Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 5, pp. 1903–1912
DOI : 10.47974/JDMSC-2351

A proposed new encryption method for image based on two levels of chaotic maps

Ebtehal Talib *
Aseel Wadood Majeed †
Ministry of Higher Education and Scientific Research
Baghdad
Iraq

Zainab Jalil Taher §
Department of Computer Science
University of Technology
Baghdad
Iraq

Abstract

This article, two-level encryptions algorithms combining two chaotic maps (logistic and tent maps) is proposed for images encryptions. These maps are used to encrypt an image to verify if the safe cipher's properties of diffusion and confusion are met. The first map generates a key to execute the permutation process, while the second generates a key for the substitution process. Experimental results explain that the proposed algorithms offer high levels of security and are resistant to statistical and differential attacks.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cryptography, Image encryption, Logistic map, Tent map, Diffusion, Confusion.*

1. Introduction

Secure image transfer has become more important with the rapid expansion of mobiles network, Internets for Thing, cloud computing, and social network [1]. To ensure a secure route for data transfer across multiple communication channels, it is vital to encrypt images sent over networks [2]. Data Encryptions

* *E-mail:* talibebtehal@gmail.com (Corresponding Author)
† *E-mail:* Aseel_wadood@yahoo.com
§ *E-mail:* 10883@uotechnology.edu.iq

© Taru Publications

Standard (DES), Advance Encryptions Standards (AES), and other encryptions techniques cannot be used for image encryption because images have large file sizes, significant redundancy, and strong correlations between neighbouring pixels [3]. Therefore, chaotic maps provide faster encryption through simple mathematical calculations, thereby enhancing performance in online image encryption applications compared to complex iterations, such as DES and AES [4].

Chaos suggests a disordered state, while a map is a scientific development that exemplifies certain chaotic behaviour [5]. Since chaos signals have crucial properties, like as being extreme sensitive to the initials condition and frameworks parameter, having fake - irregular properties, but not being periodic like turbulent waves, they are believed to be beneficial in practical applications [5]. As a result, the use of chaos theory in encryption opens up a sizable portion of the fields for a data securities. The Chaos framework be the magnificent and powerful crypto-framework due to its resistance to statistical attacks [6]. Data security is a key area where the blending of chaotic supposition and cryptography is possible. The study of data security emphasizes chaos-based image encryption [2], [7]. Accordingly, the encryption of images is not nearly as straightforward as that of words due to various persistent media characteristics, such as information limits and significant information overflow, making it challenging to handle them with traditional encryption techniques [8], [9].

2. Chaotic Map

The integration of chaotic maps with cryptographic frameworks takes data security seriously. The study of data security pays a lot of attention to chaos-based image encryption. The encryption of images is not nearly as straightforward as that of text due to various persistent media characteristics, such as significant information overflow, which make it challenging to handle them with traditional encryption techniques [9], [10]. There are numerous chaotic algorithms for encrypting data, including Logistic, Baker, Fibonacci, Tent, Hyper, and Arnold map, so explains a chaotic map use in the suggested encryption algorithm.

2.1. *Logistic maps*

One of the most popular types of Chaotic map use in images encryptions is one-dimensional (1D) logistic maps, that discover by authors. The main features of this map are its non-determinism, irregularity, and periodicity [2], [11]. The logistic map was expressed mathematically as shows below [12]:

$$X_{n+1} = B(X_n - X_n^2) \tag{1}$$

where X_nThe initial value is a number between 0 and 1, anywhere in that range. The user must construct a chaotic sequence for the parameter B estimations to occur between 3 and 4. Equation (1) produces a chaotic random configuration, which is employed to encrypt the image [4], [12].

B value in equation (1) is based on [12]:

- If B is greater than 0 and lower than 1……. the characteristics will be in a stable condition.
- If B is greater than 1 and lower than 3… the characteristics will quickly advance.
- If B is greater than 3 and lower than 3.44949… the populace will be encouraged to alternate between two qualities continuously.
- 3.44949< B < 3.54409, the general population will gravitate toward constant motions among four traits from nearly all underlying situations.

Every underlies condition will shifted toward motion between 8 characteristics when B increases past 3.54409 realistically. When $B \approx 3.56995$, the situation is regarded as the start of chaos. When $3.57 < B \leq 4$, the user's guide is confusing. There is a hidden area that displays the disorganized condition.

2.2. *Tent maps*

One for simpler chaotic map be tent maps. It features a straightforward guide with multiple meanings and a single dimension. The tent map's disorderly practices were diagnostically concentrated in its chaotic zone with respect to the invariant thickness and the force range [10]. It was discovered that progressive band parting shifts in the chaotic location as the climax intensifies and assembles at the progress point into the quiet area [13]. Tent map practices are currently in the cycle because it is topologically conjugate. This is how it is given in the following equation [14]:

$$X_{n+1} = f\mu \begin{Bmatrix} \mu X_n \, for \, X_n < \frac{1}{2} \\ \mu(1 - X_n) for \, \frac{1}{2} \leq X_n \end{Bmatrix} \quad (2)$$

The result of the $f\mu$ is the interval selected as $(0, \frac{1}{2})$ or (0,1) where μ is a positive genuine steady, such as =2, while n is generating a sequence in (0,1), X_0 is assumed to be a new ensuing position [7], [14].

3. Related Work

In [1], the images be separat into three channels (R, G, B), converted from pixel to bits, then the Arnold cat maps be applied, followed by four-dimensional systems, called Lorenz system. In [4], An image be separated into three channels (R, G, B), so skew tent maps was apply for confusions and a hyper - chaotic systems for the 6^{th} - order CNN apply for diffusion. To maintain uniformity and low autocorrelation, this paper proposed a new couple map lattice with Markov properties, based on the class of chaos [5], [6], the colour image is split into (R, G, B) channels, then Chen's hyperchaos map is applied, and the resulting sequences are converted into DNA matrix codes, which are then XORed to obtain the final result. In [7], an improved Logistic Map for encryption is proposed, using a zigzag transformation and block scrambling to achieve the

best representation for diffusion and confusion. In [8], a proposed method that combined Sine chaotic and 1D logistic maps to address the concepts of confusion and diffusion was used. The study in [10] employed a proposed method that combined multiples chaotic map (2D Logistics Sine, Linear Congruently Generators, Bernoulli map, Tent maps), Shannon's ideas, KAA maps to address confusion and diffusion concepts. In [11], the study used a proposed method for encrypting colour images based on an alternative chaotic mapping structure. A Chaotic matrix was generated using 1D & 2D logistics map, an XOR operations is then applied to them. In [12], the colour image was converted into the (R, G, B) colour channels, and then Chen's hyper - chaotic maps & DNA sequences were used for encryptions. In [13], the novel encryptions method base on delay & cascade maps was proposed, use tent delay - sine cascades with logistics maps. In [14], a new method was proposed using hyperchaotic & DNA sequence for images encryptions.

4. The Proposed Image Encryption Algorithms

An encryptions and decryptions algorithms are the two components for proposal. The proposed image encryption algorithm uses two chaotic maps to generate two key sequences for confusion and diffusion, providing it with two levels of security. Chaos maps cause confusion due to their true randomness, high sensitivity to key inputs, lack of recurring patterns, and the complexity of their input-output relationships. Figure 1 shows the proposed encryption algorithm.

5. Metrics for Performance Assessment

An effectiveness for a proposed picture encryptions algorithms is evaluated using various metrics. These indicators are the Correlation Coefficient, Unified Averages Chang Index, Number for Pixels Changes Rate (NPCR).

5.1 *NPCR and UACI*

An resistance for encryptions algorithms to the differentials attack is demonstrated by NPCR & UACI results [15]. Equation (3) describes how NPCR is calculated, which measures a pixels differences among original and encrypt image. A higher NPCR rating is obtained with a greater degree of pixel randomness [16]:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W*H} * \ 100\% \tag{3}$$

A means intensity for the variations among originals images and the encrypt images is measured by UACI, as explained in equation (4) [17]:

$$\mathrm{UACI} = \frac{1}{L}\left[\sum_{i,j} \frac{P(i,j) - C(i,j)}{255}\right] * \ 100\% \tag{4}$$

D(i, j) is:

$$\mathrm{D(i,j)} = \begin{cases} 0 \ P(i,j) = C(i,j) \\ 1 \ P(i,j) \neq C(i,j) \end{cases}$$

P(i, j) & *C(i, j)* the pixels value for originals & encrypt image, while *W* & *H* represents a width & height for a images and *L* be greatest pixels values for both image [18].

5.2 *Correlation Coefficient*

A correlations coefficients (*r*) are another important metric of evaluate effectiveness for the encryptions scheme. A values ranging from -1 to 1 is obtained when calculate a correlations coefficients among two pixel in x & y [19], [20]. For an encryption method to be immune to statistical attacks, a correlations coefficients among adjacent pixel is close to the zero, indicating no correlations [21]. Otherwise, statistical attacks could potentially uncover an encrypted image because values near 1 & -1 indicated high positive & negative correlation. A correlations coefficients is calculate use equation (5):

$$r_{x,y} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{1}^{N}(X_i - E(x))(y_i - E(y))$$

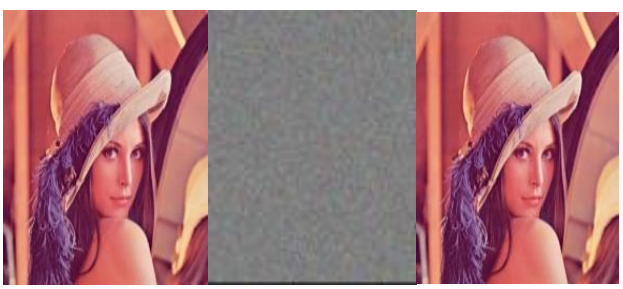
$$E(x) = \frac{1}{N}\sum_{1}^{N} X_i$$

$$D(x) = \frac{1}{N}\sum_{1}^{N}(X_i - E(x))^2$$

In this case, *X* and *Y* denote the pixel for originals & encrypted image, respectively, as well as pixels that surround them, whereas E(X) denotes X's expect values and D(X) denotes *X's* variance. A covariance between *X* & *Y* denoted by *Cov(X, Y)*.

6. Results and Discussion

Several images (Lena, Peppers, and Baboon) are employed, which are popular in image processing. These are all 512×512 in size. Additionally, comparisons with similar algorithms from the literature are made. In Figures 1 and 2, the original images of Lena and the baboon are shown in column (a), followed by encrypted image in column (b) & decrypted image in column (c).



(a) (b) (c)

Figure 1

(a) Plains Lena Images, (b) Encrypted Images, (c) Decrypted Images.



(a) (b) (c)

Figure 2
(a) Plains baboon Images, (b) Encrypt Images, (c) Decrypted Images.

Tables 1, 2, and 3 present the performance assessment values after applying the suggested technique to a few test images.

Table 1

Performance Evaluations for Proposed Algorithms.

Image	NPCR	UACI	Correlation Coefficient	Encryption Time	Decryption Time
Lena	0.99735479 12597656	0.49922002 65522876	0.001278434 0173696445	1.5 seconds	0.8 seconds
peppers	0.99697095 7438151	0.49888429 33006536	0.001456028 2273352037	1.5 seconds	0.8 seconds
baboon	0.99661039 62418301	0.49914391 90055107	0.000553839 3547101594	1.5 seconds	0.8 seconds

Table 2

Key Space Analysis for the Proposed Algorithm.

Parameter	Result
Parameter Numbers	4
Precision/ parameter	10^{-4}
Key space	$4*10^{55}$
Resistance to Brute-force attack	

Table 3

Performances Evaluations Comparisons with Other Method.

References	Image Size	NPCR	UACI	Correlation Coefficient
Proposed algorithm	**512*512**	**99.84**	**49.92**	**-0.0012**
[1]	170*170	99.64	29.52	-
[4]	256*256	99.60	33.9	-
[5]	256*256	99.61	-	-0.023

[6]	256*256	99.10	15.38	-0.0140
[7]	256*256	99.6221	33.5887	-0.0237
[8]	512*512	99.6161	33.4975	-0.0004
[10]	256*256	99.6254	30.57	-0.0036
[11]	256*256	98.36	27.97	-0.0007
[12]	256*256	98.6810	33.4647	- 0.0137
[13]	256*256	99.6094	33.4635	−0.0011
[14]	256*256	93.21	32.48	-0.0050

- The NPCR value indicates the degree of pixel change among plains & ciphered image, the high NPCR value is desirable. The NPCR value of (Lena, peppers, and baboon**)** images indicates a difference between plain and ciphered images is approximately (99.48%, 99.50%, and 99.46) respectively, which means there are significant pixel changes.
- The UACI value indicates the intensity change among plains & cipher image, a lower UACI value is desirable, which means the encryption algorithm is preserving the intensity information for pixel. UACI value for (Lena, peppers, and baboon**)** images indicates (49.92%, 49.89%, and 49.91%) respectively, which means the encryption algorithm is preserving the intensity information of the pixels.
- The correlation coefficient indicates a linear correlation among originals images & encrypt images. A low correlation coefficient (close to zero) is generally desirable, as it indicates that the encryption algorithm has made significant changes and introduced high level for randomness, which is desirable for secure encryptions. A correlation coefficient value of (Lena, peppers, and baboon**)** images indicates (-0.0012784340173696445, 0.0014560282273352037, and 0.0005538393547101594) respectively, which means almost no linear correlation among originals images & encrypted images.
- Encryption Time: An encryptions times of propose algorithms is 1.3 second, which means propose algorithms is very fast. A times to encrypted the images can vary depend on the hardware capability & images sizes.
- A results explain a encryptions algorithms is performing well in terms of pixel changes (NPCR), intensity preservation (UACI), and disrupting any linear relationship between originals and encrypt images (correlation coefficient). This indicate a proposed algorithms had comparable or better performance than those estimated for its counterparts in the literature, as evidenced by comparisons across numerous method metrics.

7. Conclusion

A colour image encryptions algorithms with two layers of security based on two chaotic maps is proposed. These maps were used to implement confusion and diffusion to obtain robust cryptographic security. A variety of metrics, including correlation coefficient analysis, UACI, and NPCR, were used to evaluate proposed algorithm performance. The suggested colour-image

encryption algorithm performed well and resisted both differential and statistical attacks. Finally, the proposed algorithm had comparable or better performance than its counterparts in the literature, as indicated by the values of its numerous metrics.

References

[1] A. Bisht, M. Dua, S. Dua, and P. Jaroli, "A color image encryption technique based on bit-level permutation and alternate logistic maps," *J. Intell. Syst.*, vol. 29, no. 1, pp. 1246–1260 (2019).

[2] H. A. Al-Asady, O. Q. J. Al-Thahab, and S. S. Hreshee, "Robust encryption system based watermarking theory by using chaotic algorithms: A review paper," *J. Phys. Conf. Ser.*, vol. 1818, no. 1 (2021), doi: 10.1088/1742-6596/1818/1/012086.

[3] J. Yu, W. Xie, Z. Zhong, and H. Wang, "Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation," *Chaos Solitons Fractals,* vol. 162 (2022), doi: 10.1016/j.chaos.2022.112456.

[4] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik,* vol. 125, no. 5, pp. 1671–1675 (2014), doi: 10.1016/j.ijleo.2013.09.040.

[5] Q. Liu, P.-Y. Li, M.-C. Zhang, Y.-X. Sui, and H.-J. Yang, "A novel image encryption algorithm based on chaos maps with Markov properties," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 506–515 (2015), doi: 10.1016/j.cnsns.2014.06.005.

[6] A. Y. Niyat, R. M. H. Hei, and M. V. Jahan, "A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system," in *Proc. Int. Congr. Technol. Commun. Knowl. (ICTCK),* (2015).

[7] 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, Art. no. 656 (2019), doi: 10.3390/e21070656.

[8] I. A. Taqi and S. M. Hameed, "A new color image encryption based on multi chaotic maps," *Iraqi J. Sci.,* vol. 59, no. 4B, pp. 2117–2127 (2018).

[9] G. Veena and M. Ramakrishna, "A survey on image encryption using chaos-based techniques," *Int. J. Adv. Comput. Sci. Appl.,* vol. 12, no. 1 (2021).

[10] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11541–11554 (2023), doi: 10.1109/ACCESS.2023.3242311.

[11] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Opt. Lasers Eng.,* vol. 82, pp. 79–86 (2016), doi: 10.1016/j.optlaseng.2015.12.006.

[12] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.,* vol. 85, no. 2, pp. 290–299 (2012), doi: 10.1016/j.jss.2011.08.017.

[13] G. Zhang, W. Ding, and L. Li, "Image encryption algorithm based on tent delay-sine cascade with logistic map," *Symmetry*, vol. 12, no. 3, Art. no. 355 (2020), doi: 10.3390/sym12030355.

[14] Y. Zhang, "Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik,* vol. 126, no. 2, pp. 223–229 (2015), doi: 10.1016/j.ijleo.2014.08.129.

[15] A. Abirami and S. Palanikumar, "Proposed security models for node-level and network-level aspects of wireless sensor networks using machine learning techniques," *Iraqi J. Sci.,* vol. 64, no. 12, pp. 6493–6508 (2023), doi: 10.24996/ijs.2023.64.12.32.

[16] S. M. Khudaier and B. A. Mahmood, "A review of assured data deletion security techniques in cloud storage," *Iraqi J. Sci.,* vol. 64, no. 5, pp. 2492–2511 (2023), doi: 10.24996/ijs.2023.64.5.33.

[17] N. A. Ali, A. M. S. Rahma, and S. H. Shaker, "3D content encryption using multi-level chaotic maps," *Iraqi J. Sci.,* vol. 64, no. 5, pp. 2521–2532 (2023), doi: 10.24996/ijs.2023.64.5.35.

[18] M. G. Alwan, E. T. Khudair, and E. F. Naser, "A hybrid algorithm based on the Aizawa attractor and rabbit-lightweight cipher for image encryption," *Iraqi J. Sci.*, vol. 64, no. 12, pp. 6534–6547 (2023), doi: 10.24996/ijs.2023.64.12.35.

[19] M. J. Obaid and N. F. H. A. Saffar, "Asymmetric image encryption based on singular cubic curve with chaotic map," *Iraqi J. Sci.*, vol. 65, no. 5, pp. 2605–2618 (2024), doi: 10.24996/ijs.2024.65.5.21.

[20] M. D. Abdul-Jabbar and Y. A. A. S. Aldeen, "A key-based hybrid approach for privacy and integrity in multi-cloud," *Iraqi J. Sci.,* vol. 64, no. 11, pp. 5952–5963 (2023), doi: 10.24996/ijs.2023.64.11.39.

[21] J. von der Assen, A. Huertas Celdrán, J. Luechinger, P. M. Sánchez Sánchez, G. Bovet, G. M. Pérez, and B. Stiller, "RansomAI: AI-powered ransomware for stealthy encryption," in *Proc. IEEE Global Communications Conference (GLOBECOM),* Kuala Lumpur, Malaysia, pp. 2578–2583 (2023), doi: 10.1109/GLOBECOM54140.2023.10437393.

Received May, 2025