2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE) | 979-8-3503-7156-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/AMATHE61652.2024.10582063

Hybrid Image Encryption for WISN in Privacy Protection and Security of Public Big Data Using Chaotic Maps

Nikhitha Geddada
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India
ng3479@srmist.edu.in

Aditi Sahu
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India
as6463@srmist.edu.in

Suseela G
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India
suseelag@srmist.edu.in

Jayshnav S
Department of Computing Technologies
SRM Institute of Science and Technology
Chennai, India
js4264@srmist.edu.in

Suchi Arora
Department of Networking and Communications
SRM Institute of Science and Technology
Chennai, India
sa3590@srmist.edu.in

***Abstract*— Image big data has become pervasive in today's world. Every day huge volumes of data are being transferred across systems. Significant advancements have been made in networking and file transfer technologies. Due to the remarkable expansion of network infrastructures, multimedia transmission has become inevitable. Image data is being produced at a faster rate and the variety of data types is expanding rapidly. A number of big data-related surveillance applications use wireless image sensor networks (WISN). Important and sensitive data must be hidden from different hackers trying to break into the system. So, encryption is used to hide sensitive information from various hackers. Lorenz attractor along with the chaotic maps are used to withstand statistical attacks. Dual confusion and dual diffusion are implemented so as to ensure maximum chaos and makes the encryption system strong against attacks. The pixels of the image are scrambled using logistic maps so that only authorized users can decipher it. Through the integration of tent map and logistic map, this study approaches an efficient image encryption algorithm.**

Keywords— Image Encryption, Confusion, Diffusion, Chaotic maps, Logistic map, Tent map, Lorenz attractor

I. Introduction

Wireless image sensor networks are extensively employed in vital applications, which has resulted in a significant amount of image data being accumulated by sensors. The data frequently comprises visual information pertaining to the network's monitored phenomena, events, or immediate surroundings. Image communication has developed potential applications, including surveillance, industrial control systems, smart home systems, habitat monitoring, and critical infrastructure monitoring, as a result of the significance of WISN. The enormous volume of image data created and shared inside the network, which is available to authorized users for a variety of uses including monitoring, analysis, and decision-making, is referred to as "image public big data." Applications such as surveillance, environmental monitoring, and healthcare depend heavily on this visual data. In order to safeguard data privacy and defend the network from threats, appropriate security measures must be taken.

Encryption processes images in an effort to protect sensitive and confidential data by converting them to a format that is challenging to decipher in the absence of the corresponding decryption key. In WISNs, data privacy needs to be guaranteed, and chaotic maps work well for encrypting a lot of data, including images. Numerous security issues, such as privacy threats, misuse of sensitive data, and data breaches, might arise from this. Using encryption is essential to preventing these threats. In order to execute image encryption and assess the outcomes in accordance with predetermined criteria, this project mixes hybrid chaotic maps with the Lorenz attractor. A high degree of encryption is provided by chaotic maps, making it exceedingly difficult for adversaries to decode the encrypted image from the original file. The degree of encryption and efficiency is measured my two metrics named UACI and NPCR values.

Among the modules utilized to put these encryption approaches into practice are:
'matplotlib.image' is used to read an image and display intermediate results. 'matplotlib.pyplot' provides the original image, encrypted and decrypted images, and histograms. 'numpy' stores and manipulates image data. 'cv2' and 'OpenCV' provides functions for image processing and computer vision tasks.

II. Literature Survey

Chaotic maps have attained wide interest in the sector of digital image encryption. Due to the increase in the network bandwidth, multimedia of large sizes is now being transferred from one device to another [1]. The following two phases are generally implemented in any chaotic encryption process:

a. Pixel Shuffling (Confusion) phase: Pixel shuffling is a technique used in image processing for scrambling the pixel positions of the image. It involves rearranging the pixels and changing their current positions and this results to pixel decorrelation [2,3].

b. Pixel modification (Diffusion) phase: This phase involves modifying the pixel values [4,5] and this makes the encryption even more complex and harder to decrypt. The

chaotic maps used are Tent map [6,7], Logistic map [8-12]. These maps are used for pixel diffusion [2,6] in two separate stages. For pixel confusion [4,6] Lorenz attractor [13-16] is used. The extensive research done on image encryption [1,10,12] prove that traditional methods aren't the best way to encrypt an important sensitive image. This project combines the two chaotic maps and applies the Lorenz system [13,15,16] for this reason and aims to bring a computationally higher-level encryption.

The combination of tent map [10,11,17] and logistic map [7,8,12] have been implemented. The standard images used for digital image encryption are used in this project: Lena [3,5,7], Horizon [5,18] and a test image. To evaluate the complexity level of the encryption, this paper uses different parameters: Key sensitivities [21], Histogram analysis [2,3,19], Auto pixel correlation [17,18], the Unified Average Change in Intensity (UACI) [5,19,20] and number of Changing Pixel Rate (NPCR) [21].

III. Proposed System

This research work presents a method for encrypting images that combines two chaotic maps: logistic and tent map as shown in Fig. 1. The ultimate objective is to increase variability and security of the required image transmitted in a WISN. Real-time encryption ensures timely protection of sensitive data and enhances the overall security of the network. To avoid excess confusion, resulting in overlapping of pixels, a pixel is allocated to each point on the Lorenz attractor, which is a chaotic system. The degree of chaos in the system may be altered to produce a variety of visual effects, such as changes in texture, pattern, or colour distribution, by varying a constant parameter called 'r'. This flexibility of dynamically adjusting the 'r' value enables fine-tuning of the encryption algorithm based on specific security requirements or application scenarios. Diffusion is the method by which the pixels are dispersed throughout the image which is done using the tent map. The next step of confusion and diffusion uses the logistic map, where each pixel is mapped to the equation

$$x = r * x * (1 - x) \tag{1}$$

Multiple stages of confusion and diffusion, each employing different chaotic maps, creates a multi-layered efficient encryption scheme. The resulting encrypted image is evaluated using the UACI and NPCR values, which measure the degree of correlation and the percentage of changed pixels between the original and encrypted images, respectively. Furthermore, the primary sensitivity is assessed to determine how sensitive the encryption method is to changes in settings or inputs, and a histogram analysis is performed to find any notable deviations in the distribution of pixel values. The recommended image encryption method has exceptional security and overall unpredictable properties, which henceforth qualifies it for practical application with key generation as shown in Fig. 2.

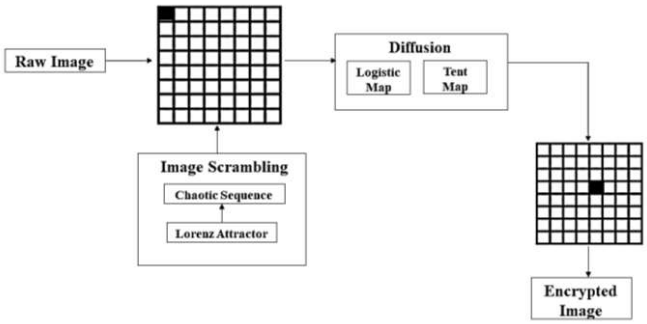

Fig. 1. Block diagram for encryption process.

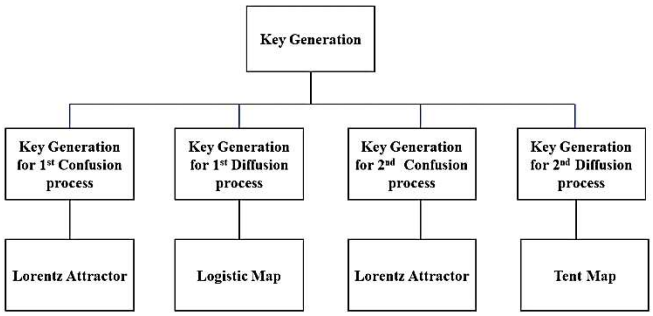

Fig. 2. Key Generation

IV. Proposed Solution

A. Confusion

The pixel shuffling image encryption method moves each pixel of the original image to a different position in order to make an intermediate encrypted image. It ensures that the final image is unpredictable and hard to decode, which makes it resistant to attempts to discover the original image.

1. Lorenz attractor

Lorenz attractor, a chaotic system, generates seemingly random yet deterministic sequences. The Lorenz attractor is unpredictable and makes it hard to figure out the encryption keystream and it is utilized in image encryption. It also guarantees unpredictability by jumbling the positions and values of pixels. The butterfly effect is a real-world application of the Lorenz attractor. The strong bifurcation of the Lorenz system makes it a preferable choice for key generation.

$$\frac{dX}{dt} = \sigma(Y - X) \tag{2}$$

$$\frac{dY}{dt} = -XZ - Y + rX \tag{3}$$

$$\frac{dZ}{dt} = -bZ + XY \tag{4}$$

Where 'X', 'Y', 'Z' are the state variables representing the system's dynamic behavior. 't' is the independent variable, usually representing time. 'σ', 'r', 'b' are parameters that influence the behavior of the system.

B. Diffusion

Diffusion is a crucial step in image encryption that aims to disperse the statistical redundancy present in the original image. Diffusion is the process of substituting new pixel value using the old pixel value and any reversible operation. In the encryption process, the diffusion operation and the scrambling operation are interleaved. Pixel value scrambling is a technique used to change the pixel values of the original image into an intermediate encrypted image. This process involves performing a bitwise XOR operation on each pixel with another set of values, which are typically generated using a secret key. By scrambling the values of pixels using this method, the resultant encrypted image becomes highly randomized and difficult to decipher without the correct decryption key. When the process of confusion followed by diffusion are done to encrypt an image, it increases the rigidity and makes the encryption system stronger.

1) Logistic maps: Logistic maps generate pseudorandom sequences of numbers which are used to modify pixel values and shuffle pixel positions. Logistic maps are used to perform the diffusion process in image encryption. It is very simple chaotic map that has been studied for its cryptographic applications. It is a non-linear quadratic equation that shows chaotic behavior. It expressed as:

$$x_{n+1} = \alpha x_n(1 - x_n) \tag{5}$$

2) Tent maps: The Tent map is also a chaotic map which is frequently utilized for generating truly random numbers, and it exhibits random behavior as the value of μ approaches its upper limit of 2. For every value in the range, $0 \leq \mu \leq 2$, random values are given as output which are within the range $0 \leq x \leq 1$. It is expressed as

$$x_{n+1} = \mu x_n, x_n < 0.5 \tag{6}$$

$$\mu(1 - x_n), x_n > 0.5 \tag{7}$$

C. Differential Attack Analysis

UACI and NPCR are metrics used to evaluate the resistance of an image encryption algorithm against differential attacks. They assess the algorithm's ability to disrupt the relationship between changes made to the plain image and the corresponding changes in the encrypted image. UACI and NPCR provide valuable insights on the potential effectiveness of varied attacks on an image encryption algorithm.

1) Unified Average Changing Intensity (UACI): UACI value is used to assess how well the image has been encrypted and for the purpose of differential attack analysis. It assesses the average strength of the variations between the encrypted ciphered image and the original plain image. The ideal value of UACI is considered to be 33.4%, which implies that the average intensity of the changes between the plain and obfuscated image is at an optimal level. UACI assesses the security of encryption algorithms for digital images by quantifying how effectively the algorithm transforms a plain image into an encrypted version.

$$\text{UACI} = \left[\sum_{x=1}^{M}\sum_{y=1}^{N}\frac{|s_1(x,y) - s_2(x,y)|}{255}\right] \times \frac{100\%}{M \times N} \tag{8}$$

Where M x N denotes the image resolution. S1, S2 denotes the two images and x, y denotes the pixel positions.

2) Number of Pixel Change Rate (NPCR): In order to assess how well an encryption technique diffuses the pixel values in an image, NPCR calculates the percentage of pixels that differ between two cipher-encrypted images. An NPCR score that is above 99.60% and near to 100% means that the encryption method disseminated the pixel values successfully and that even little changes to the input image or key will have a big influence on the encrypted image. Low NPCR values suggest that the two encrypted images are correlated, which jeopardizes the algorithm's security.

$$\text{NPCR} = \sum_{x=1}^{M}\sum_{y=1}^{N} BM(x,y) \times \frac{100\%}{M \times N} \tag{9}$$

Where M and N are the dimensions of the image and x, y denotes the pixel positions.

V. Experimental Results and Performance Analysis

The proposed system has been executed in a 64-bit operating system, x64-based processor, 13th Gen Intel(R) Core (TM) with 16 GB installed RAM using MATLAB. The experimental results generated are shown in the Fig. 3.

a) Plain image b) Encrypted image

Fig. 3. a) Plain images of Lena, Cameraman, Van of size 512 X 512 and b) corresponding encrypted images

A. *Histogram Analysis*

In image processing and data visualization, histogram analysis is a method used to examine the distribution of pixel values or intensities inside an image as shown in Fig. 4.1 and Fig. 4.2. The flat histogram profile of the Lena image obtained here indicates that the information present in the image is sealed. There is no dominant intensity level which makes it difficult to extract data from the image.

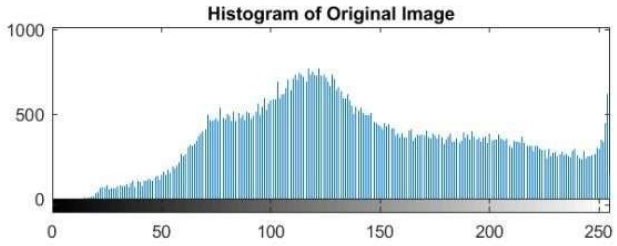

Fig. 4. Histogram of original image

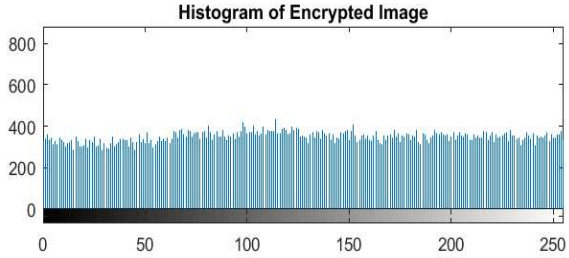

Fig. 5. Histogram after encryption

B. *Auto Pixel Correlation*

Auto pixel correlation refers to a technique used in image processing and computer vision to measure the similarity between two images or between different parts of the same image as shown in Fig. 5.1. and Fig. 5.2.

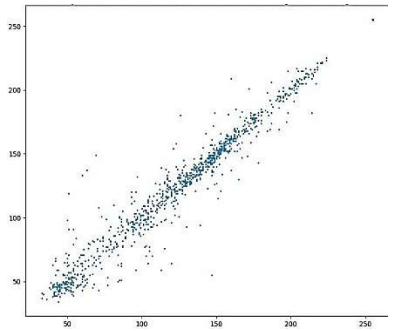

Fig. 6. Auto pixel correlation of original image

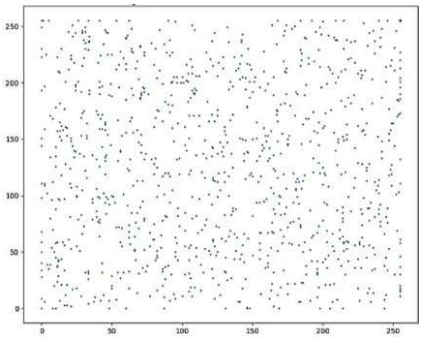

Fig. 7. Auto pixel correlation of encrypted image

It is evident from the encrypted image's dispersed distribution that there is little correlation between nearby pixels.

C. *Entropy*

Shannon's entropy provides the amount of uncertainty and randomness present in the pixel values of the encrypted image. It tells about the effectiveness of encryption. The Shannon's entropy is defined as:

$$S = -\sum(p(h) * \log(p(h)) \quad (10)$$

where p(h) is the probability of pixels of value 'h'. The image is first converted into a grayscale image and then the formula is applied to calculate the entropy.

TABLE I. ENTROPY MEASURE

IMAGE	PLAIN IMAGE	CIPHERED IMAGE
Lena	7.629	7.958
Cameraman	7.009	7.956
Barbara	7.134	7.941
Real-time image	7.235	7.859

D. UACI and NPCR Values

Based on the obtained NPCR and UACI values from table 2, it can be said that the proposed algorithm has efficiently encrypted the image. The high NPCR value obtained here indicates that small changes made to the original image lead to big changes in the encrypted image. This makes the encryption scheme resistant to differential attacks, where attackers try to exploit slight modifications in the original image to gain information about the key or data. Similarly, the high UACI value result signifies a large difference in intensity between corresponding pixels in the original and encrypted images. This implies that the encryption process effectively hides the original content, making it difficult for unauthorized users to decipher the information. In essence, high NPCR and UACI contribute to robust image encryption by ensuring sensitivity to minor changes and significant alteration of the original image data, thereby enhancing security against various attacks.

TABLE I. UACI and NPCR values

Image	UACI value	NPCR value
Cameraman	33.127	99.61
Lena	33.137	99.62
Barbara	33.156	99.61
Real-time image	33.135	99.62

VI. Conclusion

The image encryption algorithm proposed in this study is implemented using the Python modules CV2, matplotlib, numpy, chaotic_maps and has provided results that demonstrated its effectiveness in ensuring security compared to the existing methods of image encryption. This algorithm has a time complexity of O(M x N). Based on the obtained results, through thorough analysis, it was determined that this method could be used for securing and privacy protection of public big data of WISN. The algorithm leveraged the concept of hybrid chaotic maps in an effective way. Based on the obtained results, it can be concluded that the ideal UACI value of an encrypted image is ≈ 33.1%, NPCR value is ≈ 99.6% and that of Shannon entropy is ≈ 7.95. Furthermore, the research highlighted the advantage of employing multiple stages of confusion and diffusion over a singular stage process for encrypting images. The findings of this research work suggest that the proposed algorithm offers enhanced security by integrating multiple encryption stages.

References

[1] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 2nd ed., Prentice Hall, 2002.

[2] M.Brindha, "Multiple stage image encryption using chaotic logistic Map", 2017 IEEE, International Conference on Intelligent Sustainable Systems (ICISS 2017). ISBN:978-1-5386-1959-9

[3] M.-Y. Huang, Y. Huang, and M.-S. Wang, "Image encryption algorithm based on chaotic maps," Dec. 01, 2010.

[4] A. A. Alarood, E. Alsolami, M. A. Al-Khasawneh, N. Ababneh, and W. Elmedany, "IES: Hyper-chaotic plain image encryption scheme using improved shuffled confusion-diffusion," Ain Shams Engineering Journal/Ain Shams Engineering Journal, vol. 13, no. 3, pp. 101583, May 2022.

[5] G. Suseela, Y. A. V. Phamila, G. Niranjana, K. Ramana, S. Singh, and B. Yoon, "Low energy interleaved chaotic secure image coding scheme for visual sensor networks using Pascal's Triangle Transform," IEEE Access, vol. 9, pp. 134576–134592, Jan. 2021.

[6] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," Optics Communications, vol. 284, no. 19, pp. 4331–4339, Sep. 2011.

[7] J. S. Muthu and P. Murali, "Review of chaos detection techniques performed on chaotic maps and systems in image encryption," SN Computer Science/SN Computer Science, vol. 2, no. 5, Jul. 2021.

[8] A. Soleymani, Z. Ali, and J. Nordin, "A survey on principal aspects of secure image transmission," World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 6, no. 6, pp. 780–787, Jun. 2012.

[9] P. P. Dang and P. M. Chau, "Implementation IDEA algorithm for image encryption," in Mathematics and Applications of Data/Image Coding, Compression, and Encryption III, vol. 4122 of Proceedings of SPIE, pp. 1–9, August 2000.

[10] C. Li, G. Luo, and K. Qin, "An image encryption scheme based on chaotic tent map," Nonlinear Dynamics, vol. 87, no. 1, pp. 127–133, Aug. 2016.

[11] Z. Gao, Z. Liu, and L. Wang, "An image encryption algorithm based on the improved Sine-Tent map," Discrete Dynamics in Nature and Society, vol. 2021, pp. 1–16, Oct. 2021,

[12] Z. Su, S. Lian, G. Zhang, and J. Jiang, "Chaos-Based video encryption algorithms," in Studies in computational intelligence, pp. 205–226, 2011.

[13] K. Cellk and E. Kurt, "A new image encryption algorithm based on lorenz system," in 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2016.

[14] S. S. Askar, A. A. Karawia, Abdulrahman 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, pp. 44, Jan. 2019

[15] C. Zou, Q. Zhang, X. Wei, and C. Liu, "Image encryption based on improved Lorenz system," IEEE Access, vol. 8, pp. 75728–75740, 2020.

[16] C Jeyamala, S GopiGanesh, and G. S. Raman, "An image encryption scheme based on one time pads — A chaotic approach," Jul. 2010

[17] Hoshang Kolivand, Sabah Fadhel Hamood, Shiva Asadianfam, and Mohd Shafry Rahim, "Image encryption techniques: A comprehensive review," Multimedia Tools and Applications, Jan. 2024

[18] Fatih Özkaynak, "Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals," 2017 International Conference on Computer Science and Engineering (UBMK), Oct. 2017.

[19] Y. Wu, "Image encryption using the two-dimensional Logistic Chaotic Map," Journal of Electronic Imaging, vol. 21, no. 1, pp. 013014, Mar. 2012,

[20] P. Khade and M. Narnaware, "Practical Approaches for Image Encryption/Scrambling using 3D Arnolds Cat Map," in Springer eBooks, pp. 398–404, 2012.

[21] A. Soleymani, J. Nordin, and E. A. Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map," vol. 2014, pp. 1–21, Aug. 2014