article_4405.html

[24] Wang, Q., Peng, L., Xiong, H., Sun, J., & Qin, Z. *Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing*. IEEE Access, 6, (2017) 760-771.

Available: https://ieeexplore.ieee.org/document/8119793

[25] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. *Blockchain computing for the internet of things: Security and privacy issues*. IEEE Internet Computing, 21(2), (2017) 34-42.

Available:https://www.sciencedirect.com/science/article/pii/S187705091830872X