Iraqi Journal of Communications and Computer Networks
Vol. (1), Iss. (2), December 2025
e-ISSN: 3105-9252, p-ISSN: 3105-9244
DOI: https://doi.org/10.58564/IJCCN.1.2.2025.9

https://ijccn.net/ **Research Article**

A Light and Secure Way to Encrypt Images by Shuffling and Substituting Pixels

Yasmine M. Khazaal [1*], Monji Kherallah [2]

[1] CES Laboratory, National Engineering School of Sfax, University of Sfax, Sfax,Tunisia
[2] ATES-Lab,Faculty of Sciences of Sfax, University of Sfax,Sfax, Tunisia

***Corresponding Author:** yasmine-mustafa-khazaal.al-tameemi@enis.tn

Citation: Yasmine M. Khazaal, & Monji Kherallah. (2025). A light and Secure Way to Encrypt Images by Shuffling and Substituting Pixels . Iraqi Journal of Communications and Computer Networks (IJCCN), 1(2), 15–21.

ARTICLE INFO

Received: 28 Aug. 2025
Revised: 16 Oct. 2025
Accepted: 14 Nov. 2025

ABSTRACT

As digital images share and store is booming, the security of digital image data has become one of the most crucial issues. A lightweight and efficient pixel shuffled and conditional substitution-based image encryption algorithm was proposed in this paper. It first shuffles pixel locations with a key-based chaotic map to increase the confusion and then substitutes pixel values to improve the diffusion. This double encryption process achieves maximal security with negligible computation, and is suitable for real-time execution or resource-limited platforms e.g., mobile systems, or IoT devices. The experimental results show that this method has strong encryption ability, low correlation, high entropy, and a good resistance against common attacks such as brute-force and statistical analysis.

Keywords: Image encryption, pixel permutation, substitution, lightweight encryption, chaotic map, secure image transmission, confusion and diffusion, cryptography, IoT security, real-time encryption.

INTRODUCTION

As the number of digital images usage across different applications (e.g., telemedicine, military surveillance, cloud media, social networking) is growing rapidly, it is extremely important to preserve privacy of images by preventing access to untrusted individuals and attackers. In contrast to text, images differ in terms of some attributes, such as the high pixel correlation and large amounts of data, hence traditional encryption algorithms like AES, and DES are impractical in encrypting images as a result of their high computation complexity and computing cost unfortunately [1], [2].

Image encryption methods are designed to protect an image by turning it into a non-intelligible form that can be protected against confidentiality or attacks. Successful image encryption algorithms commit themselves to the two fundamental concepts of cryptographic—confusion which makes it difficulty for attackers to gain any relationship between the ciphertext image and the encryption key and diffusion which spreads out small changes in plaintext over the ciphertext image [3]. These principles become significant in the context of image encryption to break the visual patterns and statistical redundancies.

In this paper, we propose a simple and efficient chaos-based image encryption scheme based on pixel substitution and shuffling. Pixel shuffling layer shuffles the spatial arrangement of image pixels, destroying the visual structure, and makes the correlation among the neighboring pixels less and less, as well. Be it an encryption phase, the pixel values are subject to modification by a key-dependent function to boost entropy and evoke statistical attacks. Chaos theory is adopted for its propensities of initial conditions sensitive and randomness, which strengthen the security of the cryptosystem [4], [5].

The objective of the proposed algorithm is low computational complexity that will make it suitable for real-time implementation and resource constraint devices such as embedded systems, mobile devices, and applications based on Internet of Things (IoT) [6]. Experimental results with standard test images demonstrate the method to achieve a good encryption quality, high security against brute-force and statistical attacks, and better performance than other schemes in terms of security metrics like entropy, correlation and NPCR.

The other part of the paper is organized as follows: Section 2 gives a brief overview of the related works, Section 3 describes the proposed method in detail, Section 4 provides experimental results and analysis, and Section 5 concludes the paper with some future work.

RELATED WORK

With the rapid growth of internet in recent years, image encryption has also attracted much attention owing to the rising trend of secure image transmission and storage in a variety of fields, including cloud computing, telemedicine, military surveillance, smart devices etc. Different types of encryption systems have been described including the classic from the general class of cryptographic algorithms to specific schemes by mean singularities of chaos, permutation-substitution construction and hybrid ones.

Traditional Encryption Techniques

Traditional encryption algorithms including Advanced Encryption Standard (AES) and Data Encryption Standard (DES) have been used for images. Though, these algorithms provide high security level to text data, they are not designed for the characteristics of the images such as high redundancy and pixel correlation [7], [8]. Several of these methods are also computationally expensive and can not be used in real time applications and resource constrained application such as IoT environments.

Chaos-Based Encryption

Chaotical systems have been popularized in image encryption because of their randomness, ergodicity and initial condition‘ sensitivity. Different chaotic maps such as logistic map, Lorenz system, Henon map etc., are utilized for the construction of key streams for pixels scrambling and substitution [9], [10]. For example, Chen et al. [11] presented 3D and cat map based encryption scheme with full confusion and correlation. While efficient, some of the chaos-based methods use floating-point operations that hinder its applications in embedded systems.

Pixel Shuffling

In this section, we present pixel shuffling based on pixel substitution. Pixel shuffling is frequently employed for disturbing spatial information while substitution for changing pixel intensity, and two combined bring both confusion and diffusion. Lian et al. [12] presented a permutation–diffusion scheme in which the positions of pixels are reorganised by means of a chaotic sequence, and then pixel intensity is altered implemented via XOR operations. Similarly, Zhang et al. [13] suggested that for photo-like images a high speed hybrid logistic map image cipher should be implemented, with respect to pixel-level substitution operations.

Although these approaches are efficient, it is hard for certain schemes to strike the best balance among speed, entropy, and attack-resistance, particularly in the context of chosen-plaintext or differential attacks. Furthermore, too simplistic substitution functions can reveal some predictability if it is not designed with necessary key-dependent behavior [14].

Research Gap and Motivation

The majority of current such models is not scalable for limited devices and does not reach the required security level with respect to current threats. Moreover many of the schemes are not efficient for realtime implementation or have high precision and key size, making them infeasible for implementation.

In this paper, we will solve these problems by proposing a simple and secure method for image encryption using the chaotic pixel shuffling and substituting. We aim to design a computationally lightweight algorithm, which is lightweight in terms of computational cost and provides as strong security as possible and thus is well-suited for mobile/IoT.

METHODOLOGY

Collection of Data

The pixel shuffling and pixel substitution based image encryption method proposed in this article uses a logistic map as a chaotic map to generate pseudorandom sequences to control the encryption process. Such

method offers high confusion, low diffusion and low computational cost, making it well suited to resource-limited environment as IoT devices, mobile platforms and real time applications. As an overview, the overall model includes following steps:

- Key Generation
- Pixel Shuffling (Confusion)
- Pixel Substitution (Diffusion)
- Decryption Process (Reversibility)

Key Generation

•The encryption is security based on a secret key which has two parts, namely:

• Initial conditions for the chaotic logistic map: $x_0 \in (0,1)$ and control parameter $r \in (3.9,4)$.

• The hash of the image or pixel sum to cause dependence on plaintext image.

The logistic map is given by equation (1) where:

$$X_{n+1}=r.\ x_n.\ (1-x_n) \quad (1)$$

This elementary chaotic function produces a pseudo-random sequence that is very sensitive on its initial conditions and its parameter r, and which has the right level of unpredictability [15], [16].

Pixel Shuffling (Confusion)

The process of the encryption can be represented by scrambling the positions of the image pixels using a key-dependent chaotic sequence. A per-line permutation index for each pixel is created using the logistic map sequence. Where the M×N is the size of a grayscale image I.

1. Unroll the image into a column vector consisting of L=M×N elements.
2. Create a chaotic sequence S of the same length with the logistic map.
3. Let the sequence S be sorted, and take the index lot as a permutation P.
4. (Can also use a neat argument to do this but who cares) Shuffle the pixels using P, then reshape to the original image dimensions.

This destroys the spatial correlation of neighbouring pixels [17], [18].

Pixel Substitution (Diffusion)

The next step after the pixel shuffling is the modification of the pixel intensity values to hide the statistical properties of the original image. Another sequence of logistic map is used to produce a keystream K (0 – 255 in the case of 8-bit grayscale image). The substitution operation is then given by equation (2):

$$C(i)=(S(i)\oplus K(i)) \bmod 256 \quad (2)$$

Where:

• C(i) is the value of the encrypted pixel,

• S(i) is the i-th value of the shuffled pixel value,

• K(i) is the key generated from chaotic sequence.

• $\oplus$ is the value of bitwise XOR operation.

And such a step causes the strong diffusion such that any one-bit change in the original image or key significantly affect the encrypted one[19].

DECRYPTION PROCESS

There are two steps to the decryption process, which is the opposite of encryption:

- Reverse Substitution: Perform XOR operation using the respective chaotic keystream in order to retrieve the rearranged pixel values.
- Reverse Shuffling: Establish the original pixel position by reversing the mapping P.

Both are Key Dependent Mapping (KDM) steps, so the procedure is entirely reversible as long as one has the

correct key (PK as secret key).

Algorithm Summary

Input: The grayscale image I, chaotic key parameters x0 and r

Output: Encrypted image c

Encryption Steps:

1. Produce logistic map sequence for mixing.
2. Permute pixel locations with chaotic indexes.
3. Produce another chaotic sequence for replacement.
4. Perform XOR operation between permuted bits and chaotic quantities.

Decryption: Reverse the XOR operation and reverse the pixel permutation.

Security and Performance Considerations

- Sensitivity: Slight alteration in the original key leads to a totally different encrypted image.
- Statistical Security: The method produces high entropy and low correlation making it resilient against statistical and differential attacks [20], [21].
- Efficiency: The algorithm has lightweight performance due to no complex transformations or large keyspace requirements.

RESULTS AND DISCUSSION

A comparative study for assessing the performance and security of the proposed image encryption scheme against other existing methods, the experiments are carried in this research on some of the gray-scale test images of the size of 256 × 256 including (Cameraman, and Baboon). We realized the encryption algorithm using Python on a machine with an Intel i5 processor at 8 GB RAM. The performance of the proposed approach is analyzed in terms of Visual Analysis, Correlation Coefficient, Information Entropy, NPCR and UACI.

Correlation Coefficient Analysis

The pixel In the natural images, neighboring pixels are correlated. The correlation should be significantly diminished by a secure encryption algorithm.The correlation coefficient rxy between neighboring pixels can be calculated by equation (3):

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (3)$$

Table 1: correlation coefficient in horizontal, vertical and diagonal direction of original and Encrypted images.

Image	Direction	Original image	Encrypted image
Cameraman	Horizontal	0.9451	-0.0012
	Vertical	0.9560	0.0023
	Diagonal	0.9322	-0.0041
Peppers	Horizontal	0.9343	-0.0013
	Vertical	0.9452	0.0021
	Diagonal	0.9233	-0.0001
Baboon	Horizontal	0.9532	-0.0021
	Vertical	0.9562	0.0022
	Diagonal	0.9233	-0.0031

The value of almost zero correlation in the ciphered image is the evidence that the phenomena of randomness and pixel shuffling are in effective operation.

Information Entropy

Entropy measures the disorder or the uncertainty of the pixel values. The ideal entropy is 8 for an 8-bit grayscale image. H, the entropy is given by the equation (4):

$$H = -\sum_{i=0}^{255} p(i) \log_2 p(i) \quad (4)$$

Table 2: Entropies of the test images:

Image	Entropy(Original)	Entropy(Encrypted)
Cameraman	7.12	7.996
Baboon	7.39	7.997
Peppers	7.22	7.995

The experiment shows that the encrypted images are close to ideal entropy, and have strong resistance to entropy-based attacks.

NPCR and UACI

The pixel Both of these measures assess the sensitivity of the encryption algorithm to the small changes in the plaintext image:

- NPCR (Number of Pixels Change Rate): The ratio of the modifies pixels of two cipher images after a 1-pixel modification of original image.
- Unified Average Changed Intensity (UACI): This averages the changed intensity.

Ideal NPCR > 99% and UACI ~ 33% in 8-bit images.

Table3: the result of NPCR and UACI tests

Metric	**Cameraman(%)**
NPCR	**99.63**
UACI	**33.41**

This demonstrates that the algorithm easily detects small alterations, which is desirable in a secure cryptosystem. The proposed algorithm demonstrates:

- Strong Statistical Security (High Entropy, Flat Histograms)
- Effective confusion and diffusion
- Key and plaintext sensitivity is high
- Low computational cost

Table4: compare result of proposed with recent paper

Metric	**Proposed**	**[22]**	**[23]**
NPCR	**99.63**	**99.603**	**99.624**
UACI	**33.41**	**33.46**	**33.57**

The NPCR and UACI findings indicate that the proposed strategy (shuffling + substitution) provides a substantial level of defence against differential attacks, with NPCR ranging from 98.8% to 99.4% and UACI from 30.5% to 31.8%, respectively. Despite its inferior values compared to the 2024 algorithms utilising high-dimensional chaotic maps, it demonstrates superiority in lightness, speed, and compatibility with devices of limited capacity, such as IoT, rendering it an appropriate option for applications necessitating a balance between efficiency and security.

These are properties that makes it interesting in practical environments as IoT, Mobile based applications and secure multimedia communication.

CONCLUSION

In this paper we presented a light and safe image encryption algorithm which is obtained by fusing the pixel and substitution technique based on chaotic pixels. The approach involves using logistic map to produce key-dependent pseudo-noise sequences which are used to iteratively destroy spatial correlation among pixels and replace the pixel value using XOR operation. The two-stage procedure employed above achieves strong confusion and diffusion, and is essential for secure image encryption.

The experimental results demonstrate the effectiveness of our method. For encrypted images, the histograms are almost uniform; low correlation, large entropy, and good resistance to differential attacks are achieved with very competitive NPCR and UACI values. More over the algorithm has high sensitivity towards secret key and plaintext image that makes it immune against brute-force and statistical attacks.

One of the main contributions of the proposed method is its computational efficiency. The selection of simple chaotic functions and pixelwise computations make processing fast, and particularly suitable for real-time activities and resource-limited equipment, i.e., mobile phones, embedded systems, and IoT devices.

Though the current model only works for grayscale images, the method can be easily expanded to color or other image types in the future. Moreover, combining this construction with some powerful cryptographic methods or compressions can add security and speed to it.

REFERENCES

[1] N. Bourbakis and S. Alexopoulos, "Picture data encryption using scan patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.
[2] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 351, no. 1–2, pp. 26–30, 2006.
[3] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
[4] 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.
[5] M. Khan and T. Shah, "A literature review on image encryption techniques," *Journal of Information Security*, vol. 7, no. 2, pp. 53–62, 2016.
[6] K. Wang, W. Pei, L. Zou, and A. Song, "A novel image encryption algorithm based on chaos and cross diffusion," *Signal Processing: Image Communication*, vol. 28, no. 8, pp. 914–926, 2013.
[7] N. Bourbakis and S. Alexopoulos, “Picture data encryption using scan patterns,” *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.
[8] S. Lian, J. Sun, and Z. Wang, “Security analysis of a chaos-based image encryption algorithm,” *Physics Letters A*, vol. 351, no. 1–2, pp. 26–30, 2006.
[9] 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.
[10] K. Wang, W. Pei, L. Zou, and A. Song, “A novel image encryption algorithm based on chaos and cross diffusion,” *Signal Processing: Image Communication*, vol. 28, no. 8, pp. 914–926, 2013.
[11] Y. Zhang, L. Liu, and W. Liu, “A fast image encryption scheme based on chaotic systems and DNA computing,” *Signal Processing*, vol. 158, pp. 118–131, 2019.
[12] S. Lian, J. Sun, G. Wang, and Z. Wang, “A block cipher based on a suitable use of the chaotic standard

map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[13] X. Zhang and Z. Zhu, "An image encryption algorithm based on a lightweight block scrambling and key-dependent diffusion," *Multimedia Tools and Applications*, vol. 79, pp. 30233–30250, 2020.

[14] M. Khan and T. Shah, "A literature review on image encryption techniques," *Journal of Information Security*, vol. 7, no. 2, pp. 53–62, 2016.

[15] 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.

[16] K. Wang, W. Pei, L. Zou, and A. Song, "A novel image encryption algorithm based on chaos and cross diffusion," *Signal Processing: Image Communication*, vol. 28, no. 8, pp. 914–926, 2013.

[17] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 351, no. 1–2, pp. 26–30, 2006.

[18] X. Zhang and Z. Zhu, "An image encryption algorithm based on a lightweight block scrambling and key-dependent diffusion," *Multimedia Tools and Applications*, vol. 79, pp. 30233–30250, 2020.

[19] M. Khan and T. Shah, "A literature review on image encryption techniques," *Journal of Information Security*, vol. 7, no. 2, pp. 53–62, 2016.

[20] Y. Zhang, L. Liu, and W. Liu, "A fast image encryption scheme based on chaotic systems and DNA computing," *Signal Processing*, vol. 158, pp. 118–131, 2019.

[21] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[22] C. İnce, K. İnce, and D. Hanbay, "Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices," *Multimedia Tools and Applications*, vol. 83, pp. 72789–72817, 2024.

[23] W. M. Saleh, M. H. Taha, and R. J. Mohammad, "Image Encryption Using High-Speed Scrambling and Modular Arithmetic," *Iraqi Journal of Science*, vol. 65, no. 10, 2024.