Optik - International Journal for Light and Electron Optics 259 (2022) 168989

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.com/locate/ijleo

Differential cryptanalysis of diffusion and confusion based information confidentiality mechanism

Noor Munir [a], Majid Khan [a,*], Iqtadar Hussain [b,c], Muhammad Amin [d]

[a] Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan
[b] Mathematics Program, Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, 2713 Doha, Qatar
[c] Statistical Consulting Unit, College of Arts and Science, Qatar University, Doha, Qatar
[d] Department of Avionics Engineering, Institute of Space Technology, Islamabad, Pakistan

ARTICLE INFO

Keywords:
Image encryption
Chaotic map
Cryptanalysis
Chosen-plaintext attack
Logistic map
Cat map

ABSTRACT

Wireless multimedia communications have progressed significantly in recent years. As a result, there is an increasing demand for more secure media transmission to protect multimedia information. Image encryption systems have been presented throughout the years, but those based on chaotic maps are the most secure and trustworthy due to the inherent properties in such types of multimedia contents involving the pixels strong correlation and data handling capacities. In this research, we have performed differential cryptanalysis of a recently suggested cryptosystem based on a three dimensional (3D) logistic map and 3D Cat map. The originally proposed approach was based on diffusion and confusion strategy. The vulnerabilities in the understudy cryptosystem lead to the successful proposed cryptanalysis attack. The original ciphers are recovered by means of a chosen-plaintext attack. The recovered data is also subjected to some statistical analysis to check the quality.

1. Introduction

In the past few years, the demand for data security is increased with the increase in the usage of social media devices. Data encryption is one of the easiest procedures to shield sensitive data. The field of cryptography, watermarking, and steganography provides data protection strategies. Cryptography is the study of secure encryption algorithms to secure private communication. Cryptography is divided into two major categories concerning the number of keys: symmetric encryption and asymmetric encryption. Symmetric encryption involves encryption and decryption with the same private key. The asymmetric algorithms include encryption with a public key and decryption by using a private key (only known to the receiver of the message). There are many conventional encryption structures proposed for secure communication such as Data Encryption Standard (DES) [1], Triple Data Encryption Standard (3DES) [2], Advanced Encryption Standard (AES) [3], Blowfish [4], Twofish [5] and Serpent [6], etc. All the traditional encryption approaches are not considered as a standard now due to some vulnerabilities in their encryption structure.

Chaos is considered one of the significant methods of randomness in cryptography. The reliability of chaotic maps includes their sensitive dependence on initial conditions and bifurcation parameters. Several chaotic systems have been devised with perfect bifurcation features [7–12]. Many chaos-based encryption structures have been already proposed in the literature [13–21]. Numerous encryption approaches include the substitution-permutation architecture in their working strides. On the other hand, to increase the

* Corresponding author.
E-mail addresses: mk.cfd1@gmail.com, id.khan@mail.ist.edu.pk (M. Khan).

https://doi.org/10.1016/j.ijleo.2022.168989
Received 1 December 2021; Accepted 24 March 2022
Available online 27 March 2022
0030-4026/© 2022 Elsevier GmbH. All rights reserved.

time efficiency in the encryption algorithms the researchers usually neglect the addition of the number of rounds and key dependency on the plaintext. The decrease in the number of rounds and key independence increases the risk of cryptographic attacks. As a result, many cryptosystems were found vulnerable to cryptanalysis attacks [22–28].

In this research, we have performed cryptanalysis of a recently suggested cryptosystem [29]. The understudy encryption approach was based on two different 3D chaotic maps utilized to create diffusion and confusion in the plain image. The key implementation was based on bitwise XOR and pixel permutation carried by 3D Logistic map and 3D Cat map respectively. The originally proposed encryption structure was vulnerable to the chosen-plaintext attack because of the independence of the key generation. The recovered data is also subjected to some statistical analyses such as histogram, entropy, and correlation. The results of the analyses depict that the recovered data is accurate. Moreover, the weaknesses in the original structure are highlighted and some improvements in the cryptosystem are suggested.

The rest of the paper is organized as follows: originally offered encryption structure is defined in Section 2; Section 3 offers the aspects of the proposed attack; some experimental analyses are performed in Section 4; outcomes are deliberated in Section 5; finally the conclusion is drawn in the last section.

2. Originally offered encryption approach

The originally offered cryptosystem completely depends on chaotic maps. Two different types of chaotic sequences are utilized for diffusion and permutation generated from Logistic and Cat maps, respectively. The diffusion process involves the sequence generation from the Logistic map by using some specific initial conditions and chaotic parameters. The confusion is performed by taking the random sequences from the 3D Cat map and applying them to permutation diffused data.

The working strides of the originally proposed schemes are as follows:

2.1. Diffusion process

The Logistic map is considered a wide source of randomness in chaotic cryptography. The 1D logistic map is defined as

$$x_{n+1} = ax_n - ax_n^2, \tag{1}$$

Where $0 < a < 4, x_n \in (0,1), n = 0,1,2,\ldots$ and x_n represent the nth iteration of the chaotic map. This system displays chaotic behavior when $a \in [3.57, 4]$. To increase the secret keyspace and improve the dynamical behavior, the 3D Logistic map was proposed in [34] and is defined as:

$$\left\{\begin{array}{l} x_{n+1} = ax_n(1-x_n) + by_n^2 x_n + cz_n^3, \\ y_{n+1} = ay_n(1-y_n) + bz_n^2 y_n + cx_n^3, \\ z_{n+1} = az_n(1-z_n) + bx_n^2 z_n + cy_n^3. \end{array}\right\} \tag{2}$$

where $x_n, y_n, z_n \in [0,1], n = 0,1,2,\ldots$ depicts the nth iteration of the 3-dimensional logistic map. The chaotic behavior of the Logistic map occurs when the range of the parameters is $a \in (3.53, 3.81), b \in (0, 0.022)$, and $c \in (0, 0.015)$.

Step 1: The input image I is separated into red I^R, green I^G, and blue I^B layers.

Step 2: The arrays generated from the Logistic map are saved as x^R, x^G, and x^B.

Step 3: The diffusion operation is performed between the arrays of step 1 and step 2 as:

$$\left\{\begin{array}{ll} D^R = & I^R \oplus x^R, \\ D^G = & I^G \oplus x^G, \\ D^B = & I^B \oplus x^B. \end{array}\right\} \tag{3}$$

Where D^R, D^G, and D^B are diffused layers of the image.

2.2. Confusion process

The confusion is created in the diffused data by permuting the pixels values using Cat map. The authors in [38] defined the 2D Cat map as:

$$\left\{\begin{array}{c} x_{n+1} = x_n + \alpha y_n, \\ y_{n+1} = \beta x_n + (1+\alpha\beta) y_n. \end{array}\right\} \tag{4}$$

where α, β are chaotic parameters. The 3D Cat map with more chaotic behavior has been proposed in [39] as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix}, \tag{5}$$

where A is the matrix that defines the chaotic behavior with $|A| = 1$. The matrix A is defined as:

$$A = \begin{pmatrix} \delta\gamma b + 1 & \gamma & \beta + \delta\gamma + \delta\beta\gamma c \\ c + \delta b + \delta\gamma bc & \gamma b + 1 & \delta + \beta c + \delta\beta b + \delta\gamma c + \delta\beta\gamma bc \\ b + \delta ac & a & \delta a + \beta b + \delta\beta ab + 1 \end{pmatrix}, \tag{6}$$

where $\delta, \beta, \gamma, a, b,$ and c are all real chaotic parameters.

The arrays obtained from the previous step are reconstructed and expanded into a cube with side length N, here N is computed by the following mathematical expression:

$$N = ceil\left(\sqrt{3m \times n \times 3}\right) \tag{7}$$

The arrays obtained from the Cat map are also reconstructed by using the same strategy defined previously. The data matrix of Cat map arrays obtained after data reconstruction is utilized to permute the pixels of reconstructed diffused data (D^R, D^G, D^B). The diffused data is permuted according to the sorting arrangement of Cat map reconstructed data. The permuted data matrices are stored red E^R, green E^G, and blue E^B layers respectively. The final encrypted color image is named as $E(R,G,B)$. The flowchart description of the originally proposed cryptosystem is displayed in Fig. 1.

3. Proposed attack strategy

In this section, we have proposed a chosen-plaintext attack with some basic aspects which lead to the successful understanding of structure. This section includes notations for attacks, basic encryption model, differential cryptanalysis, and chosen-plaintext attack.

3.1. Notations for attack

Some notations are utilized to indicate the encryption structure and proposed attacks. Table 1 indicates the notations and their representation in the offered attack.

3.2. Basic encryption model

The proposed cryptosystem comprises a diffusion and confusion strategy. The offered encryption structure can be reconstructed by using the strategy given in Fig. 1. The encryption procedure includes the following steps:

3.2.1. Key generation

The keys generated from the Logistic map and Cat map are stored as $\boldsymbol{K_1^i}$ and $\boldsymbol{K_2^i}$, $i = 1, 2, 3, \ldots$ respectively.

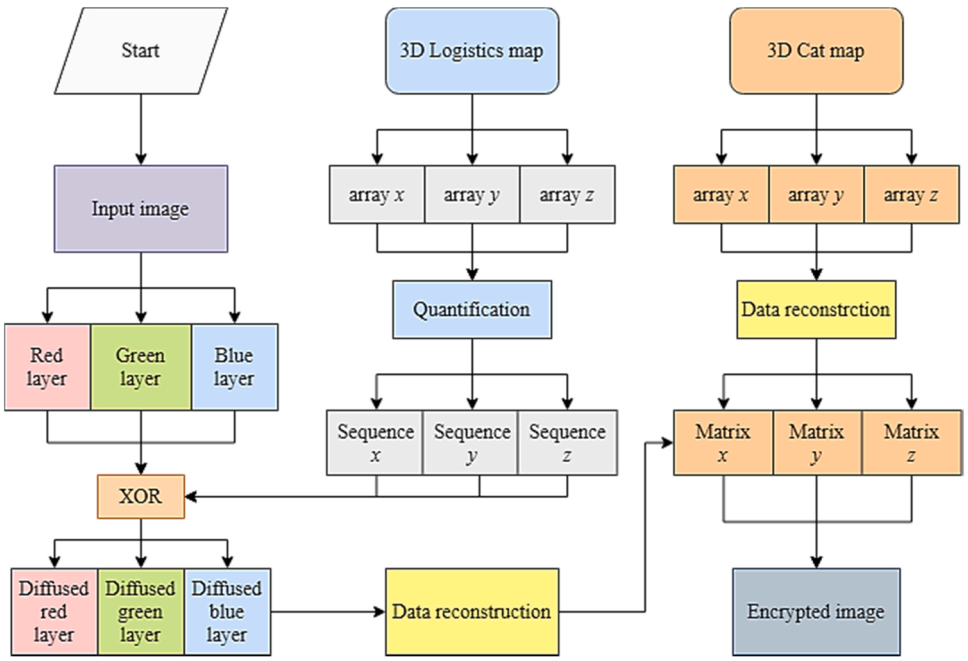

Fig. 1. Originally proposed cryptosystem.

Table 1
Notations for the offered attack.

Notation	Representation
Bold uppercase $\boldsymbol{A}$	Matrix
Upper case A	Constant
Lower case a	Variable or corresponding element of $\boldsymbol{A}$
Superscript $\boldsymbol{A}^{i}$	Matrix layers $\boldsymbol{i}$
Subscript $\boldsymbol{A}_{i}$	Different stages $\boldsymbol{i}$
$\boldsymbol{P}$	Plain message matrix
$\boldsymbol{E}$	Encrypted message matrix
$\varphi\boldsymbol{P} = \boldsymbol{P}_{1} \bigoplus \boldsymbol{P}_{2}$	XOR of $\boldsymbol{P}_{1}$ and $\boldsymbol{P}_{2}$
$\mathscr{C}\beta(\boldsymbol{P})$	Chaotic permutation

3.2.2. Diffusion using XOR

The diffusion is created in the plain message matrix $\boldsymbol{P}^{i}, i = 1, 2, 3, \ldots$ by using the XOR operation between $\boldsymbol{P}^{i}$ and $\boldsymbol{K}_{1}^{i}$ as follows:

$$\boldsymbol{E}_{a}^{i} = \boldsymbol{P}^{i} \oplus \boldsymbol{K}_{1}^{i}, \tag{8}$$

where $\boldsymbol{E}_{1}^{i}$ shows respective diffused image layers of $\boldsymbol{P}^{i}$ and $i = 1, 2, 3, \ldots$ shows red, green, and blue layers of the image matrix.

3.2.3. Confusion using permutation

The confusion operation is performed by using the chaotic shuffling operation carried by the key generated from the 3D Cat map. The chaotic permutation is performed on the diffused image layers $\boldsymbol{E}_{a}^{i}$ by using $\boldsymbol{K}_{2}^{i}$ as follows:

$$\boldsymbol{E}_{b}^{i} = \mathscr{C}\beta\left(\boldsymbol{E}_{a}^{i}, \boldsymbol{K}_{2}^{i}\right), \tag{9}$$

$$\boldsymbol{E}_{b}^{i} = \mathscr{C}\beta\left(\left(\boldsymbol{P}^{i} \oplus \boldsymbol{K}_{1}^{i}\right), \boldsymbol{K}_{2}^{i}\right) \tag{10}$$

Hence, the final equivalent encryption structure becomes:

$$\left\{ \begin{array}{l} \boldsymbol{E}_{a}^{i} = \boldsymbol{P}^{i} \oplus \boldsymbol{K}_{1}^{i}, \\ \boldsymbol{E}_{b}^{i} = \mathscr{C}\beta\left(\boldsymbol{E}_{a}^{i}, \boldsymbol{K}_{2}^{i}\right). \end{array} \right\} \tag{11}$$

3.3. Differential cryptanalysis

The differential cryptanalysis can be performed by selecting more than one pair of plaintext and its respective ciphertext. Consider that $\boldsymbol{P}_{1}$, $\boldsymbol{P}_{2}$ be the plain message matrices and $\boldsymbol{E}_{1}$, $\boldsymbol{E}_{2}$ be the respective encrypted message passed through the system (11). Therefore, the differential of ciphertext is given by:

$$\varphi\boldsymbol{E} = \boldsymbol{E}_{1} \oplus \boldsymbol{E}_{2} = \mathscr{C}\beta((\boldsymbol{P}_{1} \oplus \boldsymbol{K}_{1}), \boldsymbol{K}_{2}) \oplus \mathscr{C}\beta((\boldsymbol{P}_{2} \oplus \boldsymbol{K}_{1}), \boldsymbol{K}_{2}) \tag{12}$$

As we can also use property that

$$\mathscr{C}\beta((\boldsymbol{P} \oplus \boldsymbol{K}_{1}), \boldsymbol{K}_{2}) = \mathscr{C}\beta(\boldsymbol{P}, \boldsymbol{K}_{2}) \oplus \boldsymbol{K}_{1} \tag{13}$$

After using Eq. (13) into Eq. (12) we get,

$$\varphi\boldsymbol{E} = \boldsymbol{E}_{1} \oplus \boldsymbol{E}_{2} = \mathscr{C}\beta(\boldsymbol{P}_{1}, \boldsymbol{K}_{2}) \oplus \boldsymbol{K}_{1} \oplus \mathscr{C}\beta(\boldsymbol{P}_{2}, \boldsymbol{K}_{2}) \oplus \boldsymbol{K}_{1} \tag{14}$$

This encryption uses bit-level permutation, which scrambles the original bits without changing their values. When employing similar permutation vectors, the bits in the same coordinates will also be shifted to the same location in the ciphertexts. Therefore,

$$\mathscr{C}\beta(\boldsymbol{P}_{1}, \boldsymbol{K}_{2}) \oplus \mathscr{C}\beta(\boldsymbol{P}_{2}, \boldsymbol{K}_{2}) = \mathscr{C}\beta(\boldsymbol{P}_{1} \oplus \boldsymbol{P}_{2}, \boldsymbol{K}_{2}) = \mathscr{C}\beta(\varphi\boldsymbol{P}, \boldsymbol{K}_{2}) \tag{15}$$

Using Eq. (15) in Eq. (14) we get

$$\varphi\boldsymbol{E} = \boldsymbol{E}_{1} \oplus \boldsymbol{E}_{2} = \mathscr{C}\beta(\varphi\boldsymbol{P}, \boldsymbol{K}_{2}) \tag{16}$$

3.4. Chosen-ciphertext attack

The chosen-ciphertext attack is applied on the assumption that only selected ciphertext $\boldsymbol{E}_{i}$ and its respective plaintext $\boldsymbol{P}_{i}$ are available. The intermediate keys which lead to encryption and decryption are unaccessible. The proposed attack involves the following steps:

Construct $1 + R \times C$ chosen ciphertext, where R is the number of rows and C represents the number of columns. These ciphers are denoted as $\boldsymbol{E}_{0}$ and $\boldsymbol{E}_{r-c}$, $r \in [1, R], c \in [1, C]$, and their pixels are constructed by the following setup:

$$e_0(i) = 0, \quad i \in [1, R] \tag{17}$$

$$e_{r-c}(i) = \left\{ \begin{matrix} 2^{C-c}, & i = r, \\ 0 \quad , & i \neq r, i \in [1, R]. \end{matrix} \right\} \tag{18}$$

In other words, $\boldsymbol{E_{r-c}}$ can be created by spinning a lone bit of all zero-pixel image $\boldsymbol{E_0}$, from the first bit of the initial value to the last bit of the final value. Such an organization guarantees that any encrypted message $\boldsymbol{E}$ can be represented by $\boldsymbol{E_0}$ and $\boldsymbol{E_{r-c}}$ with binary multiplication and bit-wise XOR operations.

1. The respective plaintext obtained by the chosen-ciphertext attack is represented as $\boldsymbol{P_0}$ and $\boldsymbol{P_{r-c}}$ respectively.
2. The differential of the plaintext is defined with the property that

$$\varphi \boldsymbol{P_{r-c}} = \boldsymbol{P_{r-c}} \oplus \boldsymbol{P_0} \quad . \tag{19}$$

For any ciphertext $\boldsymbol{E} = \{e(r), r \in [1, R]\}$, its respective plaintext is denoted by $\boldsymbol{P}$, whose differential between $\boldsymbol{P_0}$ is further assumed as $\varphi \boldsymbol{P}$. We can compute $\varphi \boldsymbol{P}$ by using the expression given in Eq. (20) as:

$$\varphi \boldsymbol{P} = \prod_{r=1}^{R} \prod_{c=1}^{C} [\boldsymbol{E_{r-c}}(c) \times \varphi \boldsymbol{P_{r-c}}] \tag{20}$$

Where $\prod$ denotes the continuous bitwise XOR operation, $\boldsymbol{E_{r-c}}(c)$ represents the cth bit of the ciphertext $e(r)$.

Finally, the plaintext $\boldsymbol{P}$ is computed by

$$\boldsymbol{P} = \varphi \boldsymbol{P} \oplus \boldsymbol{P_0} \tag{21}$$

4. Experimental analysis

The proposed cryptanalysis structure is implemented for the decryption of several standard images. The experimental outcomes are displayed in Fig. 2. The standard image of Fruits with a size $512 \times 512 \times 3$ is selected for experiments. The depicted results indicate

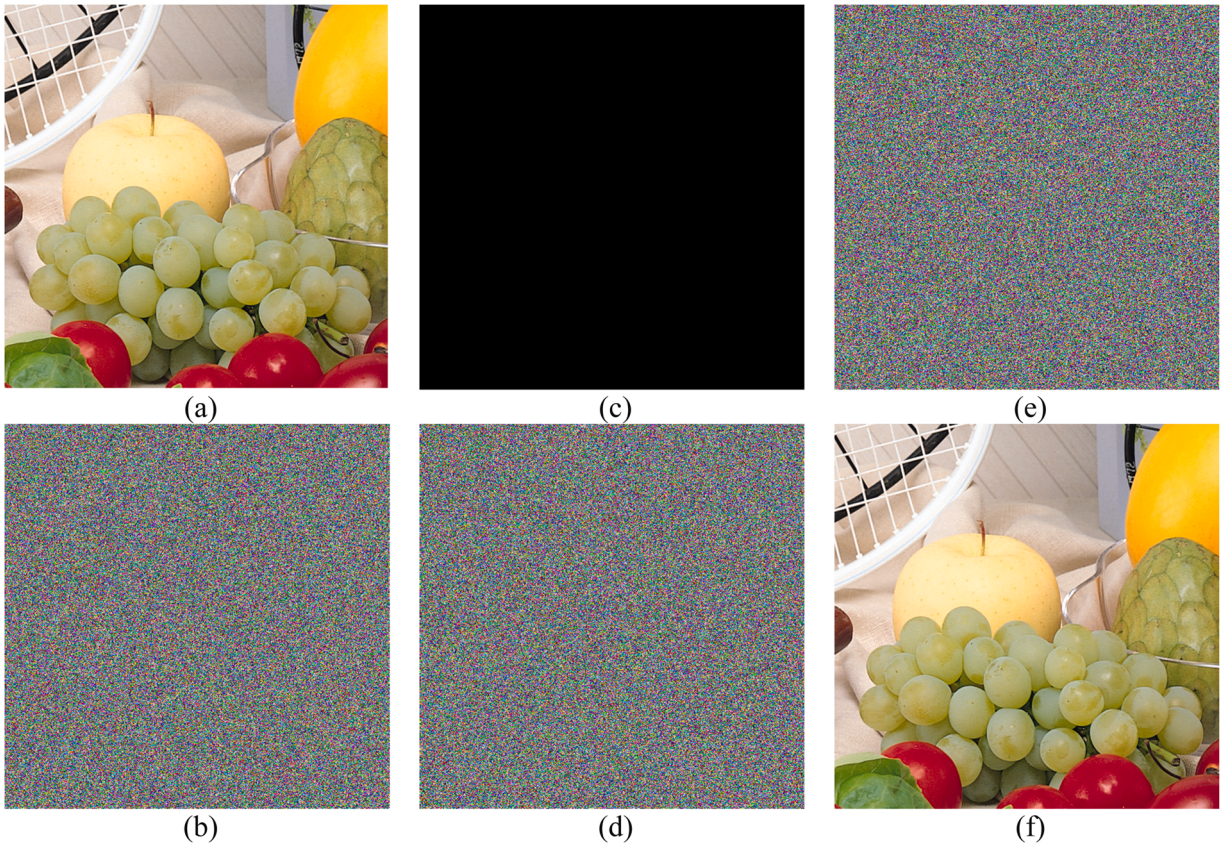

Fig. 2. Experimental results of proposed attack; (a) original image of Fruits; (a) respective cipher image of Fruits; (c) chosen cipher image $\boldsymbol{E_0}$; (d) respective decrypted image $\boldsymbol{P_0}$; (e) calculated differential image $\varphi \boldsymbol{P}$; (f) recovered Fruits image.

that the offered attack can successfully retrieve the original data from its respective ciphertext with very little computation.

Some statistical analyses are also performed on the retrieved and original data to check the quality of recovered information. The histogram, entropy, and correlation are performed to assure the accurate recovery of data.

4.1. Histogram

Histogram distribution analysis reveals the uniformity level of data. The distribution of each grey level in the image is reflected in the histogram. Fig. 3 shows histograms of the original, encrypted, and recovered images. The pixel distribution of the plain image is uneven, as can be seen. At the same time, its distribution follows a statistical pattern. In addition, the pixel distribution of the cipher image generated in this paper is extremely uniform. Similarly, the pixel distribution of the recovered image reveals the exact recovery

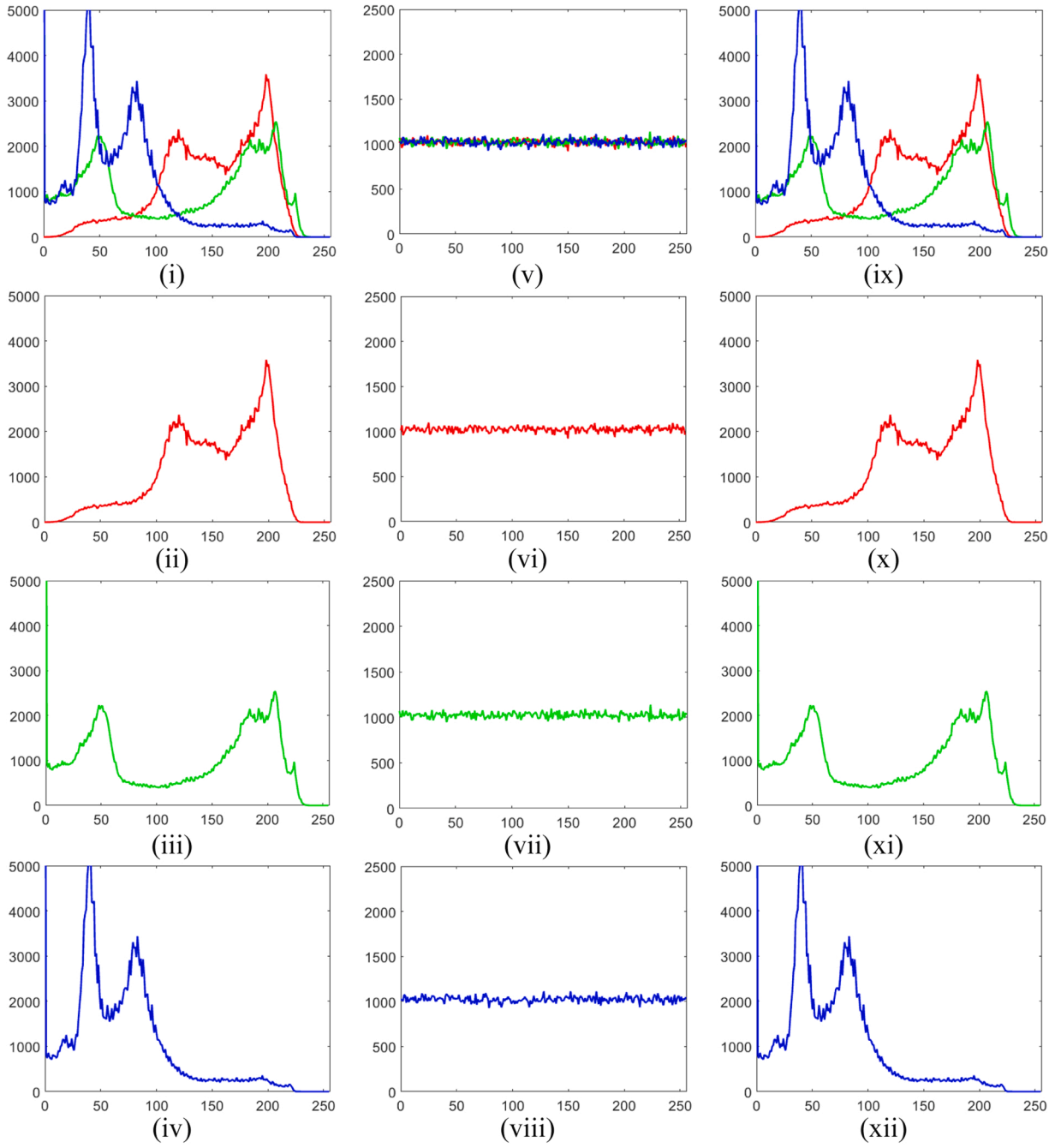

Fig. 3. Histogram of Peppers image (i-iv) original layers; (v-viii) encrypted layers; (ix-xii) retrieved layers.

of data.

4.2. Correlation analysis

It is continually fascinating to use the correlation coefficient, which is a statistical test for a algorithm's resistance to statistical assaults. The values are limited to − 1 and 1. When the correlation result is 1, the input and output images are perfectly correlated. When the value of correlation is zero, the input and output images are highly decorrelated. Let us evoke that an ideal cryptosystem should produce correlation results close to zero. To evaluate the strength of our encryption approach, we computed the correlation between original images and their respective ciphers using the following formula:

$$Correlation\_Coefficient = \frac{\mathrm{cov}(a,b)}{\sqrt{Q(a)}\sqrt{Q(b)}}, . \tag{22}$$

$$cov(a,b) = \frac{1}{R}\sum_{r=1}^{R}(a(r) - E(a))(b(r) - E(a)). \tag{23}$$

$$Q(r) = \frac{1}{R}\sum_{r=1}^{R}(a(r) - E(a))^2. \tag{24}$$

$$E(a) = \frac{1}{R\sum_{l=1}^{R} x(r)}. \tag{25}$$

where $R = M \times N$ shows the total number of pixels. To demonstrate the efficiency of the proposed attack we have calculated the correlation of original, encrypted, and recovered layers of Peppers image with size $512 \times 512 \times 3$. The results displayed in Table 1 depict that the correlation of original image layers is as same as the recovered one which reflects the zero error in the retrieved data.

4.3. Entropy

Entropy is a metric utilized in cryptography to evaluate the degree of unpredictability and randomness in an encrypted data. Because mutual information among pixels decreases as the level of disorder increases, entropy rises and becomes less predictable. The formula for calculating the entropy value $H(m)$ of any data m is:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \times \log\frac{1}{p(m_i)} \tag{26}$$

The probability of incidence of a specified pixel m_i is represented by $p(m_i)$. When the entropy of an 8-bit image is very close to 8, an encryption algorithm is good. As a result, given an encrypted image, the cryptosystem cannot deliver any evidence about the plain data. It is well known that the local entropy outperforms the global entropy as a tool for measuring randomness. The results in Tables 2 and 3 clearly show that the entropies of the original layer of the image as well recovered layers of the image are the same. This means the recovered data exhibits zero error and is exactly equal to the original data which ensures the accuracy of the proposed attack.

5. Results and discussion

5.1. Vulnerabilities in existing scheme

As we all know, an increasing number of researchers have been developing innovative data encryption approaches in the hopes of continuously improving encryption efficiency while attaining complex robustness. Yet, agreeing to this work and preceding crypt-analysis mechanisms, some of the existing encryption approaches have the subsequent issues that must be addressed.

Table 2
Correlation coefficient analysis for Peppers image.

Direction	Image layer	Original image	Encrypted image	Recovered image
Horizontal	Red	0.9567	-0.0006	0.9567
	Green	0.9586	0.0003	0.9586
	Blue	0.9966	0.0019	0.9966
Vertical	Red	0.9467	0.0012	0.9467
	Green	0.9387	-0.0001	0.9387
	Blue	0.9660	0.0005	0.9660
Diagonal	Red	0.9950	0.0013	0.9950
	Green	0.9570	-0.0004	0.9570
	Blue	0.9055	0.0015	0.9055

Table 3
Information entropy analysis for Peppers image.

Image layer	Original image	Encrypted image	Recovered image
Color	6.0496	7.9999	6.0496
Red	6.4126	7.9998	6.4126
Green	6.0547	7.9997	6.0547
Blue	6.2369	7.9998	6.2369

1. The use of fixed secret parameters or random values in the encryption structure makes it vulnerable to known cryptographic attacks. Such structures violate the design principles of modern cryptographic systems.
2. There are redundant encryption strides with similar encryption results utilized in the main structure. There is no difference in encryption effect, for example, among two sequential pixel permutation operations and one-pixel permutation operations.
3. The understudy image encryption scheme generates a huge amount of alike private keys in the keyspace while generating equivalent key streams. This, without a doubt, reduces the aptitude of the encryption scheme to withstand brute force attacks.

An attacker can easily simplify the encryption assemblies of some image encryption approach under certain conditions. Some cryptographers rely solely on statistical or randomness measures to validate the robustness of offered encryption approach, failing to completely examine and assess their security.

5.2. Improvement suggestions

In light of the aforementioned issues, we have made some suggestions for improvement. Certainly, we can say that forthcoming researchers will be capable to offer more precise and sensible answers to these concerns.

1. The generation of a hash corresponding to each plaintext and then utilization of this hash in the secret key can lead to secure encryption.
2. The cryptographer should examine the relationship among output and input for each encryption stride in the encryption procedure, and reflect whether this connection will damage or be abridged under explicit assault circumstances.
3. The increased number of rounds with some strategy in each stride may reduce the risk of attack.

To authenticate the robustness of an image encryption technique, the entire encryption structure must be examined and assessed from the perception of an assailant, in addition to standard security measures. Moreover, a comprehensive and in-depth analysis must be performed for each encryption step.

6. Conclusion

This research has evaluated the security of a recently proposed image encryption algorithm. The scheme was working on the phenomenon of diffusion and confusion carried by the 3D Logistics map and 3D cat map. The linearity between the differentials of ciphertext and plaintext was detected which leads to the differential cryptanalysis by using a chosen-ciphertext attack. The offered attack was successfully performed on the encrypted data and original data was retrieved. The original data was recovered without getting a secret key or the decryption algorithm. This paper also highlights some weaknesses in the existing schemes and suggests some improvements to get a secure cryptosystem. Therefore, the encryption scheme offered in [29] is vulnerable to differential attack and is not recommended for secure communication.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Declaration of Competing Interest

The authors declare that they have no conflict of interest.

Data Availability

The authors declare that data supporting the findings of this study are available within the article.

References

[1] Walter Tuchman, A brief history of the data encryption standard. Internet Besieged: Countering Cyberspace Scofflaws, ACM Press/Addison-Wesley Publishing Co, New York, NY, USA, 1997, pp. 275–280.
[2] IBM. Retrieved 2010-05–17.

[3] "Advanced Encryption Standard (AES)" (PDF). Federal Information Processing Standards. 26 November 2001. doi:10.6028/NIST.FIPS.197. 197.
[4] B. Schneier (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings.
[5] B. Schneier; J. Kelsey; D. Whiting; D. Wagner; C. Hall; N. Ferguson (1998–06-15). "The Twofish Encryption Algorithm" (PDF/PostScript). Retrieved 2013-01–14.
[6] Biham, Eli. "Serpent – A New Block Cipher Proposal for AES".
[7] J. Chen, J. Zhou, K.-W. Wong, Z. Ji, Enhanced cryptography by multiple chaotic dynamics, Math. Probl. Eng. (2011). Article ID 938454, 12 pages, 2011.
[8] C. Liu, T. Liu, L. Liu, K. Liu, A new chaotic attractor, Chaos, Solitons Fractals vol. 22 (5) (2004) 1031–1038.
[9] C. Zhang, W.K.S. Tang, S. Yu, A new chaotic system based on multiple-angle sinusoidal function: design and implementation, Int. J. Bifurc. Chaos vol. 19 (6) (2009) 2073–2084.
[10] X. Wang, J. Zhang, W. Zhang, Chaotic keystream generator using coupled NDFs with parameter perturbing. Cryptology and Network Security, Springer, Berlin, Germany, 2006, pp. 270–285.
[11] B.O. L. Amalia, A. M. Gonzalo, G. E. Alberto, P. D. Gerardo, R. G. Miguel, and M.V. Fausto, "Trident, a new pseudo random number generator based on coupledchaotic maps," in Proceedings of the 3rd International Conference onComputational Intelligence in Security for Information Systems (CISIS '10), pp.183–190, 2010.
[12] R.S. Katti, R.G. Kavasseri, V. Sai, Pseudorandom bit generation using coupled congruential generators, IEEE Trans. Circuits Syst. II vol. 57 (3) (2010) 203–207.
[13] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, W.J. Buchanan, Chaos-based confusion and diffusion of image pixels using dynamic substitution, IEEE Access 8 (2020) 140876–140895.
[14] M. Khan, N. Munir, A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic, Wirel. Pers. Commun. (2019), https://doi.org/10.1007/s11277-019-06594-6.
[15] El Hanouti, I., El Fadili, H., Souhail, W.and Masood, F., 2020, October. A Lightweight Pseudo-Random Number GeneratorBased on a Robust Chaotic Map. In 2020 Fourth International ConferenceOn Intelligent Computing in Data Sciences (ICDS) (pp. 1-6). IEEE.
[16] Lal Said Khan, Mohammad Mazyad Hazzazi , Majid Khan, Sajjad Shaukat Jamal , A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly nonlinear substitution boxes, Chinese Journal of Physics, Volume 72,
[17] N. Munir, M. Khan, Z. Wei, et al., Circuit implementation of 3D chaotic self-exciting single-disk homopolar dynamo and its application in digital image confidentiality, Wirel. Netw. (2020) httpsdoi.org10.1007s https://doi.org/10.1007/s11276-020-02361-9.
[18] Z. Hua, Y. Zhou, H. Huang, Cosine-transform-based chaotic system for image encryption, Inf. Sci. vol. 480 (Apr) (2019) 403–419.
[19] M. Alawida, J.S. Teh, A. Samsudin, W.H. Alshoura, An image encryption scheme based on hybridizing digital chaos and _nite state machine, Signal Process. vol. 164 (Nov) (2019) 249–266.
[20] Elkamchouchi H, Makar M (2005) Measuring encryption quality for bitmap images encrypted with rijndael andkamkar block ciphers. In: NRSC 2005Proceedings of the 22nd national radio scienceconference, 2005. IEEE, pp 277–284X.
[21] L. Wang, Teng, X. Qin, A novel color image encryption algorithm based on chaos, Signal Process. vol. 92 (4) (2012) 1101–1108 (Apr).
[22] N. Munir, M. Khan, S.S. Jamal, M.M. Hazzazi, I. Hussain, Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map, Math. Comput. Simul. (2021), https://doi.org/10.1016/j.matcom.2021.06.008.
[23] I. El Hanouti, H. El Fadili, K. Zenkouar, Cryptanalysis of an embedded systems' image encryption, Multimed. Tools Appl. 80 (2021) 13801–13820, https://doi.org/10.1007/s11042-020-10289-7.
[24] N. Munir, et al., Cryptanalysis of internet of health things encryption scheme based on chaotic maps, IEEE Access vol. 9 (2021) 105678–105685, https://doi.org/10.1109/ACCESS.2021.3099004.
[25] I. El Hanouti, H. El Fadili, Security analysis of an audio data encryption scheme based on key chaining and DNA encoding, Multimed. Tools Appl. 80 (2021) 12077–12099, https://doi.org/10.1007/s11042-020-10153-8.
[26] Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C; JohnWiley & Sons: Indianapolis, IN, USA, 2015.
[27] Kerckhoffs's Principle. Available online: ⟨http://crypto-it.net/eng/theory/kerckhoffs.html⟩.
[28] C.E. Shannon, , Communication theory of secrecy systems, Bell Syst. Tech. J. 4 (1949) 656–715.
[29] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, W. Wang, A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques, IEEE Access vol. 9 (2021) 61334–61345, https://doi.org/10.1109/ACCESS.2021.3073514.