Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

An approach for encrypting images using a four-dimensional logistic map

Baydaa Jaffer Al-Khafaji[1]*, Abdul Monem S. Rahma[2]

[1]Iraqi Commission for Computers and Informatics, Informatics institute for postgraduate studies, IRAQ

[1]Computer Science Department College of Education for Pure Science/ Ibn Al-Haitham University of Baghdad, IRAQ

[2] Computer Science Department, Al-Maarif University College, IRAQ

*Corresponding Author: Baydaa Jaffer Al-Khafaji

DOI: https://doi.org/ 10.31185/wjps.343
Received 02 March 2024; Accepted 07 April 2024; Available online 30 Jun 2024

ABSTRACT: Encrypting image transmission has been one of the most complex challenges with communication technology ever. Millions of people utilize and share photographs via the internet for personal and professional purposes. One approach to secure picture transfer over the network is to use encryption techniques to transform the original picture into an unreadable or garbled version. Several novel and encouraging possibilities for creating secure Image data encryption techniques are presented by cryptographic algorithms grounded in chaotic logistic theory. Developing a foolproof method for encrypting both black-and-white and color image is the primary focus of this work. Both grayscale and color images can be encrypted using the keys generated by combining the chaotic logistic with the image's density in the first stage of the proposed system's encryption process. The original image can then be recovered in the second stage, which is the inverse of the encryption process. Two publicly available standard grayscale and color photographs were analyzed to evaluate the suggested approach. Peak signal-to-noise ratio (PSNR), unified average changing intensity (UACI), and number of pixels change rate (NPCR) were found to be 6.6268, 51.3011, and 100, respectively, according to the test findings.

Keywords: AES, chaotic maps, chaotic flows, PSNR, NPCR, UACI

1. INTRODUCTION

Modern technology has made it possible to transmit large amounts of data, images, documents, audio, and video in a matter of seconds. End user data may be at danger due to the information's transmission across a single frequency band [1], [2] Information interchange, authorization, Google Maps, satellite, healthcare, and military applications are just a few of the many businesses that rely on images. Keeping these images safe from prying eyes is the next biggest obstacle. Data encryption is one method to prevent hacking. Cryptography is a way to secure data transmissions by encoding them in a way that only the intended recipient can decipher .We guarantee your privacy, authenticity, integrity, and the absence of any form of denial of service [3], [4]. There is a difference between picture encryption and text encryption [5]. Multimedia files are not well-suited for traditional encryption techniques like AES because of their large data capacity, high redundancy, and substantial pixel correlation [7], [8]. Edward Lorenz made history in 1963 when he applied chaos theory to an algorithm on a computer [6]. Many people have been interested in chaotic-based cryptography in the past ten years because to the unauthorized person's noise-like signal, ergodicity, mixing, and sensitivity to the initial conditions. Similarities between these features and those of top-notch ciphers, like confusion and diffusion, have been suggested [9], [10]. Researchers in the area of information security have offered a plethora of photo encryption methods based on chaotic algorithms The Logistic map is one of several chaotic map-based picture encryption algorithms . Attacks using crypto analysis have a much lower efficacy on chaotic functions with more dimensions [11], [12]. To meet the increasing need for efficient and safe picture encryption algorithms, lightweight image encryption approaches have recently arisen as a potential solution. Mobile phones, tablets, and

embedded algorithms are examples of devices with limited resources, therefore lightweight image encryption methods are ideal because of their simple implementation, low memory utilization, and low computational complexity. While encrypting digital images, these methods usually use a mix of chaotic maps, Feistel ciphers, XOR-based encryption, linear transformations, and substitution and permutation operations [13],[14]. Lightweight image encryption methods have various uses, but they've also encountered security issues, most notably attack vulnerabilities. Due to this, studies should be conducted to create efficient and simple picture encryption methods that are also light weight and off extra protection [15][16]. High throughput, or the ability to handle massive volumes of data quickly, is just as important as the security requirements when it comes to picture encryption methods. Parallel processing is a tempting option to increase the throughput of picture encryption since it is available on most computer platforms with parallel processing capabilities [17]. But these kinds of hardware capabilities aren't typically considered while developing picture encryption techniques. Chaotic sequences, typically described by progressively computed recurrence relations, constitute the backbone of most picture encryption systems.

2. CHAOTIC ALGORITHMS

Discrete Algorithms Even though chaotic patterns are formed by deterministic algorithms, they often appear random and unpredictable There are several algorithms that exhibit this behavior, including physiological and pathological ones. Some of the many uses for chaotic algorithms include chaotic-based computation and communication [20]. These uses stem from chaotic algorithms' distinctive characteristics, such as their sensitivity to starting conditions and parameters. Some deterministic nonlinear dynamic algorithms produce behavior that looks like randomness; these algorithms are called chaotic algorithms. Different parameter values might cause the algorithm to produce oscillation periods at its output that are independent of the beginning conditions and parameters. Consequently, the outputs of these algorithms are very conditional. For digital data encryption, chaotic algorithms are advantageous due to their inherent randomness and repeatability among close iterations [18]. Most chaotic algorithms fall into one of two categories: chaotic flows or chaotic maps:

-chaotic flows: Continuous dynamic algorithms exhibiting chaotic behavior are known as chaotic flows.
- chaotic maps: Discrete algorithms that display chaotic behavior are known as chaotic maps.

3. RELATED WORK

- The work of A. M. Abbas and colleagues in 2021 [19]. Using pixel-level parallelization, the suggested method for encrypting chaotic images accelerates the production of chaotic sequencing. This approach to developing an image encryption method entails making use of the addition operator and a group built over points of an elliptic curve (EC) to generate a discrete chaotic sequence. By making encryption and decryption methods extremely parallelizable, the design takes advantage of parallel processing platforms including GPU acceleration, multi-core CPUs, and DSPs. The suggested technique outperforms state-of-the-art EC-based picture encryption schemes, according to complexity analysis. Data processing speed can be increased by 3.93 times on a quad-core CPU according to real-world experiments.

- The work of P. P. Values and colleagues in 2021 [20]. Presented a method for plain-image encryption that uses the input image's pixel intensities to adjust the logistic map's variable values. By changing the parameter values row by row, the same encryption and decryption approach can be employed. The logistic map's history, including its fixing points and periodic cycles, is considered in the proposed variable modification technique. A positive Lyapunov exponent indicates that the logistic map is chaotic, and the subsequent interval of changing values supports this theory. In terms of UACI and NPCR, the experimental results reveal that the proposed method achieves the maximum values of 33.4857% and 99.6143 percent, respectively.

- [21] J. Ferdush et al. (2021). Put forward an approach to lightweight picture encryption that makes use of a common framework and an algorithm that is based on two chaotic maps, namely Arnold and Logistic. The procedure entails finding the optimal starting point for the logistic map by first establishing initial values for all variables and then applying an optimization technique. The optimal chaotic control variable, r, is subsequently chosen at random from the interval (0–4) using a genetic algorithm. Afterwards, the picture is made secure. While UACI and NPCR achieved the greatest values of 26.51% and 99.54%, respectively, the approach attained an Entropy value of 7.9762 and a PSNR value of 9.808. The time it took to encrypt the image was 8.8939 seconds.

- As stated in [22] by Yousef Alghamdi, Arslan Munir, and Jawad Ahmad in 2022. Introduces an efficient, secure, and lightweight method for encrypting images using logistic maps, permutations, and the Advanced Encryption Standard (AES) S-box. The suggested method uses SHA-2 to create the logistic map's starting parameters from the

plaintext image, pre-shared key, and IV. For the purposes of permutations and replacements, the logistic map generates irrational numbers. PSNR stands at 8.7880, while UACI and NPCR both reach 99.6368 percent and 33.5531 percent, respectively, at their peak. It takes 0.1056 seconds to encrypt image.

4. PROPOSED SYSTEM

The primary goal of this process is to safeguard images by implementing a novel encryption method that relies on density and a 4D chaotic logistics map. In order to circumvent the logistic insecurity weakness, a new 4D logistics map is constructed using an image's density value. Then, the image is encrypted using both the generated map and a master encryption key. The following are the steps of the proposed system, as depicted in Figure 1:

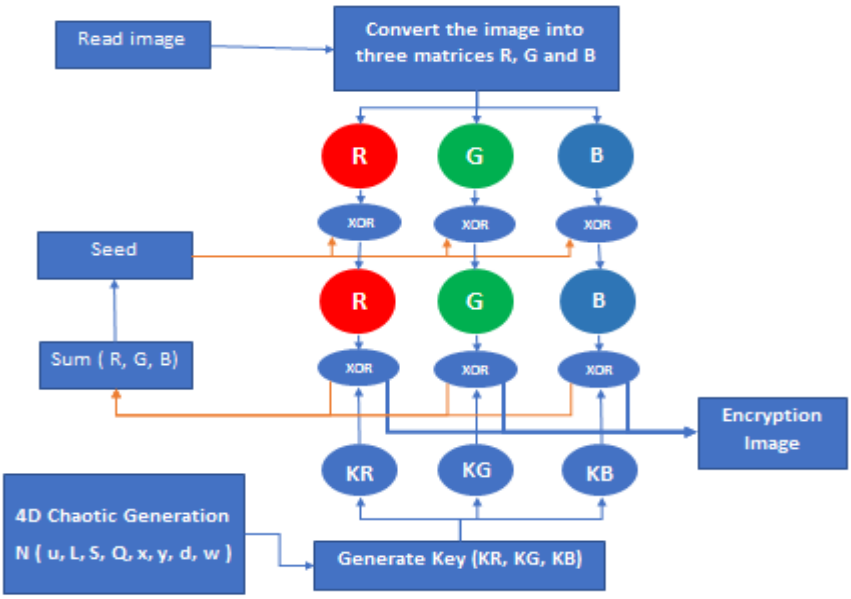

Figure 1. A block diagram of the proposed method

Encryption algorithm

INPUT: image, Initial (u, L, S, Q, x, y, d, w), Seed

OUTPUT: image encryption

Begin:
Step 1: Convert the image into three matrices
R, G, B = read(image)
Step 2: Generate Logistics Chaos Keys
Logistic4D = Generate (u, L, S, Q, x, y, d, w)
*KR[i] = (x[i]*1000000 + (y[i] * w[i]) * 1000000) %256*
*KG[i] = (y[i]*1000000 + (d[i] * w[i]) * 1000000) %256*
*KB[i] = (d[i]*1000000 + (x[i] * w[i]) * 1000000) %256*
Step 3: Encryption Using XOR Operation
For all x, y Do {where 0 ≤ x ≤ Size, 0 ≤ y ≤ Size}
R[x][y] = (R[x][y] XOR Seed) XOR KR
G[x][y] = (G[x][y] XOR Seed) XOR KG
B[x][y] = (B[x][y] XOR Seed) XOR KB
Seed = R[x][y] + G[x][y] + B[x][y]
End For// Size, Size

5. IMPLEMENTATION AND RESULT

Without relying on the plaintext or encryption key, an image encryption system should be impenetrable to all known types of attacks. To ensure consistent use of the encryption key, an appropriate picture encryption technique should be capable of converting any image from plain text to ciphertext using random generation. Using a for-dimensional logistics map and security analysis, the proposed method of photo encryption is tested in this section. Figures 2 display the encrypted data

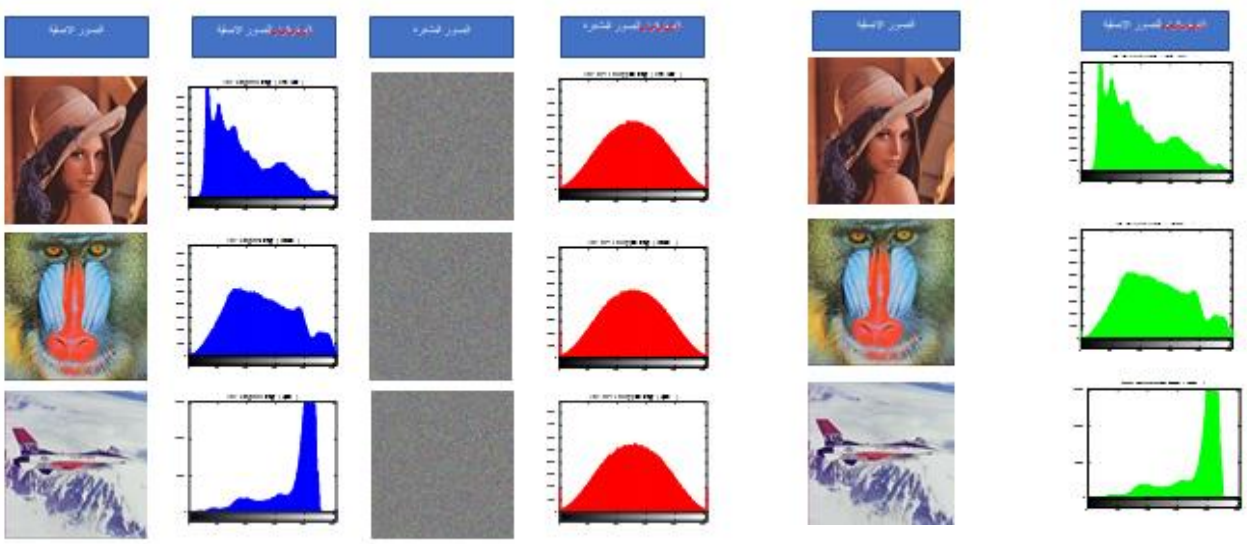

Figure 2. the implementation of algorithm

The MSE and PSNR values of the original and encoded images are displayed in Table 1.
While a lower PSNR number suggests greater encryption quality, a higher MSE value indicates better encryption results. The decrypted stage's MSE and PSNR values are 0, respectively.

1- MSE and PSNR analysis

Table 1

Image Name	Encrypt		Decrypt	
	MSE	PSNR	MSE	PSNR
Lena	28220.714	3.625	0	∞
Baboon	25708.321	4.030	0	∞
Airplane	31074.851	3.206	0	∞

6. CONCLUSION

Much work has already been done on this subject in prior works on chaotic logistic 3D. In contrast, this research details a secure and efficient way to create keys and encrypted images using the XOR operation, utilizing chaotic logistic 4D with picture density. We have tested the suggested approach on a wide range of image kinds and sizes. Based on the testing data, the optimal values for PSNR, UACI, and NPCR are seventy-seven thousand, fifty-one thousand, and one hundred, respectively. Based on the testing findings, we can conclude that our algorithm is quite secure and can successfully resist a range of attacks. These results demonstrate that our method can hold its own against other methods of chaos-based image encryption that have been developed in the past.

7. REFERENCES

[1] W. A. Shukur, A. Badrulddin, and M. K. Nsaif, "A proposed encryption technique of different texts using circular link lists," Periodicals of Engineering and Natural Sciences, vol. 9, pp. 1115-1123, 2021

[2] FA Abdullatif, WA Shukur Blind Color Image Steganography in Spatial Domain - Ibn AL-Haitham Journal For Pure and Applied Science 2011,24(1),338-346cy44

[3] Baydaa Jaffer Al-Khafaji, Abdul Monem S Rahma. Proposed new modification of AES algorithm for data security, Global Journal of Engineering and Technology Advances, (2023) *Vol. 3, No. 12, pp* 117–122

[4] B.J AlKhafaji, M Salih, S Shnain, Z Nabat,segmenting video frame images using genetic algorithms,2020 Periodicals of Engineering and Natural Sciences 8 (2), 1106-1114.

[5] M. Francois and D. Defour, "A pseudo-random bit generator using three chaotic logistic maps," *HAL Sci. Ouvert.*, pp. 1–22, 2013.

[6] S. Lian, "A block cipher based on chaotic neural networks," *Neurocomputing*, vol. 72, pp. 1296–1301, 2009, doi: 10.1016/j.neucom.2008.11.005.

[7] W. H. Abdulsalam, R. S. Alhamdani, and M. N. Abdullah, "Speech Emotion Recognition Using Minimum Extracted Features," 1st Annual International Conference on Information and Sciences (AiCIS), pp. 58-61, 2018.

[8] Y. Dong, X. Huang, Q. Mei, and Y. Gan, "Self-adaptive image encryption algorithm based on quantum logistic map," *Secur. Commun. Networks*, vol. 2021, pp. 1–12, Jan. 2021, doi: 10.1155/2021/6674948.

[9] B.J AlKhafaji, MA Salih, SAH Shnain, OA Rashid, AA Rashid, MT Hussein,2021, Applying the Artificial Neural Networks with Multiwavelet Transform on Phoneme recognition, Journal of Physics: Conference Series 1804 (1), 012040.

[10] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 6, pp. 1341-1352, 2006.

[11] May A. Salih, Shaymaa AbdulHussein Shnain , Baydaa Jaffer AlKhafaji, Using RC6 in embedding information in spatial parts of image construction, Turkish Journal of Computer and Mathematics Education,2021,12,(11).

[12] Arabic and English Texts Encryption Using Proposed Method Based on Coordinates System.WA Shukur, ZMJ Kubba International Journal of Advances in Soft Computing & Its Applications 2023, 15 (2),

[13] S. SH. Hussein, S. SH. Altyar, L. A. Tawfeeq, and E. S. Harba, Reconstruction of Three-Dimensional Objects from Two-Dimensional Images by Utilizing Distance Regularized Level Algorithm and Mesh Object Generation, Baghdad Science Journal, 2020, *17(3):*899–908, 2020.

[14] Bushra Kh AlSaidi, Baydaa Jaffer Al-Khafaji, Suad Abed Al Wahab, Content Based Image clustering Technique Using Statistical Features and Genetic Algorithm. Engineering, Technology & Applied Science Research 2019,9(2).

[15] Iptehaj Alhakam, Nassir H Salman, An Improved Probability Density Function (PDF) for Face Skin Detection, *Iraqi Journal of Science,* 2022,*Vol. 63, No. 10, pp: 4460-4473*, DOI: 10.24996/ijs..63.10.31

[16] H. S. Harba,E.S. Harba, S. SH. Hussein, and M. K. Farttoos, "Improving accuracy of CADx system by hybrid PCA and backpropagation", IEEEXplore,2018.

[17] B.J AlKhafaji, M Salih, S Shnain, Z Nabat, improved technique for hiding data in a colored and a monochrome image, Periodicals of Engineering and Natural Sciences, 2020, 8 (2), 1000-1010

[18] Prof. Abdul Monem S. RahmaPh.D Baydaa Jaffer Al-Khafaji, Optimizing Symmetric vs. Asymmetric Image encryption mathematically, International Journal of Advances in Engineering and Management (IJAEM) ,2022,4(9).

[19] D. Roohbakhsh and M. Yaghoobi, "Color Image Encryption using Hyper Chaos Chen," International Journal of Computer Applications, vol. 110, pp. 9-12, 2015.

[20] N. Ramadan, H. E. H. Ahmed, S. E. Elkhamy and F. E. Abd El-Samie, "Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map," *American Journal of Signal Processing*, vol. 6, pp. 1-13, 2016.

[21] A. K. A. Hassan, "Proposed Hyperchaotic System for Image Encryption," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, pp. 37-40, 2016.

[22] Y. Alghamdi, A. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, pp. 1–25, 2022, doi: 10.3390/e24101344.