MATHEMATICAL MODELING AND COMPUTING, Vol. 11, No. 3, pp. 702–709 (2024)

An efficient and lightweight image encryption technique using Lorenz chaotic system

Singh P. K., Jha B.*, Kumar S.

Department of Computer Science,
Central University of South Bihar, Gaya, Bihar
**Corresponding author: balmukund@cusb.ac.in*

(Received 10 March 2023; Revised 17 September 2024; Accepted 19 September 2024)

In the past few years, to store and transmit image data securely, numerous research initiatives on image encoding have been conducted. The primary objective of the image encryption technique is to safeguard the image by sabotaging the pixel pattern. Researchers suggested a safe, portable, and simple to use image encryption technique in this work. The encryption of the image is done using a bit-wise XOR operation, where the bit-wise operation is applied on each pixel of the plain image with a pseudo-random number that is created by the Lorenz chaotic system, to prevent unwanted access to confidential image data. The results of the experiments demonstrate that the suggested technique offers effective image encryption and decryption. The key stream of the encrypted image is made up of pseudo-random digits generated by the Lorenz Chaotic System. Several experimental tests have been performed, including histogram, correlation, information entropy, and differential analysis. The experimental findings reveal that the suggested approach performs image encryption and decryption efficiently.

Keywords: *cryptography; image encryption; Lorenz chaotic system.*
2010 MSC: 68 **DOI:** 10.23939/mmc2024.03.702

1. Introduction

Computer networks have revolutionized the use of information over the past 20 years. Information can be sent and received remotely through the internet by authorized people. The information must be kept secure from unauthorized change, shielded from unauthorized access (confidentiality), and available only to authorized parties when necessary (availability). In the last few years, multimedia security has evolved to include a category of tools and prototype expertise for digital media safety and improvement under a range of different attacks. Nowadays, information sent across the internet is not just text data but also multimedia data. A lot of information travels through networks i.e. involvement of the internet increases the congestion of the network that's why the security of the data becomes important. Therefore, encryption is required to maintain the security [1–5]. The procedure for converting plain text into cipher text, or readable format into an unreadable format, is known as encryption. To implement encryption, an encryption key (secret key) is used, which is a collection of numeric values known to both the sender and the recipient of encrypted content. Despite the fact that encrypted data appears random, it can be decoded by a person that acquires the encrypted data and has access to the encryption key. Encryption is of two types: (a) Symmetric Encryption: each party uses the same confidential key to encode and decode message; e.g. DES, 3DES, AES, RC4, etc. (b) Asymmetric or Public Key Encryption: in this, there are two keys: one is used during the encryption process at the sender side while the other is used at the time of decryption at receiver side; e.g. Diffie Hellman key exchange protocol, DSS, ElGamal, Elliptic-curve cryptography etc. [6–10]. Digital image security has gained interest and numerous image cryptographic algorithms that have been suggested to improve image security for the image being transmitted and stored on the cloud. However, the security of image sharing on networks is important. Image encryption is the process of hiding information that helps to transmit the image in a secure manner. The primary challenge in developing image encryption methods is the

difficulties in shuffling and diffusing the pixels of the image quickly. In this aspect, algorithms based on chaos have demonstrated good results. Chaotic maps have similar to traditional encryption algorithms but distinct characteristics like Ergodicity, initial condition sensitivity, and control parameters [6, 11–13]. Conventional encryption techniques, for example, are sensitive to secret keys, whereas chaotic maps are sensitive to beginning conditions and parameters [14]. The major difference between these two algorithms is the encryption operations: conventional encryption algorithms are based on finite sets, while chaos-based algorithms are based on real numbers that have strict mathematical sense. Therefore, to use of chaos in encryption is needed for better security performance. Fridrich proposed the Primary permutation-diffusion technique for image encryption based on chaos in 1998 [15].

2. Lorenz chaotic system

The 17th century is when the theory of fractional-order derivatives was first introduced. Since its introduction, it has developed predominantly as a pure theoretical area of mathematics. However, it has recently been demonstrated that differential fractional-order systems can be useful for physics, engineering, and even financial research. Since a chaotic system must have a border, the chaotic attractor is restricted in phase space. Determining the chaotic attractor's boundary is crucial for chaos management, chaos synchronization, and other applications [16]. In 1963, Lorenz found that the first chaotic system, which is an autonomous the third-order system with only two quadratic terms, produces complicated dynamic behaviors [17]. To convert a plaintext image into a cipher-text image, image encryption requires a very large key space. In the proposed algorithm, pseudo-random numbers were created utilizing the Lorenz chaotic system. It is said that the Lorenz system is

$$\begin{aligned} l' &= t(m-l), \\ m' &= vl - m - ln, \\ n' &= lm - un, \end{aligned} \tag{1}$$

where t, u, and v are variables. Depending on the values of t, u, and v, the appearance of a chaotic map will be very different on a different plain. Therefore, the values of t, u, and v produce an odd chaotic sequence.

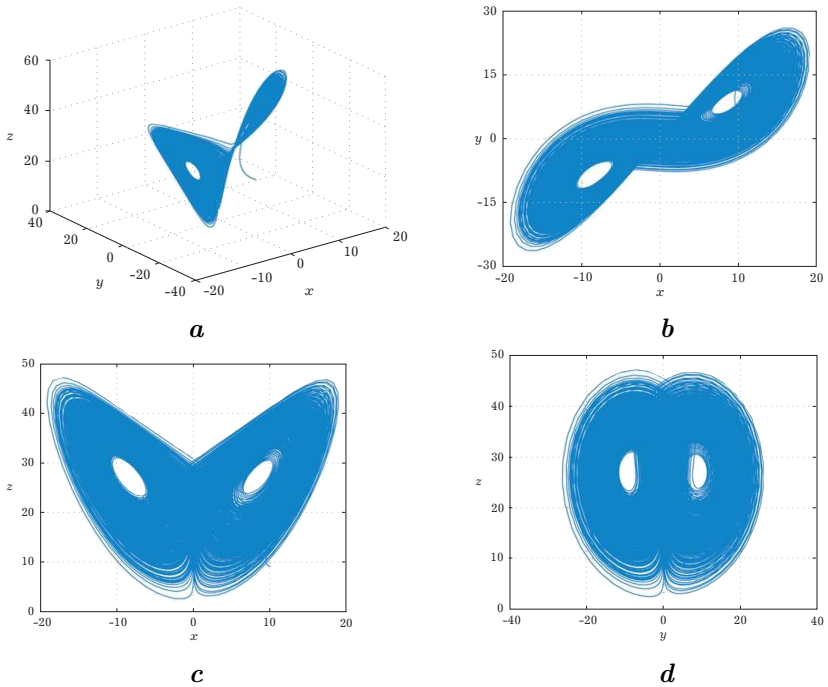

Fig. 1. The chaotic attractor of Lorenz: (***a***) all directions, (***b***) direction x-y, (***c***) direction x-z, (***d***) direction y-z [18].

3. Proposed algorithm

3.1. The image encryption algorithm

Following are essential elements of proposed image encryption method.

Algorithm 1

Input: Original image and random numbers produced by the Lorenz Chaotic System.
Output: Encrypted Image.

1: Enter the 512×512 grayscale image.
2: Enter all of the above image's associated pixel values into the 512×512 matrix **img**.
3: Create a series of pseudo-random numbers using the Lorenz Chaotic System and store them in a **rand_Lorenz** matrix with a 512×512 size.
4: The diffusion process was applied by performing a Bitwise-XOR operation on a sequence produced by the Lorenz chaotic system and a plain image, with the results being saved in the **encr_img** variable.
5: An encrypted image called **encr_img** is the last one to be stored in the image format.

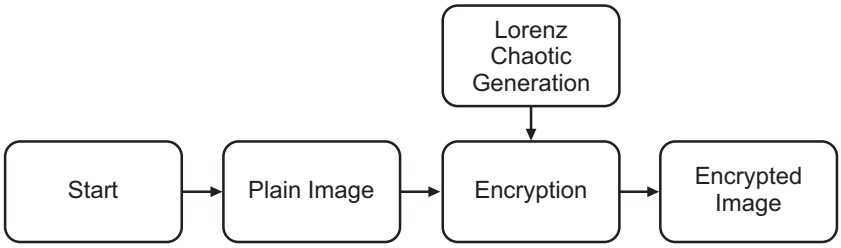

Fig. 2. Diagrammatic representation of suggested image encryption algorithm.

3.2. The image decryption algorithm

Following are essential elements of the proposed image decryption method.

Algorithm 2

Input: Encrypted image and random numbers produced by the Lorenz chaotic system.
Output: Original Image (gray scale Image).

1: Enter the cipher image.
2: Save each pixel's corresponding value of the above image in matrix **encr_img** of size 512×512.
3: Generate the sequence of pseudo-random numbers using the Lorenz Chaotic System, convert it into a 1D array, and finally, store it in array **rand_lorenz**. Also, convert encrypted image **encr_img** into a 1D array and store it into **encr_img_1d**.
4: Applied the decryption process by using Bitwise-XOR operation between **encr_img_1d** and **rand_lorenz**, and got the plain image.
5: Convert the obtained plain image's 1D array into 2D matrix **Image_Decr** and finally, **Image_Decr** is stored in the image format and it is an original plain image i.e. grayscale.

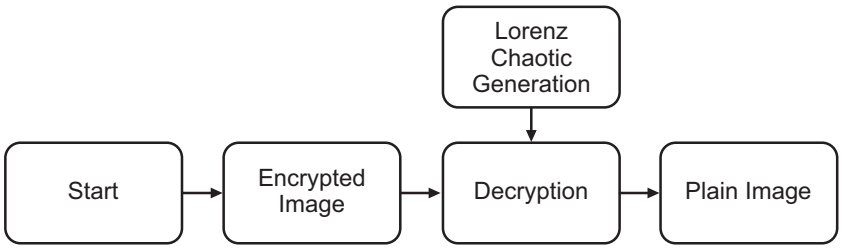

Fig. 3. Schematic representation of suggested image decryption technique.

4. Experimental results

4.1. Histogram analysis

Image histogram gives information about the allocation of image pixels. To inhibit statistical analysis assaults from obtaining every significant message from cryptographic image's histogram, the allocations of the cryptographic image must be uniform. The histogram allocations of the encrypted images are uniform, making it extremely impossible for anybody to read and extract the real image using a statistical attack, as seen in the figures below.

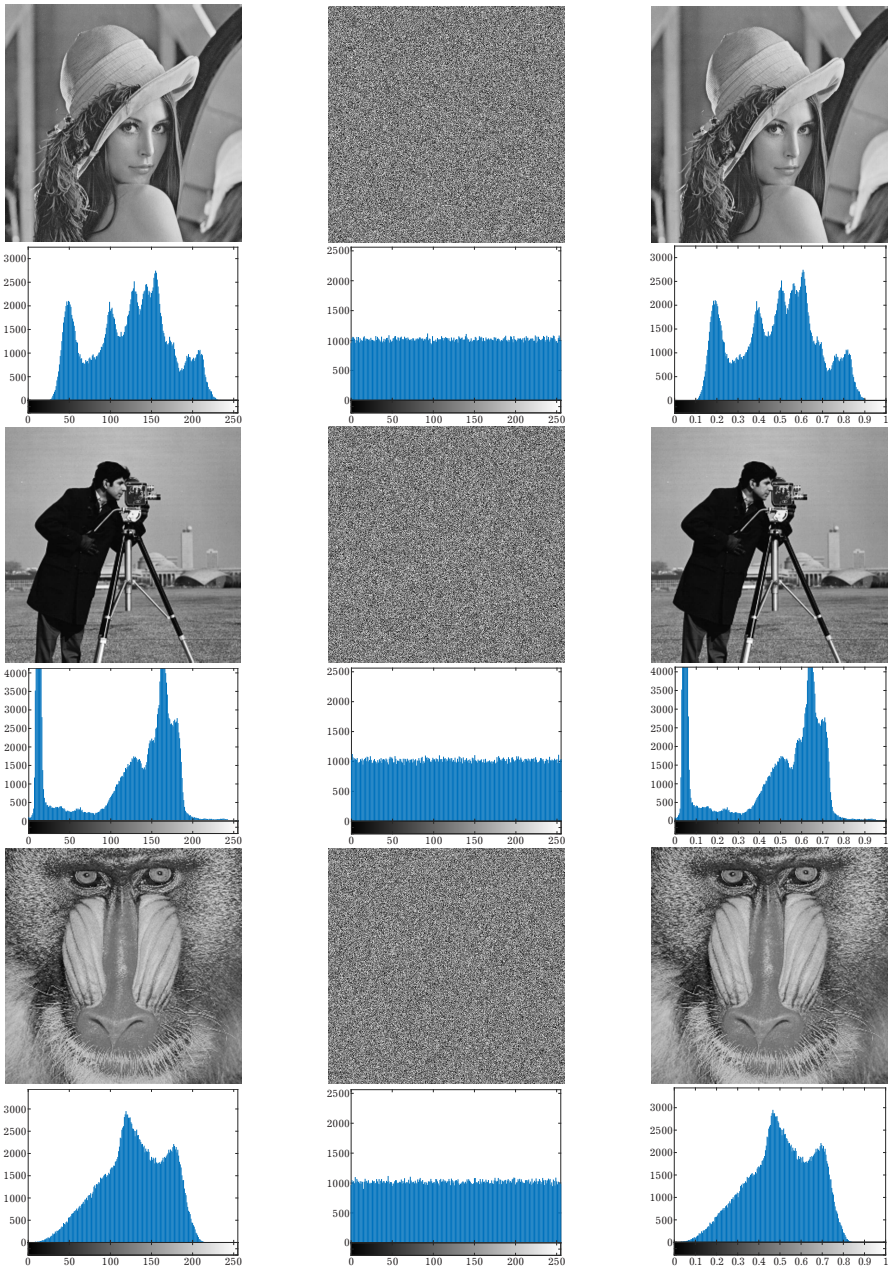

Fig. 4. The suggested algorithm's simulation results for three grayscale images. The 1^{st} row contains the plain, encrypted, and the decrypted Lena, while the 2^{nd} contains histogram of plain, encrypted, and decrypted Lena. The 3^{rd} row contains plain, encrypted, and decrypted cameraman, while the 4^{th} contains histogram of plain, encrypted, and decrypted cameraman. The 5^{th} row contains the plain, encrypted, and the decrypted mandril, while the 6^{th} contains histogram of plain, encrypted, and decrypted mandril.

4.2. Correlation analysis

The neighboring pixels in the plain-text image exhibit high horizontal, vertical, and diagonal correlations. The correlation values of image's pixel are reasonably low in an ideal encryption scheme to guard against statistical assaults. The following table shows the correlation allocation of two neighboring pixels along three axes. As observed in original image, the distributions of close pixels are significantly concentrated, indicating a considerable relationship. Yet, because allocations of neighboring pixels are random, the encrypted version of the main image has a poor correlation. When the neighboring pixel correlation is zero, it is optimal for a good image encryption approach [19]. Found it interesting, we utilized the following formulae in order to determine the correlation analysis:

$$Corr = \sum \frac{(l-\mu_l)(m-\mu_m)P(l,m)}{\sigma_l \sigma_m}. \tag{2}$$

In the above equation, $P(l,m)$ is the probability of a pixel value to be present at position (l,m), and the μ and σ symbols stand for the parameter's mean and standard deviation respectively. Table 1 shows three different correlations i.e. horizontal, vertical, and diagonal for different main and encoded images.

Table 1. Plain images' correlation coefficients with their associated encryption images.

Image	Horizontal correlation	Vertical correlation	Diagonal correlation
Lena	0.9719	0.985	0.9593
Encoded lena	0.0012	−0.0018	−0.0020
Cameraman	0.9831	0.9900	0.9733
Encoded cameraman	0.0023	0.0005	−0.0004
Mandril	0.9337	0.9123	0.8669
Encoded mandril	0.0012	0.0001	−0.0038

4.3. NPCR & UACI

Attackers usually try to decipher encrypted images by making little modifications to the original image and observing how much of a difference the encrypted image makes. For example, they may edit a single pixel in the original image and compare the differences between the original and encrypted versions. These studies investigated the effects of modifying a single pixel in the encoded image's actual image. Two approaches, NPCR and UACI, are used to assess the sensitivity of a single-bit alteration in the actual image. NPCR is the number of pixels changing per second in encrypted images [20]. When the original image even slightly changes, the encrypted image must be drastically updated. The Unified Average Changing Intensity (UACI) is used to calculate the average intensity of the pixel difference between two images [21]. The following formulae are used to calculate NPCR and UACI:

$$\text{NPCR} = \frac{\sum_{i,j} K(i,j)}{U \times V} \cdot 100\% \tag{3}$$

$$\text{UACI} = \frac{1}{U \times V} \sum_{i,j} \left(\frac{C_1(i,j) - C_2(i,j)}{255} \right) \cdot 100\%. \tag{4}$$

Table 2. NPCR as well as UACI estimates (in %).

Image	NPCR	UACI
Lena	99.6093	33.4635
Cameraman	99.6093	33.4635
Mandril	99.6093	33.4635

C_1 and C_2 are the encrypted images that were created by changing one bit in the plain image, where U and V stand for the image's rows and columns. The NPCR and UACI values of different images were experimentally determined; the findings are reported in Table 2. It illustrates how a minor modification to the source images can result in a notable distinction in the encoded image. The suggested method thereby defends against differential attacks.

4.4. Information entropy analysis

The information entropy is a way for determining the degree of unpredictability in an encryption scheme. It computes the pixel distribution for each gray-scale pixel value. If the entropy score is high, the distribution will be uniform. When the mutual information of an encrypted image drops, the entropy value of the image falls. If an image has a more uniform distribution, it will be more resistant to statistical assaults. The following equation can be used to define it [20]:

$$E(T) = -\sum_{i=1}^{N} P(t_i) \log(P(t_i)), \tag{5}$$

where t_i is the ith gray value, $P(t_i)$ is the probability of gray level t_i. For gray-scale images, the level having intensity values between 0 to 255, the maximum value of the entropy is 8 (ideal condition) [22]. The entropy of different gray images is shown in Table 3. The results show that the entropy of the cipher images is near 8, which is preferred. This suggests that the proposed image encryption technique almost prevents the information from leaking.

Table 3. Information entropy's outcomes.

Image	Information entropy
Lena	7.4451
Encoded lena	7.9994
Cameraman	7.0480
Encoded cameraman	7.9992
Mandril	7.2925
Encoded mandril	7.2925

5. Conclusion

A lossless and lightweight image encryption technique is given in this study, which employs the Lorenz Chaotic System to create a chaotic series of pseudo-random integers. Encryption is done with Bitwise-XOR operation using pseudo-random numbers generated by Lorenz chaotic system. Since the ciphered image's neighboring pixel correlation is much lower than that of the plain image, and the entropy of the encrypted image is approaching its maximum value. So,it avoids correlation attacks. Therefore, image encryption is cryptographically ensured in the transition from a source to a destination over the network. Since the values of NPCR and UACI are very high and meet the standards accepted in the industry, the differential attacks are difficult to guess the key for breaking the encrypted image. In the future, the work is experimented with and tested over all three component of the color image which is red, green, and blue to produce a cipher image, so that the color image can also be transmitted through a transmission line in a safe way.

[1] Wang X., Xue W., An J. Image encryption algorithm based on Tent-Dynamics coupled map lattices and diffusion of Household. Chaos, Solitons & Fractals. **141**, 110309 (2020).

[2] Wang X., Feng L., Zhao H. Fast image encryption algorithm based on parallel computing system. Information Sciences. **486**, 340–358 (2019).

[3] Wang S., Wang C., Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. Optics and Lasers in Engineering. **128**, 105995 (2020).

[4] Luo Y., Yu J., Lai W., Liu L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications. **78**, 22023–22043 (2019).

[5] Man Z., Li J., Di X., Sheng Y., Liu Z. Double image encryption algorithm based on neural network and chaos. Chaos, Solitons & Fractals. **152**, 111318 (2021).

[6] Abdmouleh M. K., Khalfallah A., Bouhlel M. S. Image encryption with dynamic chaotic Look-Up Table. 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). 331–337 (2012).

[7] Tanenbaum A. S., Wetherall D. J. Computer Networks. Prentice Hall, New Jersey (2003).

[8] Li J., Chen L., Cai W., Xiao J., Zhu J., Hu Y., Wen K. Holographic encryption algorithm based on bit-plane decomposition and hyperchaotic Lorenz system. Optics & Laser Technology. **152**, 108127 (2022).

[9] Zhang Q. An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. 2021 2nd international conference on computing and data science (CDS). 616–622 (2021).

[10] Al-Shabi M. A. A survey on symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications (IJSRP). **9** (3), 576–589 (2019).

[11] Baptista M. S. Cryptography with chaos. Physics Letters A. **240** (1–2), 50–54 (1998).

[12] Xiong Z., Wu Y., Ye C., Zhang X., Xu F. Color image chaos encryption algorithm combining CRC and nine palace map. Multimedia Tools and Applications. **78** (22), 31035–31055 (2019).

[13] Thoms G. R., Muresan R., Al-Dweik A. Chaotic encryption algorithm with key controlled neural networks for intelligent transportation systems. IEEE Access. **7**, 158697–158709 (2019).

[14] Chen G., Mao Y., Chui C. K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals. **21** (3), 749–761 (2004).

[15] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos. **08** (06), 1259–1284 (1998).

[16] Wu Y., Noonan J. P., Agaian S. A novel information entropy based randomness test for image encryption. 2011 IEEE International Conference on Systems, Man, and Cybernetics. 2676–2680 (2011).

[17] Li D., Lu J.-a., Wu X., Chen G. Estimating the ultimate bound and positively invariant set for the Lorenz system and a unified chaotic system. Journal of Mathematical Analysis and Applications. **323** (2), 844–853 (2006).

[18] Xiao S., Yu Z., Deng Y. Design and analysis of a novel chaos-based image encryption algorithm via switch control mechanism. Security and Communication Networks. **2020** (1), 7913061 (2020).

[19] Huang C. K., Liao C. W., Hsu S. L., Jeng Y. C. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommunication Systems. **52**, 563–571 (2013).

[20] Wu Y., Noonan J. P., Agaian S. A novel information entropy based randomness test for image encryption. 2011 IEEE International Conference on Systems, Man, and Cybernetics. 2676–2680 (2011).

[21] Wang X.-y., Chen F., Wang T. A new compound mode of confusion and diffusion for block encryption of image based on chaos. Communications in Nonlinear Science and Numerical Simulation. **15** (9), 2479–2485 (2010).

[22] Ahmad M., Alam M. S. A new algorithm of encryption and decryption of images using chaotic mapping. International Journal on Computer Science and Engineering. **2** (1), 46–50 (2009).

Ефективна та легка техніка шифрування зображень із використанням хаотичної системи Лоренца

Сінгх П. К., Джа Б., Кумар С.

Кафедра комп'ютерних наук,
Центральний університет Південного Біхару, Гая, Біхар

За останні декілька років для безпечного зберігання та передачі даних зображень було проведено численні дослідницькі ініціативи щодо кодування зображень. Основна мета техніки шифрування зображення — захистити зображення шляхом саботування піксельного шаблону. У цій роботі дослідники запропонували безпечну, портативну та просту у використанні техніку шифрування зображень. Шифрування зображення виконується за допомогою побітової операції XOR, де побітова операція застосовується до кожного пікселя простого зображення з псевдовипадковим числом, яке генерується хаотичною системою Лоренца, щоб запобігти небажаному доступу до конфіденційних даних зображення. Результати експериментів демонструють, що запропонована методика забезпечує ефективне шифрування та дешифрування зображень. Ключовий потік зашифрованого зображення складається з псевдовипадкових цифр, які згенеровані хаотичною системою Лоренца. Було проведено декілька експериментальних тестів, включаючи гістограму, кореляцію, інформаційну ентропію та диференціальний аналіз. Експериментальні результати показують, що запропонований підхід ефективно виконує шифрування та дешифрування зображень.

Ключові слова: *криптографія; шифрування зображення; хаотична система Лоренца.*