Received: 04 June 2022 | *Revised:* 22 June 2022 | *Accepted:* 24 June 2022
DOI: 10.37917/ijeee.18.2.9 *Early View* | *December 2022*

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Original Article

An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences

Ghofran Khaled Shraida, Hameed Abdulkareem Younis
Department of Computer Science, College of CSIT, University of Basrah, Basrah, Iraq

Correspondence
*Ghofran Khaled Shraida
Department of Computer Science, College of CSIT,
University of Basrah, Basrah, Iraq
Email: itpg.ghofran.khaled@uobasrah.edu.iq

Abstract
Experts and researchers in the field of information security have placed a high value on the security of image data in the last few years. They have presented several image encryption techniques that are more secure. To increase the security level of image encryption algorithms, this article offers an efficient diffusion approach for image encryption methods based on one-dimensional Logistic, three-dimensional Lorenz, DNA encoding and computing, and SHA-256. The encryption test demonstrates that the method has great security and reliability. This article, also, examines the security of encryption methods, such as secret key space analysis, key sensitivity test, histogram analysis, information entropy process, correlation examination, and differential attack. When the image encryption method described in this article is compared to several previous image encryption techniques, the encryption algorithm has higher information entropy and a lower correlation coefficient.

KEYWORDS: Chaos theory, Deoxyribonucleic Acid (DNA), hash function, image encryption, logistic map, Lorenz attractor.

I. INTRODUCTION

Since the Internet's introduction into our lives, information security has become critical. With practically everything are available to anybody on the world with a few mouse clicks, protecting personal information on the Internet is important. One method of safeguarding information is to convert the image into an unintelligible form that seems to be a random noisy image. Image encryption is the name given to this method. For a long time, image encryption has piqued the curiosity of scholars all over the world. Image encryption employs certain conventional encryption methods, such as, DES, AES, and RSA [1], [2]. However, when used to a system that encrypts a huge number of images or video, the conventional encryption technique is less efficient. As a result, the necessity to create unique image encryption techniques arises. In the realm of information encryption, the chaotic system possesses better features. Chaos possesses a number of complicated qualities that aid in the development of more safe and durable encryption schemes. It is sensitive to beginning value circumstances, unpredictable, and has a high bifurcation complexity [3], [4]. Chaotic patterns contain Hénon map, Lorenz map, logistic map, Arnold Cat map, and others [5]. This complexity of chaotic mapping may be seen in the features of some encryption processes that are comparable to ideal ciphers, such as, avalanche, balancing, aliasing, and diffusion [6]. Some encryption methods based on chaos theory are devised and used to image encryption in order to assure the security of image information during transmission and storage.
Furthermore, several of the outstanding characteristics of deoxyribonucleic acid (DNA) computing have lately been discovered, for example: tiny energy loss, huge storage space, and large-scale computational parallelism. As a result, the employment of complementary DNA principles to encrypt information technology has made significant progress. Therefore, the algorithms based on DNA and chaotic system use the advantages of both fields to provide image protection in an effective way. [7]–[10] These research papers proposed merging DNA coding and chaos theory in image encryption schemes. In [11] a unique color image encryption technique using one-time pad was proposed. To improve the robustness of the suggested algorithm, the secret keys and the Hamming distances between the DNA matrices are used to construct the key streams from the 3D Skew Tent Map (3D-STM). In [12] a new encryption and decryption technique for validating image transfer across information correspondence frameworks was presented. Both are indistinguishable using hybrid chaotic confusion processes and the mitochondrial DNA (mtDNA) diffusion technique, which reduce equipment use complexity and enhance framework security. In [13] a novel DNA-based RGB image encryption algorithm using the hash function SHA-256 and the Nonlinear Chaotic Algorithm (NCA) map-based Coupled Map Lattice (CML)

was presented. In [14] a color image encryption technique depending on a double-chaos system and DNA computing at the bit level was proposed. The Arnold algorithm was used to scramble the original image's three-color components for this technique. In [15] a new encryption approach based on dynamic DNA and 4-D memristive hype-chaos was suggested.

However, these DNA encoding image encryption algorithms still exist problems including: DNA encoding rules are limited, and the limited DNA computation rules, key sensitivity is low, etc. In view of these problems in the proposed encryption algorithm, the algorithm proposed described in our paper will integrate DNA coding principles with DNA computing, as well as, the outstanding properties of a chaotic map. The plain image's SHA-256 hash is employed to produce secret keys; if the plain image changes slightly, this will make a significant difference to the sensitivity of the cryptosystem, increasing the security.

The algorithm makes use of a 256-bit secret key S produced by applying the SHA-256 algorithm on the original image. We construct the starting values of the one-dimensional logistic map and three-dimensional Lorenz system using the secret keys. Because the secret keys are so closely connected to plaintext, the cryptosystem can withstand brute force, chosen-plaintext, and chosen-ciphertext attacks. The sequences generated by 1D logistic map and 3D Lorenz system are combined to obtain a key image the size of the original image. Then, the key image and the original image are converted to DNA coding and the process of XOR between the original image and the key image is performed. Thus, the final encrypted image is generated.

The remainder of the paper is arranged as follows: The essential principle of the suggested method is explained in Section **II**. Section **III** discusses the suggested image encryption technique. Section **IV** proposes experimental results, as well as, a security analysis. Comparing the results with other image encryption algorithms is discussed in Section **V**. Finally, in Section **VI**, the conclusions are reached.

II. Basic Theory

A. Hash-256

Integrity security is mostly provided by utilizing hash functions. Hash-256 is a popular cryptographic hash function that provides a 256-bit hash result that is commonly represented as a 64-digit hexadecimal number. Because of its high level of security, even a single bit modification can cause a considerable variation between two images [16]. S is a 256-bit secret key separated into 8-bit chunks, yielding 32 chunks. Following that, every four chunks are joined together, yielding 8 groups (K_i), therefore, k may be written as follows:

$$K_i = \sum_{n=0}^{3} \frac{b_{4i-n}}{2^6}, \quad (1 \le i \le 8), (1 \le b \le 32) \qquad (1)$$

The initial values can be derived as follows:

$$\begin{cases} p_1 = \frac{k_1}{k_1 \times k_2} \\ x_1 = \frac{k_3}{k_3 \times k_4} \\ y_1 = \frac{k_5}{k_5 \times k_6} \\ z_1 = \frac{k_7}{k_7 \times k_8} \end{cases} \qquad (2)$$

B. 1D Logistic Map

We employ a 1D logistic map [17] in this suggested approach to combined it with 3D Lorenz system. 1D logistic map can be defined as follows:

$$\hat{p} = rp(1-p), x \in [0,1] \qquad (3)$$

where $p \in [0,1]$, $r \in (0,4]$.

C. 3D Lorenz System

As a continuous three-dimensional chaotic system, Lorenz system is defined as follows [18]:

$$\begin{cases} \hat{x} = a(y-x) \\ \hat{y} = cx - y - xz \\ \hat{z} = xy - bz \end{cases} \qquad (4)$$

The system's control parameters are a, b, and c. The system in (4) achieves a hyper-chaotic mode when a = 10, b= 8/3, c = 28. It is essential to disperse the system by the fourth-order Runge-Kutta method for encrypting image.

D. DNA Encoding and Computing

A (adenine), G (guanine), C (cytosine), and T (thymine) are the four deoxy nucleotides that make up DNA. G and C are complementary, as are A and T. In a binary system, 0 and 1 are complementary to each other. As a result, the four bases might be encoded as 00, 11, 01, and 10. According to complementary, there are 24 different types of DNA encoding methods, but only eight encoding choices are efficient due to the complimentary connection between the four, as shown in Table 1.

TABLE 1
DNA Encoding Rules

Rules	0	1	2	3	4	5	6	7
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

The gray value of a pixel in an image cryptosystem may be represented as its matching binary sequence, which can subsequently be translated into a DNA strand. On the other hand, a pixel value may be generated from a DNA strand. For example: using DNA encoding Rule 4, the pixel value 196 and its binary sequence 11000100 might be encoded into the DNA sequence GCAC. As a result of decoding the DNA sequence with Rule 6, on 55 is obtained. As with binary numbers, the DNA sequences can be XORed in the same way, and the results are influenced by the rule that used to perform these operation. The details of the XOR DNA operation rules is shown in the Table 2.

TABLE 2
XOR DNA OPERATION

⊕	A	C	T	G
A	G	T	C	A
C	T	G	A	C
T	C	A	G	T
G	A	C	T	G

III. PROPOSED CRYPTOSYSTEM

Following the separation of the original image into three-color channels and the transformation of decimal pixels into strands of DNA for each channel, both of 1D logistic map and a 3D Lorenz system are constructed, concatenated, and turned into DNA strands. It should be mentioned that the beginning conditions for the generation of chaotic systems are based on the SHA-256 function of the original image. Then, the channels' DNA strands are transformed into three binary bit streams after inter-channel operations are performed during the diffusion phase. These bit streams are transformed back to pixels with decimal values. The encrypted image is created by combining the channels.

The three-color channels of a plain color image, namely red, green, and blue, are separated and saved as independent matrices, R, G, and B, respectively. Following that, these matrices' decimal pixel values are transformed to 8-bit binary representation. The rules that are listed in Table 1 are utilized to convert these arrays into DNA sequences. The suggested image encryption procedure consists of the following steps.

Step 1. Color channel extraction:

Extract the red, green, and blue channels (of size n = M × N) from the plain image as distinct arrays R, G, and B.

Step 2. R, G, and B modifications to DNA sequences:

First, pixels with decimal values in arrays R, G, and B are transformed to 8-bit binary representations. Using the rules in Table 1, transform the binary arrays into DNA strand representations using Rules 5, 6, and 7, respectively.

Step 3. Generation of chaotic sequences:

generate chaotic sequences p using a 1D Logistic map, as seen in (3). By following the technique outlined in (4), the 3D Lorenz chaotic system creates x, y, and z chaotic sequences. Then, combined the two chaotic sequences as follows:

$$\begin{cases} px = p + x \\ py = p + y \\ pz = p + z \end{cases} \quad (6)$$

The sequences px, py, and pz are converted to X, Y, and Z mask images as follows:

$$\begin{cases} X = \mathrm{mod}(\mathrm{round}(px * 10\text{^}4), 256) \\ Y = \mathrm{mod}(\mathrm{round}(py * 10\text{^}4), 256) \\ Z = \mathrm{mod}(\mathrm{round}(pz * 10\text{^}4), 256) \end{cases} \quad (7)$$

X, Y, and Z sequences are formed with the same size as RGB channels.

Step 4. DNA strand formation from chaotic sequences:

Decimal values in X, Y, and Z is converted to 8-bit binary representations, then, translated to DNA strands according to the rules 5, 6, and 7, respectively. Following this, DNA strands are organized into six arrays: R, G, B, X, Y, and Z.

Step 5. XOR operation on DNA sequences:

XOR operation between arrays R, G, and B is performed as follows:

$$\begin{cases} G' = R \oplus G \\ B' = G \oplus B \\ R' = R \oplus G' \end{cases} \quad (8)$$

Now, XOR operation between arrays (R′,G′, and B′) and (X, Y, and Z) is performed as follows:

$$\begin{cases} R'' = R' \oplus X \\ G'' = G' \oplus Y \\ B'' = B' \oplus Z \end{cases} \quad (9)$$

These procedures are carried out utilizing the DNA XOR rules listed in Table 2 above.

Step 6. Conversion of DNA sequences to binary form:

Apply the rules 0, 1, and 2, respectively, to the DNA strands in R″, G″ and B″ to convert them back to binary arrays.

Step 7. Generation of encrypted image:

The binary-valued pixels are converted to their decimal equivalents. Then, the three channels are merged to produce the encrypted image.

Fig. 1 depicts the encryption algorithm flow chart. The decryption algorithm is just the opposite of the encryption method.

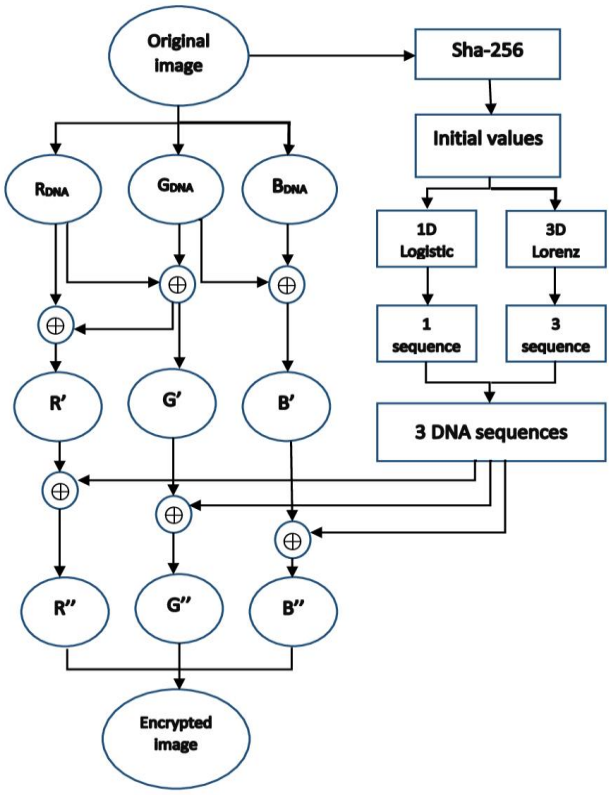
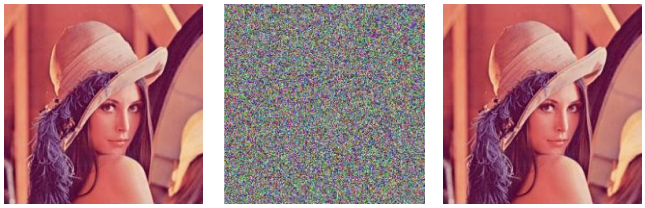


Fig. 1: The Flow Chart of Encryption Algorithm.

IV. Simulation Result and Security Analysis

As the input image in this article, we utilize a normal 256×256×3 color image of "Lena" in png format. We utilize MATLAB R2013a with 8 GB RAM and Intel(R) Core(TM) i5-4310U processor and 32-bit Windows 8 to simulate the encryption and decryption operations. Fig. 2 depicts the encryption and decryption of a Lena 256×256 color image. The plain-image Lena is shown in Fig. 2(a). Fig. 2(b) shows the encrypted image of Lena, whereas Fig. 2(c) shows the decrypted image for recovering the plain image of Lena.



(a) (b) (c)

Fig. 2: (a) the plain-image Lena, (b) the encrypted image of Lena, and (c) the decrypted image of Lena.

A. Key Space

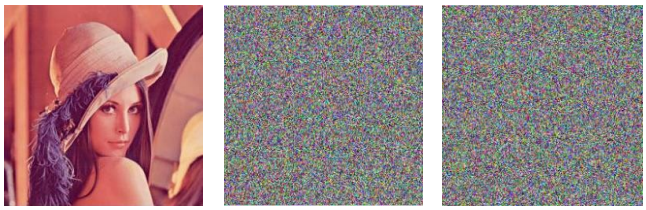
In terms of cryptography, a key space greater than 2^{100} might provide a high level of security [19]. The keys in the proposed cryptosystem are:

1) The starting values of p_1, x_1, y_1, and z_1.
2) The logistic map parameter r.

For the starting values p_1, x_1, y_1, and z_1 and for parameter r, the size of the key space is 10^{70} if the precision is 10^{14}. We can get $10^{70} = (10^3)^{23.3} \approx (2^{10})^{23.3} \approx 2^{230}$, which is sufficient to thwart the all-out attack. As a result, brute force attacks on the key are not feasible.

B. Key Sensitivity

A good cryptosystem should be sensitive to the secret key, which means that even little changes in the secret key will result in a considerable change in the output. To encrypted Lena image, we do the test of the secret key sensitivity using a slightly different key from the original key. One of the keys p_1, y_1 is changed, while, the other keys' parameters remain intact, and the encrypted image is decrypted using the modified keys. As shown in Fig. 3, no useful information is decrypted, implying that the suggested cryptosystem can withstand the exhaustive attack.

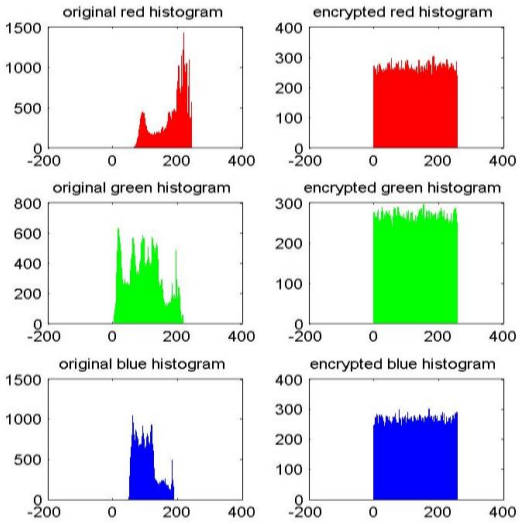


(a) (b) (c)

Fig. 3: Tests of Key Sensitivity: images deciphered with (a) the proper keys, (b) $p_1 + 10^{-14}$, (c) $y_1 + 10^{-15}$.

C. The Histogram Analysis

In image analysis, the image histogram is an important feature. A perfect cipher image should have a uniform frequency distribution. Fig. 4 depicts the original and encrypted image histograms; it is obvious that the encrypted image histograms are random-like and uniform, implying that the suggested approach does not give any relevant statistical information in the encrypted image.



(a) (b)

Fig. 4: Histogram Analysis: (a) red, green, and blue histograms for a plain image of Lena, (b) red, green, and blue histograms for a cipher image of Lena, respectively.

D. Information Entropy

The information entropy determined by (10) is an important characteristic for determining the unpredictability of the encrypted image. Gray values are distributed more equally, and the entropy is closer to its optimal value:

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \log_2\left(\frac{1}{p(m_i)}\right), \sum_{i=0}^{M-1} p(m_i) = 1 \quad (10)$$

where m_i $(i = 0, 1, \cdots, M-1)$ depicts grayscale values, $p(m_i)$, $(i = 0, 1, \cdots, M-1)$ reflects the likelihood of a pixel with value mi occurring. For an encrypted image with 256 gray scale, the entropy should optimally be 8, indicating that the information is unclear. The average information entropy of the encrypted image in the article is 7.9973 bit, which is near to the ideal value of 8 bit. As a result, we conclude that the suggested method has a significant degree of unpredictability. The entropy for encrypted images utilizing different encryption techniques is determined and presented in Table 3, with the suggested algorithm in this study outperforming the others.

TABLE 3
Results of Information Entropy

Algorithm	Red	Green	Blue	Average
Ours	7.9972	7.9977	7.9972	7.9973
Ref.[7]	----------	----------	----------	7.9913
Ref.[8]	7.9971	7.9973	7.9974	7.9972
Ref.[9]	7.9895	7.9894	7.9894	7.9894
Ref.[14]	7.9892	7.9902	7.9896	7.9896

E. Two Adjacent Pixels Correlation

A correlation analysis determines the similarity between the cipher and the original image [20]. To

examine the correlation between the plain image and the encrypted image, we randomly picked 50,000 neighboring pixels from the original and encrypted images and computed the coefficients of correlation as follows:

$$\begin{cases} \bar{x} = \frac{1}{M\times N}\sum_{i=1}^{M\times N} x_i \\ \sigma_x = \frac{1}{N}\sum_{i=1}^{n}(x_i - \bar{x})^2 \\ \mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \\ \mathrm{corr}_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{\sigma_x}\sqrt{\sigma_y}} \end{cases} \quad (11)$$

The x and y values indicate the grayscale values of two neighboring pixels. Fig. 5 depicts the correlation between the R, G, and B components of Lena's original and encrypted images. Table 4 indicates that the correlation coefficients between neighboring pixels in the encrypted image is substantially less than in the plain image. Also, it is smaller when compared the correlation coefficients for cipher images using different encryption algorithm. These findings clearly reveal that the correlation coefficients of the plain image are close to one, while, those of the encrypted image are close to zero, and that the distribution of neighboring pixels is rather uniform. It implies that the suggested approach has successfully reduced the correlation of neighboring pixels in the plain image, resulting in almost minimal correlation between neighboring pixels in the encrypted image. As a result, the suggested method can withstand statistical attacks.

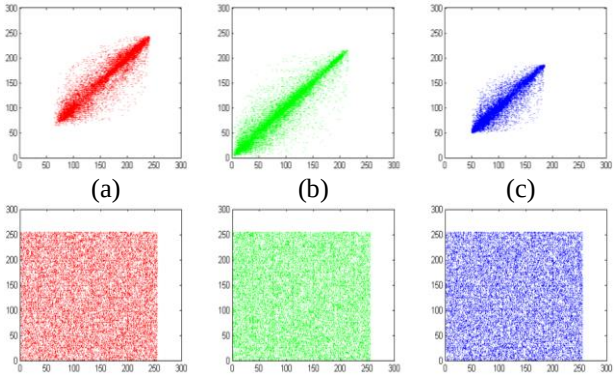


Fig. 5: The distribution of two pixels that are horizontally neighboring in the (a) red, (b) green, and (c) blue components of Lena's plain image. The distribution of two horizontally neighboring pixels in the (d) red, (e) green, and (f) blue components of Lena's encrypted image, respectively.

TABLE 4
CORRELATION COEFFICIENTS ANALYSIS

	H.	V.	D.
Plain image	0.9684	0.9860	0.9556
Our encrypted image	0.0011	-0.0013	-0.0004
Ref. [9]	-0.0080	0.0098	-0.0058
Ref. [13]	-0.0082	-0.0128	-0.0012
Ref. [14]	-0.0119	-0.0089	-0.0045

F. Differential Attack

The unified average changing intensity (UACI) and the number of pixels change rate (NPCR) for the encrypted images are commonly used to measure the number of pixels change rate.

$$NPCR = \frac{\sum_{i,j} D(i.j)}{M\times N} \times 100\% \quad (12)$$

$$UACI = \frac{1}{M\times N}\left[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100 \quad (13)$$

where M and N are the encrypted image's width and height, respectively. $D(i.j)$= 0 when it is the same value in C_1 and C_2, while, it is 1 when it is different. $C_1(i,j)$ and $C_2(i,j)$ represent two encrypted images with only one pixel value change from the corresponding plain images. To test the proposed algorithm's plain image sensitivity, one pixel is altered at random from the plain image. The suggested approach is used to construct two encrypted images by encrypting the plain and modified plain images. Table 5 shows the UACI and NPCR values for the two encrypted images. As a result, we can observe that the UACI and NPCR are near to the predicted values, indicating that the suggested method can withstand the differential attack.

TABLE 5
RESULTS OF UACI AND NPCR

Algorithm	UACI (%)	NPCR (%)
Ours	33.44	99.62
Ref. [10]	33.42	99.59
Ref. [12]	33.42	99.61
Ref. [14]	32.20	99.61
Ref. [15]	30.41	99.61

V. COMPARISON

To show its advantages, Tables 3, 4, and 5 compare the proposed cryptosystem to existing image encryption algorithms on certain performance characteristics. It is large enough to withstand the exhaustive attack for key space analysis. Our cryptosystem's correlation coefficients are closer to zero than the encryption approaches. [9], [13], [14], this demonstrates that the cryptosystem is more resistant to statistical attacks. The information entropy in this paper is greater when comparing it with those in [7]–[9], [14]. Table 5 shows that the suggested cryptosystem's NPCR and UACI values are near to optimal and higher compared with those in [10], [12], [14], [15], referring to an image cryptosystem that can withstand chosen-plaintext and known-plaintext attacks.

VI. CONCLUSIONS

A robust image encryption scheme based on the chaotic system and DNA operation is given in the suggested algorithm. We merged a 1D logistic map with a 3D Lorenz system to generate more sequences that are random. Adding the DNA XOR operation to the DNA operation process improves not only the unpredictability of the encryption, but also, the pixels diffusion effect. We discovered that the suggested approach has a decent encryption effect based on the testing results and security analyses. The results for information entropy and correlation coefficients indicate that the encryption method was able to successfully encrypt a plain image into an encrypted image. The algorithm's capacity to endure differential attacks is additionally supported by UACI and NPCR values. Furthermore, the

decrypted and plain images are identical. The suggested method has a larger secret key space and is extremely sensitive to the secret key. Moreover, the suggested technique can withstand the majority of known attacks, including statistical analysis and exhaustive attacks. All of these characteristics demonstrate that our approach is well suited for digital image encryption.

CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

REFERENCES

[1] R. Chaddha, A. Kumar, K. Sinha, and P. Paul, "Selection on Various Traditional Image Encryption Techniques: A Study," in *International Conference on Nanoelectronics, Circuits and Communication Systems*, 2018, pp. 219–228.

[2] H. Arora and J. Jain, "Comparison among RSA, AES and DES," *Int. Res. Journals Eng. Technol. Vol. 06 issue*, 2019, doi: 10.14704/WEB/V19I1/WEB19047.

[3] A. A. Abdallah and A. K. Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi J. Sci.*, pp. 324–337, 2022.

[4] A. A. Al-Hussein, "Chaos Phenomenon in Power Systems : A Review," *Iraqi J. Elecrical Electron. Eng.*, vol. 17, no. 2, 2021, doi: 10.37917/ijeee.17.2.25.

[5] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, "Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps," *IEEE Access*, vol. 9, pp. 76191–76204, 2021.

[6] S. S. Askar, A. A. Karawia, A. Al-Khedhairi, and F. S. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, no. 1, p. 44, 2019.

[7] P. Liu, T. Zhang, and X. Li, "A new color image encryption algorithm based on DNA and spatial chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 11, pp. 14823–14835, 2019.

[8] H. R. Amani and M. Yaghoobi, "A New Approach in Adaptive Encryption Algorithm for Color Images Based on DNA Sequence Operation and Hyper-Chaotic System," *Multimed. Tools Appl.*, vol. 78, no. 15, pp. 21537–21556, 2019, doi: 10.1007/s11042-018-6989-y.

[9] X. Wu, J. Kurths, and H. Kan, "A robust and lossless DNA encryption scheme for color images," *Multimed. Tools Appl.*, vol. 77, no. 10, pp. 12349–12376, 2018, doi: 10.1007/s11042-017-4885-5.

[10] X. Y. Wang, P. Li, Y. Q. Zhang, L. Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the Lorenz system," *Multimed. Tools Appl.*, vol. 77, no. 5, pp. 6243–6265, 2018, doi: 10.1007/s11042-017-4534-z.

[11] X. Zhang and R. Ye, "A novel RGB image encryption algorithm based on DNA sequences and chaos," *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8809–8833, 2021.

[12] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," *Entropy*, vol. 22, no. 2, p. 158, 2020.

[13] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018, doi: 10.1016/j.sigpro.2018.02.028.

[14] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," *IEEE Access*, vol. 8, pp. 83596–83610, 2020, doi: 10.1109/ACCESS.2020.2991420.

[15] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-Chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019, doi: 10.1109/ACCESS.2019.2922376.

[16] L. A. Shihab, "Technological Tools for Data Security in the Treatment of Data Reliability in Big Data Environments," *Int. Trans. J. Eng. Manag. Appl. Sci. Technol.*, vol. 11, no. 9, pp. 1–13, 2020.

[17] G.-C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dyn.*, vol. 75, no. 1, pp. 283–287, 2014.

[18] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[19] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimed. Tools Appl.*, vol. 79, no. 27–28, pp. 19853–19873, 2020, doi: 10.1007/s11042-020-08850-5.

[20] H. A. Younis, T. Y. Abdalla, and A. Y. Abdalla "Hiding Processing Approaches For Digital Images Encryption Using Wavelet Transform." Basrah Journal of Engineering science. Volume 8, Issue 1, Pages 1-12, 2008.