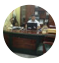
Image Blocks Encrypted then Rotated: A New Pixel-Level Scrambling Method Based Logistic Map for IOT

Conference Paper · September 2022

DOI: 10.1109/IICCIT55816.2022.10010676

Ali K. Mattar
Shatt Al-Arab University College



Raad Muhajjar
University of Basrah

Image Blocks Encrypted then Rotated: A New Pixel-Level Scrambling Method Based Logistic Map for IOT

Ali K. Mattar
Computer Science Dept.
Shatt Al-Arab University College
Basrah, Iraq
alikmattar@sa-uc.edu.iq

Raad A. Muhajjar
College of Computer Science & Information Technology
Basrah, Iraq
raadmuhajjar76@gmail.com

Ali A. Abidali
Computer Science Dept.
Shatt Al-Arab University College
Basrah, Iraq
ali.abdulrazzaq@sa-uc.edu.iq

***Abstract*— recently, grayscale images have been used in many areas such as healthcare or IoT, and securing these images has become important and necessary. Encryption is one of the most reliable and effective ways. Scrambling image contents adds an additional level of image security. This paper proposes a simple new method for scrambling gray images using a Chaotic Logistic Map and pixel-level rotation. In the proposed method, the gray image is encrypted first and then divided into several N×M non-overlapped blocks. The image blocks will be rotated according to the encryption key with angles of 90,180 and 270 degrees. In the same way, the decryption process will reverse the image block's rotation angles first, then retrieve the original image by applying the XORing operation with the same key. The efficiency of the proposed method was evaluated and analyzed by a histogram, Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI), information entropy, Peak Signal to Noise Ratio (PSNR), correlation coefficient, and Adjacent Pixels Correlation Coefficient (APCC). A comparison with other scrambling methods was performed and the results boosted the proposed method.**

Keywords—image encryption, scrambling, pixel-level, rotation, chaotic logistic map.

I. Introduction

The rapid development in information technology has made it possible to adopt it in various fields, such as the transmission of images through various electronic channels. Hence, the issue of securing these images appear as a very important issue to protect the information represented by these images [1,2]. Image encryption is one of the most important ways to secure and ensure their protection from unauthorized persons [3], where the original image is converted into another confused (encrypted) image using a secret key that enables only authorized persons to reverse the encrypted image to its original [4,5]. To reduce the correlations between image pixels to be encrypted- and thus increase the quality of the encryption process- scrambling (permutation) will be used as an important step in the encryption process [6,7]. Image scrambling is a process that allows the pixels of an image to be randomly rearranged. Mathematically, this process breaks the correlations of image pixels, and thus increases their resistance to attacks. From the visual point of view, scrambling distorts the original image. Scrambling has been used extensively with the encryption process [8,9].

There are many types of scrambling, including bit-level scrambling and pixel-level scrambling [10.11]. The pixel-level method is easier to implement because it does not need other additional internal operations such as converting pixels to binary as in the bit-level, but it may suffer from the problem of not scrambling image pixels well (Because it may depend on changing locations of the image pixels only[12], without change the values of it as in bit-level scrambling), so choosing an appropriate and simple way to scramble it as much as possible with good efficiency in results, is an important[13].

By using an image block rotation and a chaotic logic map (to generate the encryption key), this paper proposes a new technique for scrambling images at the pixel level. Our contributions are summarized as follows:

- By using a simple rotation routine without any additional procedures, the proposed method has been designed to be as simple as possible.
- Compared to other scrambling methods, dividing and scrambling the image after encryption increased its resistance against attacking types.

The rest of this paper is organized as follows: Section II presents the previous literature that reviews image scrambling. While section III describes the procedure of the proposed method in detail. Section IV gives an overview of the evaluation measures that are used to assist the proposed method. Simulation results are shown in Section V with evaluation analysis. The conclusions and future works are presented in Section VI, followed by references.

II. Litratures Review

There are a large number of papers focused recently on different methods used to scramble image contents to use it with or without an encryption algorithm. However, since the focus of this paper is on just the papers that used pixel-level scrambling, the paper won't go into details about bit-level scrambling and will only be referred to as needed. The authors in [14] used two chaotic maps, one for scrambling pixel positions of the color/gray images, and the other for the confusing relationship between encrypted and the original image. while Arnold's map algorithm was used in [15] as a scrambling method to change the original image pixels' coordinates to new ones. Subsequently, the authors in [16] used both pixel-level scrambling then bit-level scrambling on the original image beside DNA (coding, XORing process, and complementary rules) for increased performance and security. Also, the same idea of pixel and bit scrambling was utilized in [17], with SCAN (A method to reach all image pixels by different paths) and cyclic shift operations to ensure changing pixels values and positions. To ensure that the encrypted image is sensitive to any pixel change in the original image, pixels values in this article were dependent on three parameters: old pixel value, some key stream element, and an unknown secret value. A chaotic algorithm was introduced in [18] for image encryption that is divided into several sub-images and scrambled in three stages: The first stage is a bit-level scrambling of sub-images to reduce adjacent pixels correlations. In the second stage, the whole image was scrambled randomly at the pixel level. After that whole row-by-row image was used to make the encrypted image more difficult to crack. authors in [19] decided that image encryption techniques have a disadvantage point used by attackers to crack it which. This drawback results from the possibility of similarity between the encrypted image and the original one (in some encrypted images), which leads to the attacker visually perceiving that the image is already encrypted. So they introduced a pixel-level scrambling algorithm depending on chaotic maps to encrypt images to be visually sensed closer to being an original image. they also admit that may be not fully right to the traditional encryption/decryption process. A new scheme was proposed in [20] depending on some random operations to protect medical gray images. The proposed scheme randomly scrambles neighbor image pixels values after insertion of random values to image surroundings, then uses adaptive diffusion spreading this insertion to entire image pixels. The results show high efficiency, speed implementation, and robustness. while in [21] authors propose a new image encryption scheme to also protect medical gray images by merging DNA sequence technique and chaos technique to reinforce image resistance against chosen plain text attack while tinker bell map scrambling image pixels to reduce pixels correlations in the encrypted image. In [22], the authors proposed a new scheme for encryption of medical gray and colored images using the chaotic logistic map. the scheme first divided the original image into blocks and sub-blocks. scrambling each of the original image block/sub-blocks was done by three sub processes: a zigzag pattern, rotation by 90 degrees, and another random image block scrambling at a pixel level to reduce pixels correlations. However, authors in [23] proposed a piecewise linear map cryptosystem. in the encryption step, the whole image is scrambled at pixel-level once, diffused two times, then rotated with 180 degrees four times. While the decryption step, the operations performed in the encryption step will be the same but reversed to ensure that the original image is retrieved from the encrypted one. the proposed cryptosystem resists chosen/known plaintext attacks, and the authors claim that their cryptosystem can be used in actual communications.Those kinds of literature show clearly needing for supporting techniques besides pixel-level scrambling (and sometimes more than one) to produce good results. Regardless of the type of these techniques, this show supports the direction of this paper to reduce techniques associated with scrambling at the pixel level while maintaining good results as possible.

III. PROPOSED METHOD

After explaining some recent literature that is concerned with the pixel-level scrambling of the image, this section will propose a new simple method for pixel-level scrambling with the goal of keeping the results as good as possible by explaining the methodology steps used.

A. *Encryption Step*

The encryption process of the original image will be implemented using an asymmetric algorithm, where the encryption key is the same as the decryption one. The symmetric encryption algorithm is usually better for encrypting large data because of the relatively small key sizes, which means less storage and faster transmission of encrypted data [24].The encryption key used in this study is based on the non-linear simple equation of the Chaotic Logistic Map, which has been widely used in many papers (see Equ.1).

$$x_{n+1} = r\, x_n\, (1 - x_n) \tag{1}$$

where r is the control parameter of the equation that has values in the range [0,4], and the x_n is the initial value in the range (0,1). Equation Equ.1 , is very sensitive for ant small changes in its parameters, and that makes it very suitable for the encryption process for images because of its chaotic attitude and producing non-periodic nor convergent values. Figure Fig.1 , shows the behavior of Equ.1 according to the parameters: r= 3.9159, x_0=0.001, which are used to generate encryption key.

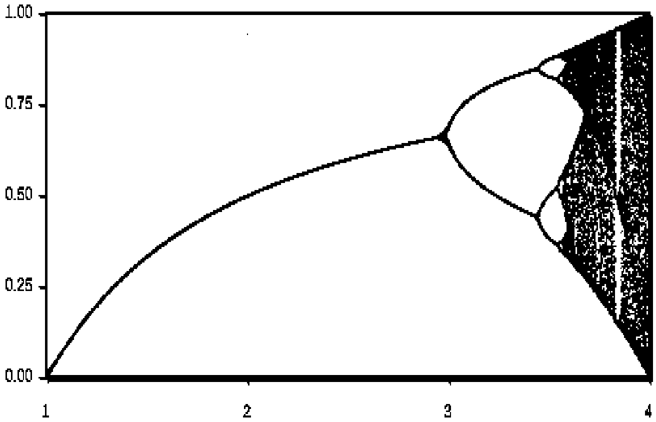


Fig. 1. Beahviour of Chaotic Logistic Map with : r= 3.9159, x_0=0.001.

B. *Blocking Step*

After the image encryption process using the Chaotic Logistic Map, the encrypted image of size N × M will be converted to K blocks (B), where each B = 32×32 pixel, preparation for using it in the rotation step. The size of the block was chosen carefully (not too large or small) to not affect the quality of the results.

C. *Blocks Rotation Counterclockwise Step*

The next step is to find rotation angles to which every encrypted block B from the previous section will be rotated according a spesific scenario. In general, rotation operation is one of the transformation operations that can take place at the 2D level,while Equ.2. can be used to rotate image blocks[25]:

$$R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \tag{2}$$

And the coordinates of any pixel in the image block B can be transferred according to the rotation angle **θ**, as in Equ.3:

$$\begin{aligned} x' &= x\cos\theta - y\sin\theta \\ y' &= x\sin\theta + y\cos\theta \end{aligned} \tag{3}$$

Where, R is the rotation matrix , (x,y) is the original image block's pixel coordinates , (x',y') is the rotated image block's pixel coordinates. To find rotation angle which transfer B in to B', a specific algorithm will be implemented called: Find Angles (see Figure Fig.2), that can be summarized:

- Calculate sum of 0's in encrypted binary key, as well as sum of 1's.
- Convert the greatest sum to binary and get the first two least significant bits LSB.

- According to the binary values of the two LBS, a specific block rotation angles will be chosen. Note that the angles chosen to rotate the blocks differ depending on which of the two sums is greater.
- B block in encrypted image will be rotated counterclockwise at **θ** angle to become B' if the algorithm used after blocking step.

IV. Evaluation measures

To confirm its effectiveness, the proposed method (shown in Fig.3) is evaluated in MATLAB R2017b using a 1.70GHz Intel(R) Core(TM) i5-4210U CPU and 12 GB RAM. This section evaluates the proposed method on several commonly used images of size 512 × 512: Lena, Pepper, and Baboon.

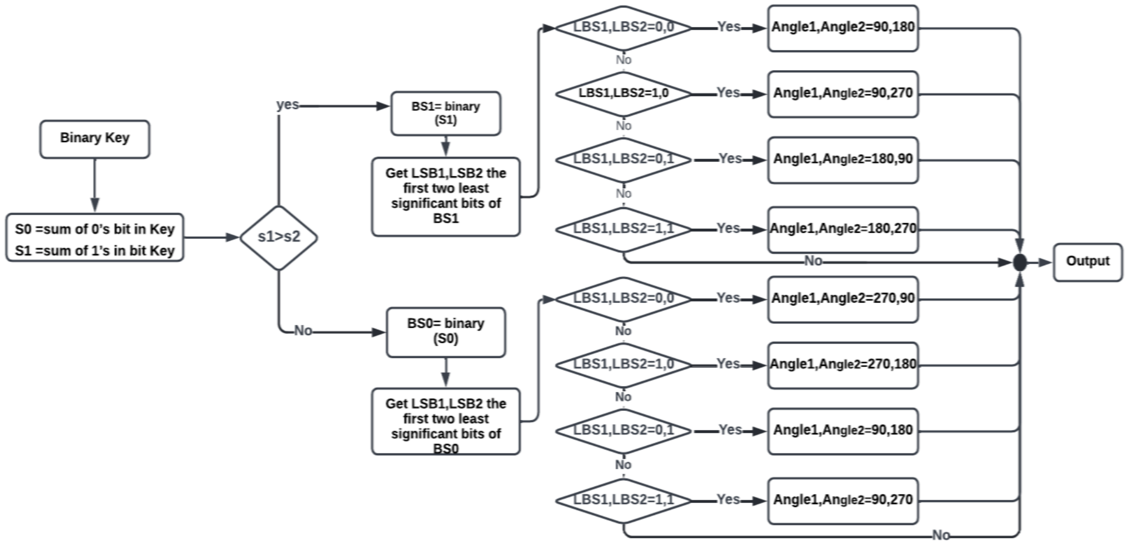


Fig. 2. Algorithem of find rotation angles

- Each B' block in encrypted image will be rotated clockwise at **-θ** angle to become B' if the algorithm used before unblocking step.

This section used rotating image blocks to scramble pixels of an encrypted image at pixel-level, however, rotating image blocks itself doesn't remove image pixels correlations, but when it done after the encryption process and converting the original image into blocks, it will definitely help break it.MATLAB imrotate function was used for rotation operation in this step, where nearest-neighbor interpolation was used to assign every output pixel in the rotated block B', without considering the influences of other pixels in B. However, imrotate function didn't use Acute, Obtuse or Reflex angles such as 30, 45, 130 degrees...etc. because the resulting B' will be larger in size than B and hence the need for more processing. Besides, the interpolation method will put 0 value for each pixel in B' surrounding the original rotated pixels. Visually, this means that the image block contains black pixels that were not originally in B.

D. *Blocks Rotation Clockwise Step*

When encrypted, blocked and rotated image reaching to the destination, Find Angle algorithm will be called again to convert every B' block to B again (reverse blocks rotation) by using clockwise imrotate function (same angles but with negative rotation **θ**).

E. *UnBlocking Step*

In this step, the encrypted and blocked image with K blocks (B), will be converted to its original size N × M again, preparing to the next step.

F. *Decryption Step*

The decryption process of the encrypted image will be implemented using the same key that generated using Chaotic Logistic Map in Equ.1

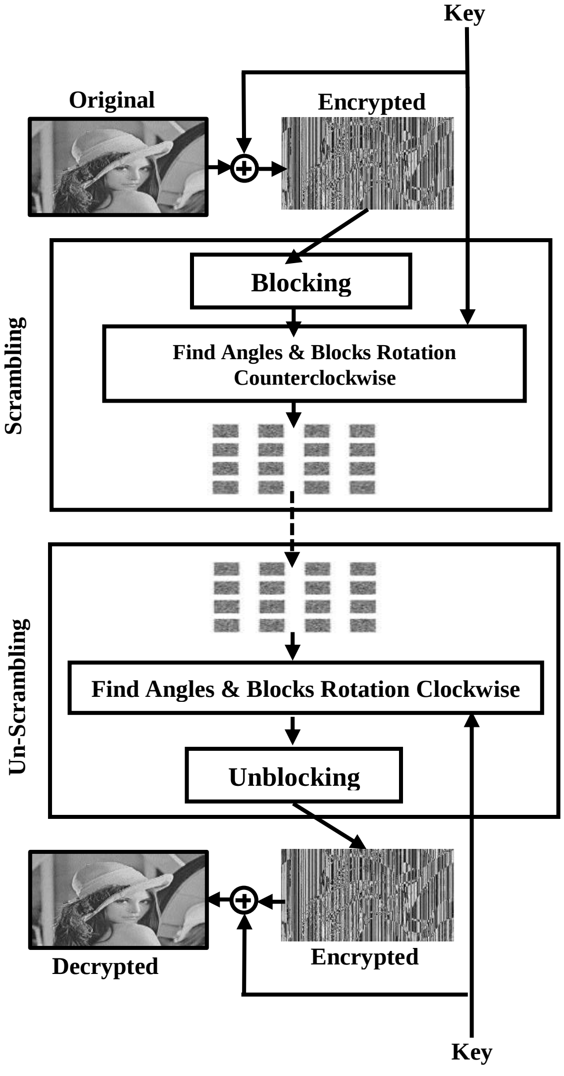

Key
Original
Encrypted
Scrambling
Blocking
Find Angles & Blocks Rotation Counterclockwise
Un-Scrambling
Find Angles & Blocks Rotation Clockwise
Unblocking
Decrypted
Encrypted
Key

Fig. 3. Proposed scrambling method

A. Histogram Analysis

The uniform histogram of the encrypted proposed method for all used images makes it resist statistical attacks because of uniform frequencies compared with the originals, as shown in figure Fig.4.

B. Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI)

NPCR and UACI is usually used in researches to analyze an important type of attack that can take place on the encryption technique called: differential attack. The value of the number of pixel change rate (NPCR) is obtained by encrypting the original image twice: first is done naturally and the second by changing only one pixel in the original image, then obtaining the percentage of the number of different pixels of the two encrypted images. Higher NPCR value, indicates to better resistance against this type of attack. For better value, NPCR should be close to 100. The NPCR equation can be defined as [26]:

$$NPCR = \frac{\sum_{i,j} Def(i,j)}{M \times N} \times 100 \qquad (4)$$

$$Def(i,j) = \begin{cases} 0 & if\ Enc(i,j) = Enc'(i,j) \\ 1 & if\ Enc(i,j) \neq Enc'(i,j) \end{cases} \qquad (5)$$

The UACI is similar to the NPCR, but the main difference is that UACI calculates the value of the actual difference between Enc(i,j) and Enc'(i,j) pixels [27], (see Equ.6).

$$UACI = \frac{\sum_{i,j} Enc(i,j) - Enc'(i,j)}{255 \times M \times N} \times 100 \qquad (6)$$

Resulted value of UACI should be close to 33.4.

C. Information Entropy

Entropy measures the amount of information available in the image contents. The entropy value E(I) of the gray encrypted images (8 bits) is closer to the optimum value of 8 [28] (See Equ.7).

$$E(I) = -\sum_{i=0}^{255} P(pix_i) \times log_2 P(pix_i) \qquad (7)$$

Where P (pix$_i$) is the probability of occurrence of the ith pixel in the image I.

D. Peak Signal to Noise Ratio (PSNR)

PSNR is used to assess the quality of encryption and decryption in the proposed method. The PSNR between the original and decrypted image will be infinite. While it will be low as possible between the original image and the encrypted image. PSNR can be calculated using Equ.8, which will be measured in decibels (dB).

$$PSNR = 10 \times log_{10}\left(\frac{L^2}{MSE}\right) \qquad (8)$$

$$MSE = \frac{1}{M \times N}\sum_{i,j}(\ I_1(i,j) - I_2(i,j)\ )^2 \qquad (9)$$

MSE is the summation squared difference between corresponding pixels of the two images I1 and I2, divided by the size of the image (See Equ.9).

E. Correlation Coefficient (CC)

The correlation coefficient CC between the image pixels before and after encryption can be used to measure the distortion in the original image. It can be calculated using the following equation [29] (See Equ.10).:

$$CC = \frac{\sum_i^m \sum_j^n (A_{i,j} - \bar{A})((B_{i,j} - \bar{B})}{\sqrt{(A_{i,j} - \bar{A})^2 (B_{i,j} - \bar{B})^2}} \qquad (10)$$

Where A and B represent the original and the encrypted image, and their means. The lower correlation coefficient value (closer enough to zero), represents a better-proposed encryption method.

F. Adjacent Pixels Correlation Coefficient (APCC)

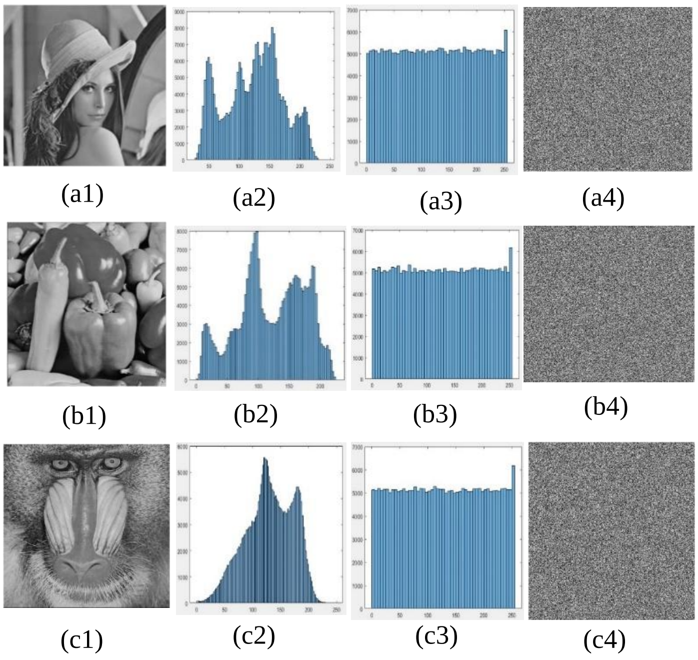
Another way to measure the distortion in the encrypted image after using the proposed encryption method, is the Adjacent Pixels Correlation Coefficient (APCC). This way depends on the fact that any randomly selected and adjacent pixels in the encrypted image in the directions: horizontal, vertical, and diagonal, must be correlated with each other with the lowest possible values (closer enough to zero) to resist statistical attacks. It can be calculated using the following equations [30] (See Equ.11-14).:

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D_x}\sqrt{D_y}} \qquad (11)$$

$$Cov(x,y) = E\big(x - E(x)\big)\ \big(y - E(y)\big) \qquad (12)$$

$$E(x) = \frac{1}{S}\sum_{i=1}^{S} x_i \qquad (13)$$

$$D_x = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2 \qquad (14)$$



(a1) (a2) (a3) (a4)

(b1) (b2) (b3) (b4)

(c1) (c2) (c3) (c4)

Fig. 4. (a1) lena image, (a2) histogram of lena image,(a3) histogram of encrypted lena image,(a4) encrypted lena image. (b1) pepper image, (b2) histogram of pepper image,(b3) histogram of encrypted pepper image,(b4) encrypted pepper image. (c1) baboon image, (c2) histogram of baboon image,(c3) histogram of encrypted baboon image,(c4) encrypted baboon image.

V. RESULTS AND DISCUSSION

Table I bellow shows the evaluation results of the proposed method according to: NPCR, UACI, correlation coefficient (cc),information entropy, and PSNR for all the encrypted images used in the paper.

TABLE I. NPCR ,UACI,INFORMATION ENTROPY AND PSNR OF THE PROPOSED METHOD

Image Name	*NPCR (%)*	*UACI (%)*	*Correlation Coefficient (cc)*	*Entropy*	*PSNR (dB.)*
Lena	99. 6376	28. 6289	0.000076	7.999329	7.015194
Pepper	99. 6117	29. 6761	-0.000729	7.999199	7.285873
Baboon	99. 6265	27. 8633	0.000037	7.999296	6.598897

From Table I above, NPCR,UACI and information entropy values are close to the optimum. While correlation coefficient (cc) is close to zero. Also, the proposed method can produce good lower PSNR values. Any attack on the encrypted image will be considered unsuccessful if the PSNR value is below 15 dB.[31].Table II shows the evaluation results of the proposed method according to: APCC for all the original and encrypted images used in the paper.

TABLE II. APCC IN THREE DIRECTIONS OF THE PROPOSED METHOD

Image Name	*Image State*	*Direction*		
		Diagonal	*Vertical*	*Horizontal*
Lena	Original	0.9593	0.9850	0.9719
	Encrypted	-0.00032	0.003639	-0.0007
Pepper	Original	0.9639	0.9792	0.9768
	Encrypted	0.000782	-0.001	-2.13E-05
Baboon	Original	0.7232	0.7634	0.8749
	Encrypted	0.001487	6.62E-05	0.001663

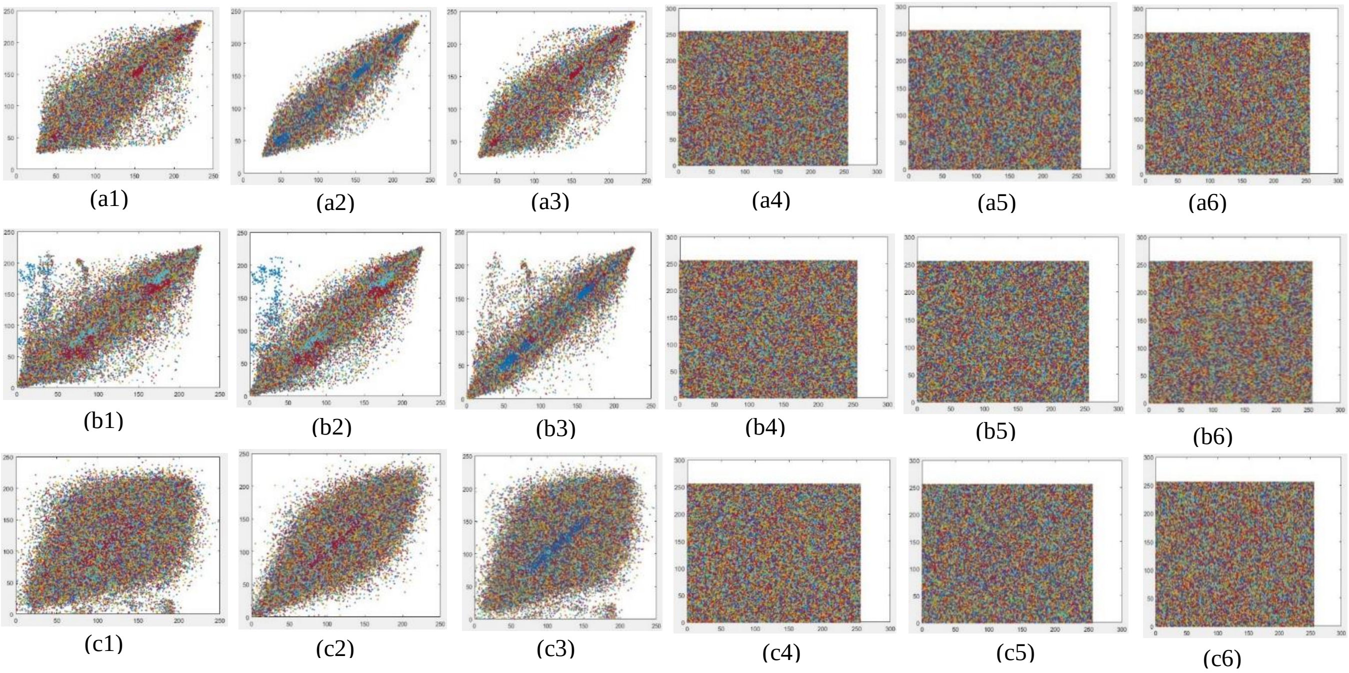

(a1) (a2) (a3) (a4) (a5) (a6)
(b1) (b2) (b3) (b4) (b5) (b6)
(c1) (c2) (c3) (c4) (c5) (c6)

Fig. 5. APCC analysis : (a1) diagonal correlation of original Lena image, (a2) virtical correlation of original Lena image, (a3) horizontal correlation of original Lena image, (a4) diagonal correlation of encrypted Lena image, (a5) virtical correlation of encrypted Lena image, (a6) horizontal correlation of encrypted Lena image,(b1) diagonal correlation of original pepper image, (b2) virtical correlation of original pepper image, (b3) horizontal correlation of original pepper image, (b4) diagonal correlation of encrypted pepper image, (b5) virtical correlation of encrypted pepper image, (b6) horizontal correlation of encrypted pepper image, (c1) diagonal correlation of original baboon image, (c2) virtical correlation of original baboon image, (c3) horizontal correlation of original baboon image, (c4) diagonal correlation of encrypted baboon image, (c5) virtical correlation of encrypted baboon image, (b6) horizontal correlation of encrypted baboon image.

TABLE III. COMPARISION OF THE PROPOSED METHOD WITH OTHER

Image Name	*Ref.*	*Information Entropy*	*NPCR (%)*	*UACI (%)*	*APCC*		
					Diagonal	*Vertical*	*Horizontal*
Lena	[31]	7.999324	99.6119	33.4661	-0.041171	0.024064	-0.009448
	[22]	7.99915	99.6077 d=2,case=2	28.6181 d=2,case=2	-0.01930	-0.02264	-0.02457
	Proposed	**7.999329**	**99. 6376**	28. 6289	**-0.00032**	**0.003639**	**-0.0007**
Pepper	[31]	**7.999314**	99.6098	33.4556	0.046131	0.026099	0.001899
	[22]	7.99927	99.6099 d=2,case=2	29.5959 d=2,case=2	0.04578	0.03890	0.01218
	Proposed	7.999199	**99. 6117**	29. 6761	**0.000782**	**-0.001**	**-2.13E-05**
Baboon	[31]	7.999285	99.6104	33.4650	-0.025113	0.009395	-0.022540
	[22]	**7.99933**	99.6075 d=2,case=2	27.5702 d=2,case=2	0.01061	-0.04469	-0.01427
	proposed	7.999296	**99. 6265**	27. 8633	**0.001487**	**6.62E-05**	**0.001663**

From Table II, pixels correlations in the encrypted image are very weak in the main three directions. While it is very strong before implementing the proposed method in all directions. This means a good resistance against statistical attacks. In Fig.5, pixels of the encrypted image in all directions are evenly distributed in the test space, unlike the pixels of the original image. Table III shows the comparison of the proposed method with the other methods. According to the comparison, the proposed method produces better APCC values than other methods in [31] and [22]. It is worth noting that UACI value is better than [22], but it is close enough to [31]. This applies to information entropy, where the values are excellent and close. Bold values in Table III are better.

VI. CONCLUSIONS AND FUTURE WORK

A new method of scrambling images is presented in this paper, based on Logistic Map, which generates encryption keys and rotates image blocks according to preset rotation angles. The simulation results show very good results when the proposed method is evaluated and analyzed. Compared to other scrambling methods with more complex algorithms, the proposed method produces better results. Healthcare and IOT fields can benefit from it. Future applications may include Wireless Sensor Networks WSN

REFERENCES

[1] H.M. Ghadirli, A. Nodehi and R. Enayatifar, “An overview of encryption algorithms in color images,” Signal Processing, vol.164, pp.163-185, 2019. https://doi.org/10.1016/j.sigpro.2019.06.010 .

[2] I.J. Kadhim, P. Premaratne, P.J. Vial and B. Halloran,”Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,” Neurocomputing, vol.335, pp. 299–326,2019. https://doi.org/10.1016/j.neucom.2018.06.075 .

[3] A.A. Shah, S.A. Parah, M. Rashid and M. Elhoseny, “Efficient image encryption scheme based on generalized logistic map for real time image processing,” Journal of Real-Time Image Processing, vol.17,no.6, pp.2139-2151, 2020. https://doi.org/10.1007/s11554-020-01008-4.

[4] M. Kaur and V. Kumar,”A comprehensive review on image encryption techniques,” Archives of Computational Methods in Engineering, vol 27,no.1, pp.15-43, 2020. https://doi.org/10.1007/s11831-018-9298-8.

[5] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius and T. Blažauskas,”An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map,” Entropy, vol.21,no.7, p.656, 2019. https://doi.org/10.3390/e21070656.

[6] C. Li, “Cracking a hierarchical chaotic image encryption algorithm based on permutation,” Signal Processing, vol. 118, pp. 203–210, 2016. https://doi.org/10.1016/j.sigpro.2015.07.008.

[7] Z. Guan, J. Li, L. Huang, X. Xiong, Y. Liu and S. Cai, “A Novel and Fast Encryption System Based on Improved Josephus Scrambling and Chaotic Mapping,” Entropy, vol.24mno.3, p.384, 2022.https://doi.org/10.3390/e24030384.

[8] R.K. Reddlapalli and S. Malik, “Novel Secured Image Scrambling Technique Using Chaotic Sequence Shuffling and Pixel Value Modification Through Random Grid Map and Its Performance Analysis,” In Applications of Computing, Automation and Wireless Systems in Electrical Engineering , pp. 935-944, Springer, Singapore, 2019. https://doi.org/10.1007/978-981-13-6772-4_81.

[9] S.T. Kamal, K.M. Hosny, T.M. Elgindy, M.M. Darwish and M.M. Fouda, “A new image encryption algorithm for grey and color medical images,” IEEE Access,vol.9, pp.37855-37865, 2021. https://doi.org/10.1109/access.2021.3063237.

[10] C.L. Li, Y. Zhou, H.M. Li, W. Feng and J.R. Du, “Image encryption scheme with bit-level scrambling and multiplication diffusion,” Multimedia Tools and Applications, vol.80,no.12, pp.18479-18501, 2021. https://doi.org/10.1007/s11042-021-10631-7.

[11] P. Ping, J. Fan, Y. Mao, F. Xu and J. Gao, “A chaos based image encryption scheme using digit-level permutation and block diffusion,” IEEE Access, vol.6, pp.67581-67593, 2018. https://doi.org/10.1109/access.2018.2879565.

[12] C. Cao, K. Sun and W. Liu,”A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map,” Signal Processing, vol.143,pp.122-133,2018. https://doi.org/10.1016/j.sigpro.2017.08.020.

[13] B. Mondal, “Cryptographic image scrambling techniques,” In Cryptographic and Information Security ,pp. 37-65, CRC Press, , 2018.

[14] R. Li, Q. Liu and L. Liu, “Novel image encryption algorithm based on improved logistic map,” IET Image Processing, vol.13,no.1, pp.125-134, 2019. doi: 2009. https://doi.org/10.1049/iet-ipr.2018.5900.

[15] S. Sun, “A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling,” IEEE Photonics Journal, vol.10,no.2, pp.1-14,2018. https://doi.org/10.1109/JPHOT.2018.2817550.

[16] K.U. Shahna and A. Mohamed, “A novel image encryption scheme using both pixel level and bit level permutation with chaotic map,” Applied Soft Computing, vol.90, p.106162,2020. https://doi.org/10.1016/j.asoc.2020.106162.

[17] X. Wang, N. Guan and J. Yang,”Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map,” Chaos, Solitons & Fractals, vol.150, p.111117, 2021. https://doi.org/10.1016/j.chaos.2021.111117.

[18] S. Anwar and S. Meghana, “A pixel permutation based image encryption technique using chaotic map,” Multimedia tools and applications, vol.78,no.19, pp.27569-27590, 2019.

[19] Z. Hua, S. Yi and Y. Zhou,”Medical image encryption using high-speed scrambling and pixel adaptive diffusion,”Signal Processing, vol.144,pp.134-144,2018. https://doi.org/10.1016/j.sigpro.2017.10.004 .

[20] S. A. Banu, and R. Amirtharajan, “Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach,” Multimedia Tools and Applications, vol.79,no.39, pp.28807-28824,2020.

[21] B. Mondal, N. Sinha and T. Mandal,”A secure image encryption algorithm using lfsr and rc4 key stream generator,” In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, pp. 227–237, 2015.

[22] Y. Zhang and Y. Tang, “A plaintext-related image encryption algorithm based on chaos,” Multimedia Tools and Applications, vol.77,no.6, pp.6647-6669, 2018.

[23] R. Alvarez, C. Caballero-Gil, J. Santonja and A. Zamora, “Algorithms for lightweight key exchange,” Sensors, vol.17,no.7, p.1517, 2017.

[24] A. Belazi, A. A. Abd El-Latif and S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,” Signal Processing, vol.128, pp.155-170, 2016.

[25] A. Zingoni, M. Diani and G. Corsini, “Tutorial: Dealing with rotation matrices and translation vectors in image-based applications: A tutorial,” IEEE Aerospace and Electronic Systems Magazine, vol.34,no.2,pp.38-53,2019. doi:10.1109 /MAES .2018 .170099.

[26] G. Zhao, G. Chen, J. Fang and G. Xu,”Block cipher design: generalized single-use-algorithm based on chaos,” Tsinghua Science and Technology, vol.16,no.2, pp.194-206, 2011.

[27] M. Khan, I. Hussain, S.S. Jamal and M. Amin,”A privacy scheme for digital images based on quantum particles,” International Journal of theoretical physics, vol.58,no.12,pp.4293-4310, 2019. https://doi.org/10.1007/s10773-019-04301-6.

[28] Y. Pourasad, R. Ranjbarzadeh and A. Mardani, “A new algorithm for digital image encryption based on chaos theory,” Entropy, vol.23,no.3, p.341, 2021.

[29] A. Alghafis, N. Munir, M. Khan and I. Hussain, “An encryption scheme based on discrete quantum map and continuous chaotic system,” International Journal of theoretical physics, vol.59,no.4, pp.1227-1240, 2020. https://doi.org/10.1007/s10773-020-04402-7.

[30] E. Quiring, D. Klein, D. Arp, M. Johns and K. Rieck, “Adversarial preprocessing: Understanding and preventing {Image-Scaling} attacks in machine learning,” In 29th USENIX Security Symposium (USENIX Security 20),pp.1363-1380, 2020.

[31] Y. Zhang,”The unified image encryption algorithm based on chaos and cubic S-Box,” Information Sciences, vol.450, pp.361-377, 2018. https://doi.org/10.1016/j.ins.2018.03.055 .