Journal of Techniques, ISSN: 2708-8383, Vol. 5, No. 1, 2023, Pages 122-128
DOI: https://doi.org/10.51173/jt.v5i1.840

JOURNAL OF TECHNIQUES

Journal homepage*: http://journal.mtu.edu.iq*

RESEARCH ARTICLE - ENGINEERING

Image Encryption Using Lorenz Chaotic System

Daniah Abul Qahar Shakir [1], Ahmad Salim [2*], Seddiq Q. Abd Al-Rahman [1], Ali Makki Sagheer [1]

[1] University of Anbar, Anbar, Iraq

[2] Middle Technical University, Baghdad, Iraq

[*] Corresponding author E-mail: ahmadsalim@mtu.edu.iq

Article Info.

Article history:

Received
11 August 2022

Accepted
13 September 2022

Publishing
03 April 2023

Abstract

In the age of the Internet, a lot of images are circulated among users, and some of these images contain financial or personal information that requires confidentiality. Encryption algorithms existed for a long time, and the data used was focused on the text data, while the multimedia data was neglected for a long time. In addition, there are significant shortcomings in 3D image coding techniques. This paper proposed a method for image encrypted and decrypted electronically using the Lorenz chaotic system, the supposed algorithm was developed by using the three equations of the Lorenz system, before that, the image pixels are destroyed using reversible shifting and rotating processes to increase the randomness of the encrypted pixels and thus the difficulty of cracking the cipher. Then he supposed technique gave the following results: The average entropy calculation was (7.285) before image encryption and (7.9974) after image encryption with an average NPCR of (99.65%) and UACI was (30.35%) this confirms that the proposed method is reliable and applicable. Moreover, the suggested technique gives the best outcomes when compared to other similar works.

Publisher : Middle Technical University

Keywords: Data Security; Cryptography; Image Encryption; Chaos System; Lorenz Chaotic System; Pixel Destroy.

1. Introduction

Data are among the important assets of all companies that should be effectively protected. When data are stored, transmitted, and processed through any form of network system, concerns related to data protection arise. Currently, many forms of data security algorithms exist, but they have their application scope, advantages, and limitations [1]. The methods applied to secure data depend not only on the form and structure of data but also on whether this data resides in a centralized or decentralized system. In institutions that support decentralized systems, protecting data is the main concern [2].

Despite the gradual development in cryptography, encrypting sensitive information in images remains to be a computationally complex task. Information security is the set of procedures and methods designed to protect private, sensitive, and confidential information from unusual access or use. Availability, integrity, and confidentiality, and play the main role in information security. Most information worldwide is currently exchanged through the Internet. Storing data publicly made it easy for users to get important information from image data. In this respect, the fragility of image data is high [2, 3].

In such an open environment, many security concerns related to the process and transmission of digital images are raised. Therefore, the confidentiality and integrity of the images should be confirmed. Encryption technology is one of the effective mechanisms against potential threats. Symmetric key encryption, as well as asymmetric key encryption, are considered to be the main type of encryption. However, due to the large amount of information carried in images, implementing encryption on images is a challenging task compared with that ordinary data. The most difficult aspect of applying encryption on images is the degradation of image quality when extracting encrypted images [2, 4]. One of the most important techniques used recently in encryption images is the chaotic system [5, 6].

Chaos denotes 'the state of disorder.' Chaos theory is a typical field in mathematics, and its behaviour in dynamic systems is highly sensitive to initial conditions [7]. The characteristics of the chaotic system are deterministic and do not make it predictable, significant, and trustworthy [8, 9]. Image encryption algorithms are based on chaos theory, which is sensitive to initial conditions. Any dynamical system can be categorized as chaos if it meets the following settings: (i) sensitive to initial conditions, (ii) topological in mixing state, and (iii) dense for periodic orbits. This work proposes a new image encryption method based on the well-known chaos map (CM) encryption method to find a fast, robust, and completely secure method to ensure sending images safely without any information leakage.

The most important sections that will be reviewed in this manuscript are a review of previous work, then clarification of the proposed system, and a discussion of the results. Finally, the work is concluded.

Nomenclature & Symbols

SAE	Stacked auto-encoder	NPCR	Number of pixels of change rate
Mod	The remainder of the division	UACR	Unified average changing intensity
1D	One-dimension	AES	Advanced Encryption Standard
2D	Two-dimension	$\oplus$	Xor gate
3D	Three-dimension		

2. Related Works

The literature review presents traditional research only in the field of image security. Various works are being conducted to strive for the use of diverse forms of security methods. Fakhr (2017) [10]. 'This research proposes a novel method called multi-key compressed sensing and machine learning privacy protection computing scheme. This computing architecture consists of users, the cloud (storing encrypted data from the owner), and a trusted third party that is responsible for distributing randomly compressed sensing keys. This method is suitable for two general computing tasks: the Euclidean distance task and the dot product task. The developed method is tested on the COREL image classification task by using Euclidean distance and autoregressive inventory prediction task. Hu et al. (2017) [11] presented a batch image encryption scheme, which introduces a stacked auto-encoder (SAE) network to generate two chaotic matrices, is proposed. Then, one group is used to generate a total shuffle matrix to shuffle the pixel positions on each ordinary image, and the other group is used to generate a series of independent sequences. Each sequence is used to confuse the relationship between the replacement and encrypted images. Given the advantages of SAE's parallel computing, this scheme is effective, which greatly reduces the complexity of runtime. The mixed application of shuffling and obfuscation also enhances the encryption effect. To evaluate the efficiency of the program, we compare it with the popular 'logistics map' and achieve excellent performance in terms of running time estimation. Experimental results and analysis showed that the scheme provides effective encryption and can resist brute force, and statistical and differential attacks.

Many algorithms and techniques have been proposed based on chaotic systems that aim to encrypt 3D images. In [12] proposed encryption algorithm for 3D images depends on a chaotic system in addition to Deoxyribonucleic acid, the proposed algorithm gave good results, but it is considered a bit complicated. In [13] suggested an encryption algorithm for 3D images based on the chaotic values generated by the chaotic system in addition to the substitution technique taken from the AES algorithm, the proposed method gave competitive results. In [14] proposed a triple image coding technique that combines the chaotic systemو Arnold synergistic approach and the affine Hill technique. The proposed method is good but very complex.

There have been many previous studies that aimed to build an image encryption system based on the chaotic Lorenz equations. In [15] proposed an image encryption system based on Lorenz equations and Julia fractal key, the proposed hybrid method gets good results with less complexity. However, the proposed method gave fairly good results and the entropy was not competitive enough. In [16] proposed a chaotic system, which has been designed from three stages based on Lorenz equations, the equations have been modified and lost the character of linearity, where an exponent is added to the equation, the proposed method is good but very complex and consumes the system resources. This work aims to build an efficient and simple 3D image encryption system based on the chaotic Lorenz equations.

3. Lorenz Chaotic System

Recently, many image encryption schemes based on chaotic mapping have been proposed. Given that chaotic systems are highly sensitive to initial conditions and parameters, the interest in chaos schemes increased highly in many fields, such as the protection of databases, the Internet, transaction, and banking. That is, cryptography has strong encryption characteristics. A chaotic cryptographic system is resistant to any statistical attack. Although good accomplishments have been achieved in this field, a lot of issues remain and limit the application of existing encoding/decoding algorithms in actual systems.

In 1963, the American scientist Lorenz discovered during a weather study, a system called the Lorenzo system [17]. This system is considered the first dynamic system to show individual interactions and possesses rich, complex, and non-linear dynamic behaviour. Equation (1) is the dynamic equation that shows the three dimensions of the Lorenz system [18].

$$\begin{cases} \frac{dx}{dt} = a(y-x) \\ \frac{dy}{dt} = cx - xz - y \\ \frac{dz}{dt} = xy - bz \end{cases} \tag{1}$$

Where a, b, and c are the parameters of the Lorenz system, the ideal values for these parameters are: a=10, b=2.666, and c>=24.75, these values were obtained by experiment.

Fig. 1 shows the chaotic attractors generated from the Lorenz system [18]. The figure shows the difference between the three values (x, y, and z) and illustrates that these values are non-cyclical and unpredictable. In addition, the dynamic orbit is a three-dimensional double-helical structure [19].

The Lorenz system has many features that make it suitable in cryptographic operations, the most important of which are: The equations contain six parameters that can be used to increase the key space and thus the difficulty of predicting the key, moreover, the multidimensionality makes the dynamics of the system more complex [20].

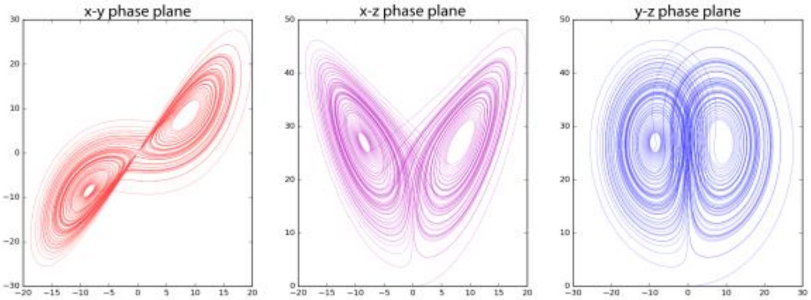

Fig. 1. Lorenz system chaotic attractors

4. The Proposed Encryption Schema

Recently, many different algorithms for image encryption and decryption utilising chaotic graphs have been proposed. Chaotic-based image encryption is highly desired in that field due to its performance and sensitivity. Previous works have demonstrated low-dimensionality image encryption based on this method, but these works are limited because of the limited key space with some flaws in the proposed models. For advanced security algorithms, 3D functions and algorithms are available to encounter security attacks.

4.1. Lorenz System Modification

The proposed work first illustrates the workflow and then describes the mathematical representation and the equation with all the required symbols. Finally, the algorithm is shown step by step to define the input, output, and steps. The proposed work is a Lorenz chaotic system that is useful in encrypting–decrypting a 3D image with three channels (red, green, and blue), where the proposed technique can be used to encrypt colour or grayscale images.

This section will be about how to create a hybrid methodology to encrypt and decrypt a three-channel (R, G, and B) image. However, to create a 3D chaotic encryption/decryption model from the Lorenz equations system, the original Lorenz equations (1) had to be modified to generate a sequence that preserves the dynamism and randomness to be used as a key in the image encryption process. The following three equations illustrate the proposed modified equations for the dimensions (first, second, and third) respectively.

$$x_i = (|a * (y - x_{i-1})| * i) \ mod \ 256 \tag{2}$$
$$y_i = (|cx - xz - y_{i-1}| * i) \ mod \ 256 \tag{3}$$
$$z_i = (|xy - b * z_{i-1}| * i) \ mod \ 256 \tag{4}$$

Where i is an integer number starting from one and it is the initial values of (x, y, and z). Certainly, the value of i in the equations will not linearly affect the equation so that it is easy to predict because the process between the value and the equation is a multiplication process, in addition to that, the resulting value of the equation is calculated the modular by the 256 to produce a single byte number that can be combined with the image hence pixel encryption.

The key space is how many keys can be implemented differently in a cryptographic system. In the proposed work, the key space is provided to be the higher security for CM. The 1D chaos is designed with less key space compared to 2D and 3D chaos, but the linear 3D type is less suitable. For this reason, 3D non-linear chaos is employed for security purposes. In this work, six conditions are used for the key space (a, b, c, x, y, and z) which will be resistance against exhausted attacks.

4.2. Destroy Image Process

This process aims to destroy the link between the pixels of the original image before it is encryption, to increase the entropy and thus make the image encryption process more robust. The demolition process must be reversible and able to return the original image after the decryption process, so the rotate operations are used in addition to the Xor gate. Rotate the image by n, where n is an integer and preferably (2, 3, or 4) to make a good difference from the original pixel value. In contrast, the reconstruction process is done after decrypting the reverse completely from the process of demolishing the image.

4.3. Proposed Encryption/Decryption Schema

The encryption schema proposed in this work consists of the following stages: firstly, the correlation between the pixels in the original image is destroyed and then divided into parts (R, G, and B); secondly, the three dimensions obtained from the Lorenz system equations are scrambled with the three arrays resulting from the first step to encrypt all the pixels; finally, the three parts that were encrypted in the previous step are combined to form the final encrypted image.

To illustrate the proposed scenario for image encryption, it will be explained in the form of a scheme and an algorithm. Fig. 2 illustrates the technique designed in this work for image encryption. Furthermore, Table 1 shows in detail the steps through which the proposed encryption scenario is used to encrypt images by using a modified chaotic Lorenz system.

Table 1. Image Encryption Algorithm

Input: Original Image (Lorenz Parameters)	
Output: Encrypted Image	
Begin:	
Step1:	Destroyed Image = destroy image by using the process in (4.2)

```
Step2:    R, G, and B = Decompose destroyed image to RGB
Step3:    Generate key sequences (X, Y, and Z) from modified Lorenz equations by using Lorenz parameters. (Equations 2, 3 ad 4)
          Encrypted R= Destroyed R $\oplus$ X (Key from step 3 Xor Image pixels)
Step4:    Encrypted G= Destroyed G $\oplus$ Y
          Encrypted B= Destroyed B $\oplus$ Z
Step5:    Encrypted image =  combined encrypted (R,  G, and   B)
Step6:    Return ( Encrypted image )
 End
```

The decryption scheme is the exact opposite of the encryption scheme, where the original image must be released by the encrypted image and the encryption key. The proposed decryption schema has the following stages: firstly, the image must be decomposed into parts (R, G, and B); secondly, the key obtained from the Lorenz system equations is scrambled with the three arrays resulting from the first step to decrypt the image; finally, the three parts that were decrypted in the second step are rebuild then combined to return the original image. Fig. 3 illustrates the proposed technique designed for image decryption.

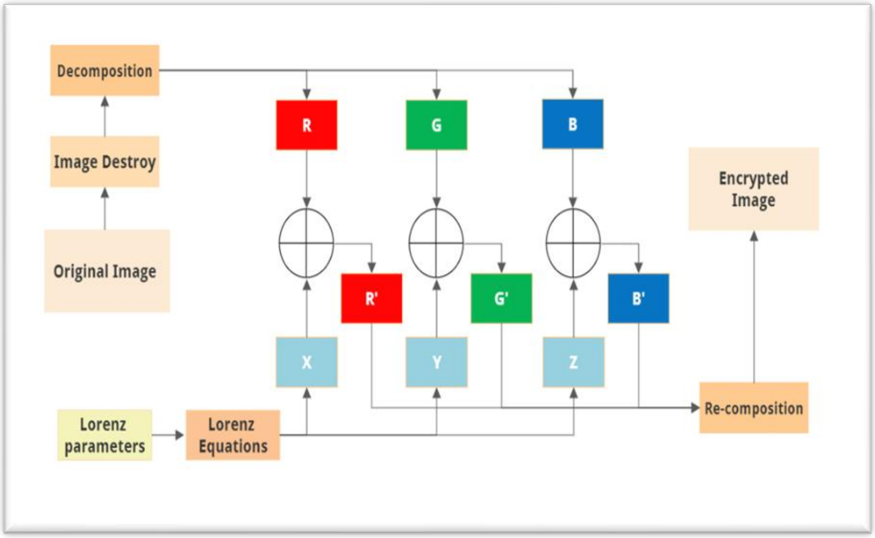

Fig. 2. Proposed Encryption Schema

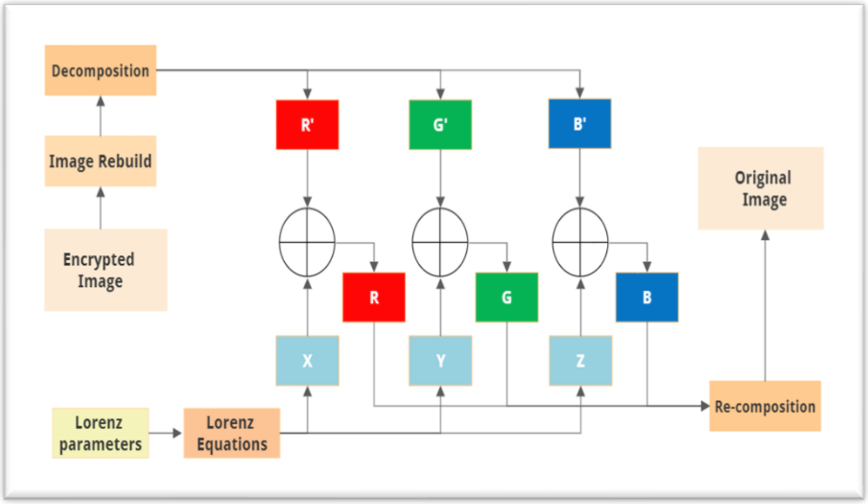

Fig. 3. Proposed Decryption Schema

5. Results and Discussion

The implementation and the results of the supposed system are illustrated in this section. As mentioned, many steps are performed to implement the supposed encryption-decryption technique using the supposed 3D chaotic technique. The equations and their initial values are predefined along with the supposed values that are used in the steps of the supposed algorithms. Lena's image with JPG extension is used with the supposed algorithm for image encryption and decryption at the same time. The same image is used in both operations, then the entropy of the results is calculated. Visual Studio 2019 environment was used to accomplish these steps, and the code is written after the steps of the algorithms are finalized. A Core i7 computer was used with 8 GB RAM and a CPU speed of 2.4 to build and test the proposed system. The supposed work accomplishes the goals of image encryption-decryption within a promising result that can be implemented with any other image to gain highly secure data. The initial values for each key used as a parameter in the Lorenz equation, are provided in Table 2. These parameters were used for encrypting in the proposed system and all results in this chapter depend on these parameters. Some of these values were selected according to the recommendations of previous work, and the other values were chosen randomly.

Table 2. Key values

Keys	Values
X	0.5
Y	2.93
Z	1.32
A	10
B	8/3
C	28.97

5.1. Pixel Diffusion

To visualize and determine how the pixels of each image are diffused, a comparison between the original image and the encrypted image is provided in Fig. 4. The pixels differ. The original RGB image and the pixel diffusion in the encryption images, the system tested on three images named Lena, Birds, and Butterfly, all images with size 512*512. From the images, the deformation rate of the encrypted image is remarkably high, given that no features of the original image remain in the encrypted images. This finding indicates that the proposed encryption algorithm is good and competitive in this aspect.

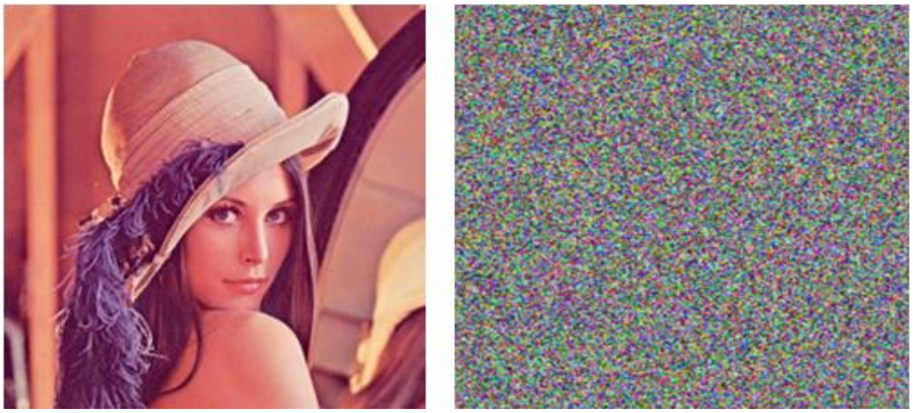

Fig. 4. The pixels diffusion of the Lena image

5.2. Histogram Visualisation

Histograms of the original and encrypted image are provided in Fig. 4. The histogram of the encrypted image in the figure, where the pixels are distributed evenly for the entire image set, leaves no useful data to anyone who tries to perform a security attack, especially in a situation in which a statistical attack can be performed on the image. From the results, the histogram values of the Lena image after the decryption are the same as the histogram values of the original image. Meanwhile, the histogram of the encrypted image leaves no useful data at all. Moreover, the histogram ratio was almost identical between the image before and after encryption, and this confirms that the proposed method preserved the image details and there was no loss. All results are obtained from the MATLAB environment directly and visualized in the following figure.

The strength of the encryption mechanism is evident in the images from histogram analysis through two points. Firstly, a great match is observed between the histogram image of the original image and the image after decryption (The entropy ratio was very similar between the two images as the value of mean squared error was less than 0.1). Secondly, the histogram image of the encrypted image shows that the distribution of pixels is largely flat, which indicates the strength of the encryption technique proposed. As a result, the histograms of the encrypted image show that all the images are similar in features, and this confirms that the proposed encryption method is good in the face of statistical attacks.

5.3. Entropy Calculation

The higher the uniformity of the distribution of the grey value is, the larger the info of the entropy will be. The ideal value of 8 is obtained in this case of the information entropy value of the encrypted image by the supposed method. As the entropy value in. Table 2 indicates the values of the entropy from the original and encrypted images. The entropy of the encrypted Lena’s images is almost the same at 7.9975, which is a promising value. In contrast, the entropy of the original image is significantly lower. In addition, the table shows a comparison between the proposed encryption technique and several other similar methods in terms of entropy (the comparison will be based on Lena's image). The results obtained by the proposed method are close to the optimal value, which means that the encrypted images will be more uniformly distributed, and the suggested system is efficient for image encryption. Moreover, according to the results shown in Table 3, it can be found that the proposed encryption technique has higher entropy values than other techniques in the related works, which also displays that the suggested method has a high degree of randomness.

5.4. NPCR and UACI Calculation

Several pixels of change rate (NPCR) and unified average changing intensity (UACI) are calculated in this section, these metrics are used to measure the resistance of the proposed method to differential attacks. The former is known as the ratio of the pixels of an image that varies amongst the encrypted image. The latter is known as the ratio of the difference amongst the encrypted images within A*B. The high difference ratio between the original and encrypted image shows that analysing and decrypting the image without the key are difficult processes. This finding indicates the strength of the algorithm and its impact on the encrypted image. Table 4 illustrates the NPCR and UACI of the supposed work in comparison with other methods (the comparison will be based on Lena's image). From the table, the NPCR and UACI values provide a promising result for the supposed algorithm compared with those for other algorithms. Compared with other methods, it is clear that the proposed method is superior, especially since the resulting values are closer to the optimal values. Moreover, the results confirm that the proposed method in this paper is well resistant to differential attacks. Moreover, the results confirm that the encryption algorithm is reliable as it achieved a strong difference between the original image and the encrypted image and did not preserve any of the features of the original image, which may thus facilitate the process of image detection through any kind of differential attacks.

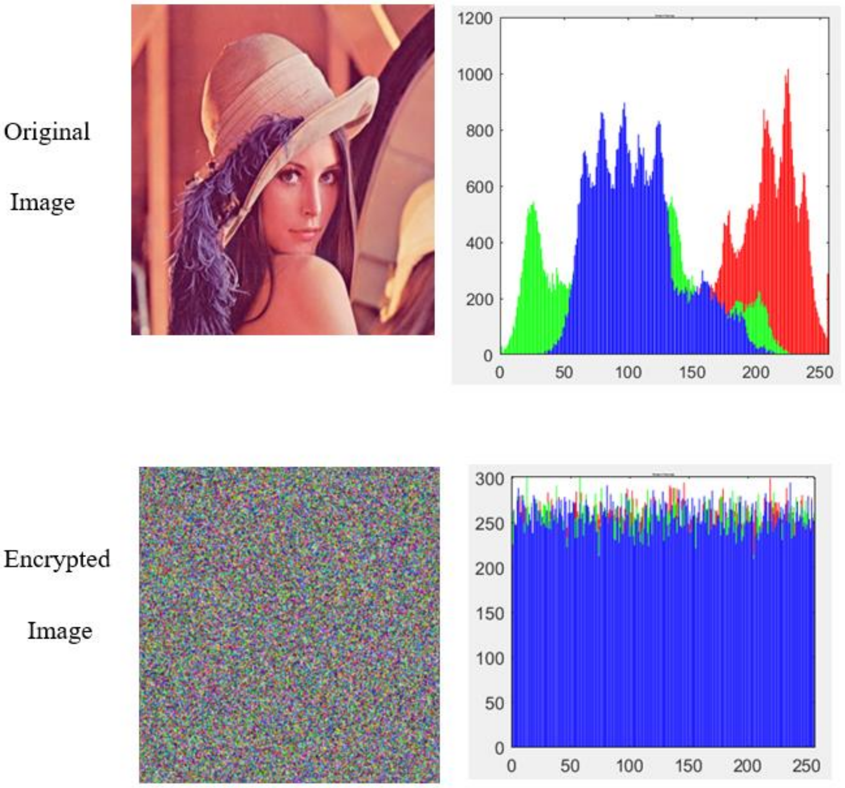

Fig. 5. Histogram Visualization of the Lena Image

Table 3. Compression of the Entropy Results

Technique	R	G	B
Original image	7.564	7.644	7.583
The proposed technique	7.9975	7.9973	7.9972
Technique [11]	7.9974	7.9971	7.9974
Technique [15]	7.9973	7.9972	7.9967

Table 4. NPCR and UACI Comparison

Method	NPCR (%)	UACI (%)
The supposed method	99.65	30.35
Method [11]	99.61	36.26
Method [15]	99.6	33.51
Method [16]	99.63	33.48

6. Conclusions

Encrypting 3D images in a secure and uncomplicated manner is a major challenge in the field of information security. In this paper, an image encryption scheme is proposed to encrypt grayscale or color images based on the Lorenz chaotic system. Chaotic systems have great advantages, the most important of which is that they are very sensitive to the base case, which makes them suitable for encryption techniques. The results prove that the proposed technique is competitive and good at resisting many known attacks that are used with encrypted images such as statistical attacks and brute-force attacks. Furthermore, the proposed algorithm outperformed many similar algorithms, and this confirms that the proposed work is competitive and can be adopted to maintain the confidentiality of digital images.

Acknowledgement

The research team thanks Prof. Dr. Ali Jubaeer for his assistance in the completion of this paper.

References

[1] S. R. Maniyath and V. Thanikaiselvan, “An efficient image encryption using deep neural network and chaotic map,” Microprocessors and Microsystems, vol. 77, p. 103134, 2020.

[2] M. T. Gaata and F. F. Hantoosh, “An efficient image encryption technique using chaotic logistic map and rc4 stream cipher,” International Journal of Modern Trends in Engineering and Research, vol. 3, no. 9, pp. 213–218, 2016.

[3] S. Ahadpour, Y. Sadra, and Z. ArastehFard, “A novel chaotic encryption scheme based on pseudorandom bit padding,” arXiv preprint arXiv:1201.1449, 2012.

[4] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, “Analytical study of hybrid techniques for image encryption and decryption,” Sensors, vol. 20, no. 18, p. 5162, 2020.

[5] A. Xing-Xing, S. Ke-Hui, H. Shao-Bo, and W. Hui-Hai, “Design and application of multi-scroll chaotic attractors based on simplified Lorenz system,” Acta Physica Sinica, vol. 63, no. 12, 2014.

[6] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos, Solitons \& Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[7] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, “Cryptanalysis of a discrete chaotic cryptosystem using external key,” Physics Letters A, vol. 319, no. 3–4, pp. 334–339, 2003.

[8] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A modified AES based algorithm for image encryption,” International Journal of Computer and Information Engineering, vol. 1, no. 3, pp. 745–750, 2007.

[9] C. He, K. Ming, Y. Wang, and Z. J. Wang, “A deep learning based attack for the chaos-based image encryption,” arXiv preprint arXiv:1907.12245, 2019.

[10] M. W. Fakhr, “A multi-key compressed sensing and machine learning privacy preserving computing scheme,” in 2017 5th International Symposium on Computational and Business Intelligence (ISCBI), 2017, pp. 75–80.

[11] F. Hu, J. Wang, X. Xu, C. Pu, and T. Peng, “Batch image encryption using generated deep features based on stacked autoencoder network,” Mathematical Problems in Engineering, vol. 2017, 2017.

[12] A. N. Kengnou Telem, H. B. Fotsin, and J. Kengne, “Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems,” Multimedia Tools and Applications, vol. 80, no. 12, pp. 19011–19041, 2021.

[13] M. Tanveer et al., “Multi-images encryption scheme based on 3D chaotic map and substitution box,” IEEE Access, vol. 9, pp. 73924–73937, 2021.

[14] M. A. Lone and S. Qureshi, “RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher,” Optik, vol. 260, p. 168880, 2022.

[15] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, “A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map,” Entropy, vol. 22, no. 3, p. 274, 2020.

[16] T. Li, W. Yan, and Z. Chi, “A new image encryption algorithm based on optimized Lorenz chaotic system,” Concurrency and Computation: Practice and Experience, vol. 34, no. 13, p. e5902, 2022.

[17] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, “Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys,” Neural Computing and Applications, vol. 31, no. 7, pp. 2395–2405, 2019.

[18] Z. Wu, P. Pan, C. Sun, and B. Zhao, “Plaintext-related dynamic key chaotic image encryption algorithm,” Entropy, vol. 23, no. 9, p. 1159, 2021.

[19] I. Grigorenko and E. Grigorenko, “Chaotic dynamics of the fractional Lorenz system,” Physical review letters, vol. 91, no. 3, p. 34101, 2003.

[20] J. Ahmad, F. Masood, S. A. Shah, S. S. Jamal, and I. Hussain, “A novel secure occupancy monitoring scheme based on multi-chaos mapping,” Symmetry, vol. 12, no. 3, p. 350, 2020.