JJEE

Volume 12 | Number 3 | September 2026 | Pages 576-594

Jordan Journal of Electrical Engineering

ISSN (print): 2409-9600, ISSN (online): 2409-9619

Homepage: jjee.ttu.edu.jo

Image Encryption Algorithm Based On A Modified Two-Dimensional Tent Chaotic Map

Abdelrahman A. Karawia[1,2*]

[1] Mathematics Department, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt.
E-mail: abibka@mans.edu.eg

[2] Department of Computer Science, College of Engineering and Information Technology, Onaizah Colleges, Qassim 56447, Saudi Arabia.
E-mail: akarawia@oc.edu.sa

Received: Oct 29, 2025 Revised: Jul 17, 2026 Accepted: Sep 03, 2026 Available online: Sep 15, 2026

Abstract— In this paper, a plaintext-related image encryption algorithm is proposed based on a newly constructed tent chaotic map in two dimensions (2D-TentCM). The proposed map extends the classical one-dimensional tent dynamics to two coupled dimensions resulting in stronger nonlinearity, improved ergodicity, and increased sensitivity to initial conditions and control parameters. To improve the plaintext dependence and to increase the effective key space, the initial states and the map parameters are adaptively updated by an image-derived key-mixing mechanism before the generation of chaotic sequences. The resulting keystreams are then used in a permutation-diffusion framework for encrypting the image data. The security analysis includes histogram uniformity, information entropy, adjacent pixel correlation, NPCR, UACI and key sensitivity analysis. The experimental results show that the proposed algorithm results in ciphertexts with near uniform statistical characteristics, strong avalanche behavior and high resistance to brute force, differential and plaintext related attacks. These results indicate that the proposed 2D-TentCM-based architecture is a competitive and computationally efficient candidate for secure image encryption applications.

Keywords— Two-dimensional tent map; Chaotic systems; Image encryption; Cryptographic security.

1. INTRODUCTION

Considering the rapid progress of digital communication technologies, multimedia data transmission over open and insecure networks has increased dramatically, raising concerns about data privacy and security. Among the various forms of digital content, images often contain highly sensitive or confidential information and are widely used in sensitive fields such as telemedicine, surveillance, and defense. With enhanced image encryption algorithms, communication will be better protected against cryptanalytic attacks that endanger the confidentiality and integrity of images [1]. Although traditional encryption techniques are effective for text data, they are often insufficient for protecting images because of the high dimensionality, redundancy, and large volume inherent in image files.

Currently, chaotic systems have appeared as important tools for image encryption due to their structural properties, like sensitivity to initial conditions, pseudo-randomness, and simplified operations. These properties give chaotic maps the ability to generate complex and unpredictable encryption keys. Unlike conventional encryption algorithms, chaotic map-based techniques can produce high degrees of confusion and diffusion with minimal computation, which makes them perfect for real-time and embedded systems. The comprehensive survey classifies chaos-based image encryption algorithms into spatial,

* Corresponding author
DOI: https://doi.org/10.5455/jjee.204-1761758589

temporal, and spatio-temporal domains, mentioning their development and effectiveness in securing image data [2]. Chaotic maps for image encryption are typically classified based on their dimensionality: (a) One-dimensional maps, like logistic maps and tent maps, are characterized by their simple structure and ease of implementation. However, their simple complexity may reduce their effectiveness in achieving high levels of security in cryptographic applications [3, 4]. (b) Multidimensional maps, including higher-dimensional systems such as Lorenz and Chen systems, offer increased complexity and good security properties. The survey presented in [5] presents various chaotic maps and their suitability for image encryption. (c) Hybrid cryptosystems, like those suggested in (b), involving couples of chaotic maps can also make contribution to enhanced secure algorithms by the complementary improvements from each other [6]. Even though cryptosystems based on chaos have advantages in complexity and sensitivity, they are still confronted with several issues. (a) Cryptanalysis: During cryptanalysis, many chaotic cryptographic schemes are found to be weak in analytical perception. For instance, in [7], researchers analyzed an image block cipher algorithm based on chaotic maps and exploited its weaknesses via the use of chosen plaintext attacks. (b) Key Space and Sensitivity: Having huge key space ($\gg 2^{128}$), as well as ultra-sensitive dependence on initial conditions, are necessary in dealing with brute-force attacks [8, 9]. These conditions also need to be kept in mind for the construction of chaotic systems because keeping those factors into account is important to maintain powerful security strength against probable attacks. In this paper, a novel image encryption algorithm using 2D chaotic map and dynamic switching strategy is presented. This system was studied and implemented with appropriate mathematical theories to achieve a large key space, high sensitivity, and well defense against the statistical attack and the differential attack. The main contributions of this paper can be summarized as follows.

- We propose a novel privacy-preserving image encryption framework that combines a plaintext-dependent 2D chaotic map with dynamic differentially private deep architectures, marrying cryptographic security with formal privacy protection.
- We design a novel 2D discrete chaotic map with nonlinear cross-coupling and polynomial correction terms. We demonstrate that the proposed map has strong chaotic behavior, high sensitivity to initial conditions, and positive Lyapunov exponents for a wide range of parameters.
- All NIST tests are successfully met by the suggested algorithm, exemplifying that the encrypted image is of a high level of security and random features.
- To improve the key sensitivity and enhance the security against the known-plaintext and chosen-plaintext attacks, we propose a plaintext-adaptive parameter updating mechanism in which the chaotic control parameters are extracted from image block statistics.
- A hybrid permutation-diffusion encryption pipeline is developed based on the proposed chaotic map and dynamic perturbation strategy to realize efficient and reversible image decryption and encryption.
- The proposed method is compared with AES and recent chaos based schemes under identical test images and a comprehensive security evaluation is provided by means of standard metrics like entropy, correlation, NPCR, UACI, key sensitivity and runtime analysis.

- We discuss the limitations of the proposed approach, including the dependence on proper parameter selection, and the need for further validation on more diverse image datasets and application scenarios.

The rest of the paper is structured as follows. Section 2 presents the design of a two-dimensional chaotic map and describes its mathematical properties as well as dynamic behavior. The corresponding image encryption/decryption schemes are described in Section 3. Section 4 summarizes the experimental results and security analyses including key sensitivity, NPCR, UACI and histogram analysis. Benchmarking against AES and chaos-based algorithms is given in Section 5. Section 6 presents a summary of the main results and recommendations for further research.

2. DESIGN OF A TWO-DIMENSIONAL CHAOTIC MAP(2D-TENTCM)

2.1. Mathematical Formulation

To achieve a good state of unpredictability and make chaotic behavior more complex, a new chaotic map is suggested. This map is designed by modifying the classical tent map and adding nonlinear interactions between two state variables. The suggested modified tent-based chaotic map (2D-TentCM) is defined as follows:

$$x_{n+1} = \begin{cases} (r_1 |x_n|^p + sin(\pi y_n)) \bmod 1, & \text{if } x_n < 0.5 \\ (r_1 |1 - x_n|^p + cos(\pi y_n)) \bmod 1, & \text{if } x_n \geq 0.5 \end{cases} \quad (1)$$

$$y_{n+1} = (r_2 y_n + x_n) \bmod 1$$

Where, the control parameters: x_n, $y_n \in [0, 1]$ at iteration n, r_1, r_2, and the power-law exponent: p that controls the nonlinearity of the system.

2.2. Dynamical Properties

The 2D-TentCM model exhibits good dynamical behavior, ranging from periodic to completely chaotic responses, depending on the choice of its parameters. Numerical simulations, based on Lyapunov exponent analysis and bifurcation diagrams, confirm the presence of chaotic regimes for a wide range of values r_1 and p.

- For appropriate values (e.g., r_1 = 2.0, p = 1.5), the Lyapunov exponent remains positive, indicating long-term unpredictability and dependence on initial conditions.
- The map avoids repetitive patterns and produces pseudo-random sequences that are perfect for cryptography applications by generating complex trajectories in the (x_n, y_n) plane.

The parameter ranges listed in Table 1 can be used to choose the parameters for encryption applications.

Table 1. Parameter ranges of 2D-TentCM.

Parameter	Description	Suggested Range
r_1	Tent strength	1.5 – 3.0
r_2	Coupling gain to y	1.5 – 2.5
p	Power nonlinearity	1.2 – 2.0
x_0, y_0	Initial values	(0,1)

The chaotic character of the 2D-TentCM system is confirmed by the bifurcation behavior of the 2D-TentCM map in Fig. 1 for the sequence x versus the tent strength parameter r_1, The

Lyapunov Exponent (LE) of the 2D-TentCM chaotic map versus $r_1 \in (1,3)$ with $r_2 = 2.2$, and $p = 2.0$ is presented in Fig. 2, and Fig. 3 shows the phase-space visualization. The positive Lyapunov exponent indicates the sensitive dependence on the initial conditions. The bifurcation diagram and the attractor plot show the rich nonlinear dynamics and the complex evolution of the states. For $r_1 = 1.5$, $r_2 = 2.2$, $p = 2.0$ and $(x_0, y_0) = (0.1212, 0.2323)$, the Lyapunov exponent spectrum of the proposed 2D-TentCM map was obtained as λ_1=0.591984 and λ_2=−0.44550. The positive largest Lyapunov exponent confirms the existence of chaos through sensitive dependence on initial conditions, and the negative second exponent indicates phase-space contraction, confirming that the system exhibits dissipative chaotic dynamics.

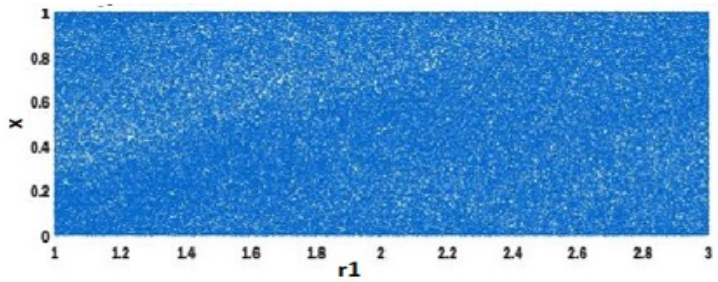


Fig. 1. Bifurcation behavior of the 2D-TentCM map as the x sequence evolves with changes in the control parameter r_1.

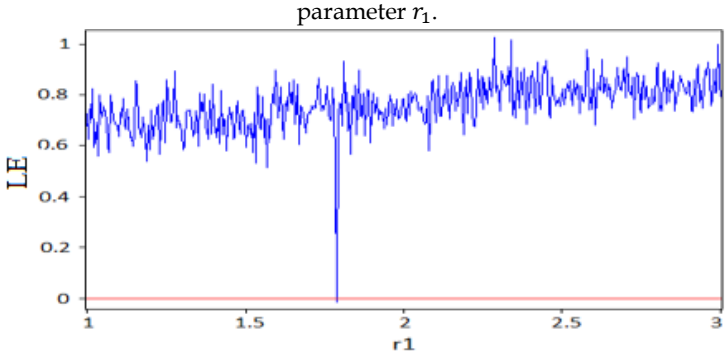


Fig. 2. Variation of the Lyapunov exponent of the 2D-TentCM map with respect to r_1 in $(1, 3)$, with $r_2 = 2.2$ and $p = 2.0$.

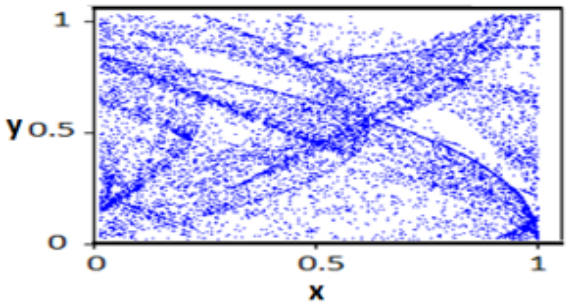


Fig. 3. Phase-space plot of the 2D-TentCM map, illustrating the chaotic attractor in the (x_n, y_n)plane.

3. THE SUGGESTED IMAGE ENCRYPTION/DECRYPTION ALGORITHM

Two novel algorithms are introduced in this section: one for encrypting images and the other for securely decrypting them.

3.1. Secure Algorithm for Image Encryption

Suppose that the original image is expressed by O = ($o_{d1,d2}$) where d1 = 1, 2, …, M, and d2 = 1, 2, . . . , N. The suggested algorithm consists of three main steps:

- secret key generation,
- pixel shuffling for the source image, and
- pixel confusion for the shuffled image.

The secret key of the suggested algorithm comprises three control parameters, r_1, r_2, and p, along with two initial values, x_0 and y_0. These values are central for initializing the chaotic map and confirming the algorithm's sensitivity and security. At this point of the suggested algorithm, the secret key is developed from the key mixing proportion method, which is outlined below.

$$\left.\begin{aligned} L_1 &= \frac{1}{256}\, mod\left(\sum_{d1=1}^{\frac{M}{2}}\sum_{d2=1}^{N} o_{d1,d2}, 256\right) \\ L_2 &= \frac{1}{256}\, mod\left(\sum_{d1=\frac{M}{2}+1}^{M}\sum_{d2=1}^{N} o_{d1,d2}, 256\right) \end{aligned}\right\} \quad (2)$$

The initial values are adapted using the following formulas:

$$\left.\begin{aligned} x_0 &= \frac{x_0+L_1}{2} \\ y_0 &= \frac{y_0+L_2}{2} \end{aligned}\right\} \quad (3)$$

Similarly, the control parameters are revised on the basis of the following equation.

$$\left.\begin{aligned} r_1 &= 1.5(L_2+1), \\ r_2 &= L_2 + 1.5, \\ p &= 0.8L_2 + 1.2. \end{aligned}\right\} \quad (4)$$

The pixel-block based adaptation in Eq. (4) adds plaintext dependence to the control parameters, resulting in higher key sensitivity and better resistance to replay and known-plaintext attacks. The linear transformation from L_2 to r_1, r_2 and p is computationally efficient and can be used to locate the chaotic map in an appropriate parameter region.

The second main step includes generating a random sequence of size M×N using 2D-tentCM formalized in Eq. (1). This sequence (x) is then used to achieve pixel shuffling on the original image. Finally, the last main step is executed by applying a bitwise XOR operation between the preprocessed sequence (y, also obtained from the map in Eq. (1)), and the shuffled image pixels. The Algorithm 1 details the procedure used to encrypt the source image **O**. In order to generate the byte-valued sequence in Algorithm 1, the chaotic output y is first multiplied by 10^{14} before the floor and modulo operations. This factor was chosen to preserve a large degree of numerical resolution from the continuous chaotic state, while still being compatible with double precision arithmetic. Specifically, 10^{14} gives about 46.5 ($\log_2(10^{14})$) bits of granularity per sample. This reduces quantisation loss, increases the sensitivity of the generated sequence and increases the effective key space of the algorithm. The selected scaling is therefore a pragmatic compromise between precision, security and numerical stability.

3.1.1. Secure Algorithm for Image Decryption

An inversion of the image encryption is performed to restore the source image from its encrypted form. It serves a crucial function in securing image communication by restricting access to the source image to authorized users only. During encryption, an image is typically scrambled and updated using keys and chaotic transformations to make it unreadable. The decryption algorithm utilizes the same keys and inverse operations to accurately restore the source image. The Algorithm 2 details the steps used to decrypt the encrypted image **E**. The diagram of the encryption and decryption processes is shown in Fig. 4.

For the color images, an RGB image has three separate color channels, so the same decryption and encryption algorithm can be used separately for each channel. Specifically, the red, green, and blue channels are processed separately using the proposed algorithm, and the three resulting cipher channels are then combined to form the final encrypted RGB image. This approach preserves the structure of the algorithm while extending it naturally from grayscale to color images.

Algorithm 1. Image Encryption

Input: Source image O, x_0, y_0, r_1, r_2, and p for 2D-TentCM.
Output: Encrypted image E.
1: Import the image O and convert it into a 1 ×MN vector.
2: Initialize the 2D-TentCM with the secret key $(\mathbf{x_0}, \mathbf{y_0}, \mathbf{r_1}, \mathbf{r_2}, \mathbf{p})$ to generate two statistically random sequences, $\mathbf{x}$ and $\mathbf{y}$, each of size 1× MN.
3: Use the generated chaotic sequences to build a plaintext-dependent permutation and diffusion process.
4: $\mathbf{x_1} = \mathbf{x_0}; \mathbf{y_1} = \mathbf{y_0}$
5: for n = 1 to MN − 1
6: if $\mathbf{x_n} < \mathbf{0.5}$
7: $\mathbf{x_{n+1}} = \mathbf{r_1} * |\mathbf{x_n}|^{\mathbf{p}} + \mathbf{sin}(\boldsymbol{\pi} * \mathbf{y_n})$
8: else
9: $\mathbf{x_{n+1}} = \mathbf{r_1} * |\mathbf{1} - \mathbf{x_n}|^{\mathbf{p}} + \mathbf{cos}(\boldsymbol{\pi} * \mathbf{y_n})$
10: end if
11: $\mathbf{x_{n+1}} = \mathbf{mod}(\mathbf{x_{n+1}}, \mathbf{1})$
12: $\mathbf{y_{n+1}} = \mathbf{mod}(\mathbf{r_2} * \mathbf{y_n} + \mathbf{x_n}, \mathbf{1})$
13: end for
13: Sort the sequence x and record the indices of the sorted elements in a new sequence z.
14: Compute Sh as follows:
15: for n = 1 to MN
16: Sh(z(n)) = O(n)
17: end for
18: Convert Sh into the binary vector B = {b_1, b_2, ..., b_{MN}}.
19: W = mod(floor(y × 10^{14}), 256))
20: Represent W as a binary vector W = {w_1,w_2, ...,w_{MN}}.
21: Perform E = xor(B,W).
22: Represent E as a decimal vector E = {e_1, e_2, ..., e_{MN}}.
23: Restructure the vector E into a 2D array of size M×N, also denoted as E.

4. RESULTS AND DISCUSSION

4.1. Visualization

This section presents results obtained on some test images from the Miscellaneous database of the USC-SIPI Image Database to visually demonstrate the effectiveness of the suggested algorithms.

Figure 5 shows the encryption/decryption results obtained using the suggested algorithms. From the obtained results, we can see that the encrypted output of the source image is a noise-like pattern, which confirms strong visual confusion. These results demonstrate the visual security of the encrypted image produced by the suggested algorithm and also satisfy the requirement of recovering the source images.

Algorithm 2. Image Decryption

Input: Encrypted image E, x_0, y_0, r_1, r_2, and p for 2D-TentCM.
Output: Source image O.
1: Import the image E and flatten it into a 1 ×MN vector.
2: Represent E as a binary vector E ={e_1, e_2, ..., e_{MN}}.
3: Initialize the 2D-TentCM with the secret key to derive two statistically random sequences, $\boldsymbol{x}$ and $\boldsymbol{y}$, each of size 1× MN as follows:
4: $\boldsymbol{x_1 = x_0;\ y_1 = y_0}$
5: for n = 1 to MN − 1
6: if $\boldsymbol{x_n < 0.5}$
7: $\boldsymbol{x_{n+1} = r_1 * |x_n|^p + sin(\pi * y_n)}$
8: else
9: $\boldsymbol{x_{n+1} = r_1 * |1 - x_n|^p + cos(\pi * y_n)}$
10: end if
11: $\boldsymbol{x_{n+1} = mod(x_{n+1}, 1)}$
12: $\boldsymbol{y_{n+1} = mod(r_2 * y_n + x_n, 1)}$
13: end for
14: W = mod(floor(y × 10^{14}), 256))
15: Represent W as a binary vector W = {w_1,w_2, ...,w_{MN}}.
16: Perform B = xor(E,W).
17: Represent B as a decimal vector Sh
18: Sort the sequence x and record the indices of the sorted elements in a new sequence z.
19: Obtain the restored image O as follows:
20: for n = 1 to MN
21: O(n) = Sh(z(n))
22: end for
23: Restructure the vector O into a 2D array of size M×N.

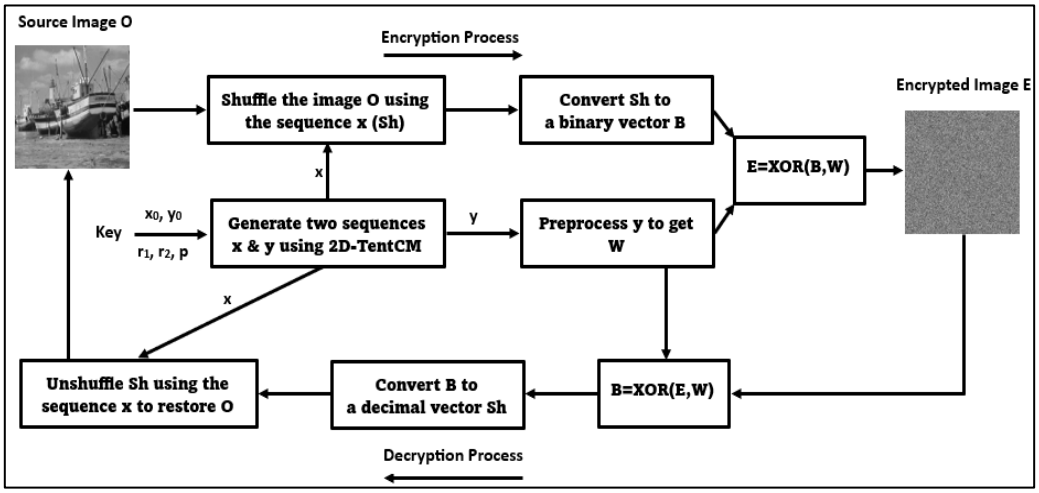
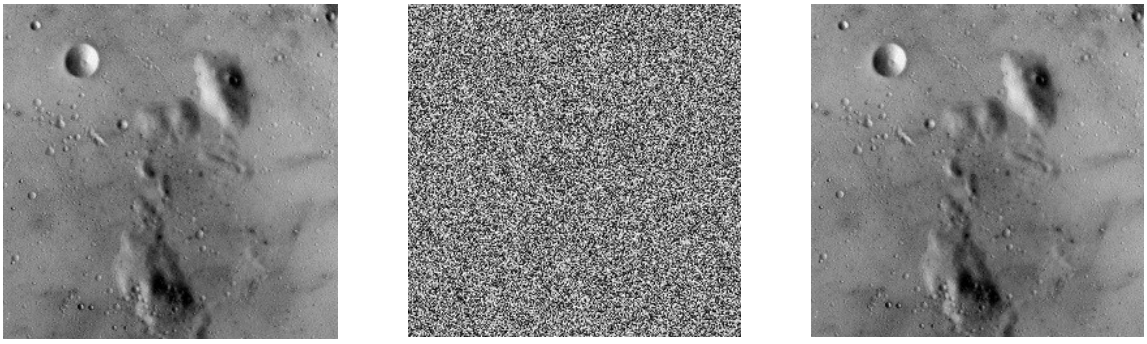


Fig. 4. Encryption/decryption diagram of the suggested algorithm.



(a) (b) (c)

Fig. 5. Results using the 2D-TentCM of the suggested algorithm: (a) Source Moon surface image (256 × 256), (b) Encrypted version of (a), and (c) Decrypted reconstruction of (b).

4.2. Histogram-Based Evaluation

It is a widely used method to investigate the statistical properties of natural images. When it comes to image encryption, a uniform histogram distribution is required as part of a defense against statistical attacks [10]. We show the results of such histogram analysis in Fig. 6 using the 'Boat' image at size 512 × 512 as an example. Quantitative evaluation of the histogram uniformity in the embedded image was conducted using the chi-square goodness-of-fit test. These p-values, given in Table 2, are greater than the conventional value of 0.05 and so should not significantly deviate from a uniform distribution. It is clear that this confirms the ability of the suggested encryption method to produce statistically uniform histograms, and hence grants robustness against statistical attacks.

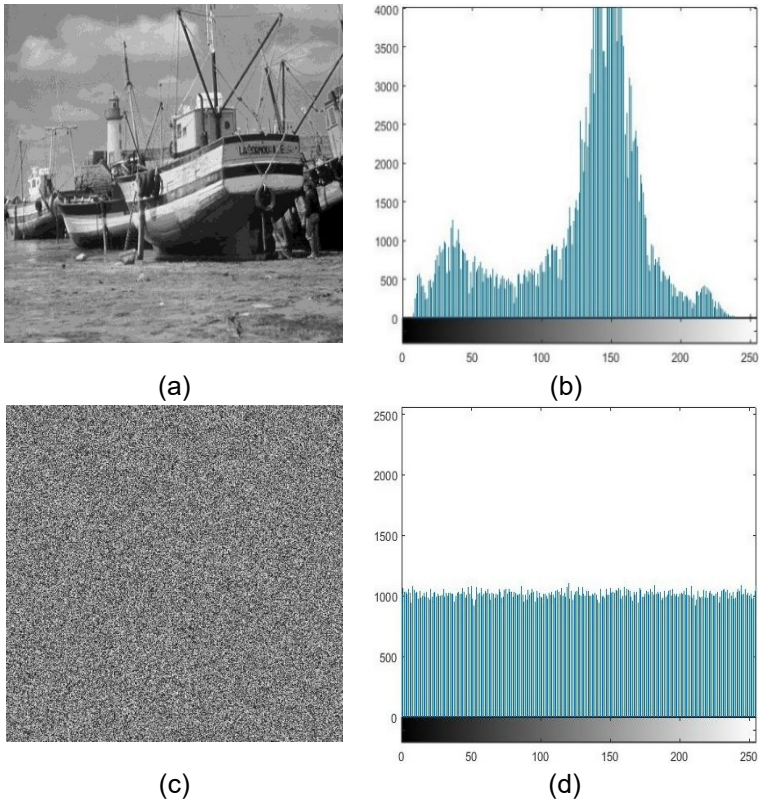


Fig. 6. Analysis of the histogram for the 'Boat' image (512 × 512 pixels); a) Source image; b) Histogram of the Source image; c) Encrypted image; d) Histogram of the encrypted image.

Table 2. Chi-square test comparisons between the source and encrypted images generated by Algorithm 1.

Image	χ^2(Source Image)	P-Value	χ^2(Encrypted Image)	P-Value
5.1.09 (256×256)	135687.57	0	251.38	0.5523
5.2.09 (512×512)	441857.81	0	228.63	0.8811
5.3.01 (1024×1024)	709340.68	0	259.68	0.4069

4.3. NIST Statistical Test Analyses

To rigorously analyze the randomness degree of encrypted images, the NIST SP800-22 statistical test suite was utilized. It is Extensively recognized for assessing binary sequences to determine whether they exhibit characteristics of true randomness-a critical property for secure crypto-graphic systems. In this study, 100 images were encrypted using the suggested 2D-TentCM chaotic encryption algorithm. The resulting ciphertexts were converted into binary streams and subjected to the NIST test suite. Each test returns a proportion value representing how many sequences out of 100 passed and a result indicating the overall result

based on the NIST criteria (typically, passing proportion > 96%). A p-value greater than 0.01 indicates that the null hypothesis of randomness is not rejected. Table 3 shows the results of 15 most frequent tests in NIST. All tests showed a strong success rate, with the Runs, FFT, and Random Excursion Variant tests. For most tests, the proportions are greater than 97%, which means that they have a very strong resistance to statistical attacks and show that the encrypted image acts like high entropy random sequences. Such results certainly reinforce the effectiveness of the 2D-TentCM algorithm for producing encrypted images without easily identifiable patterns and meeting the common notion of randomness.

Table 3. NIST statistical test results for 100 encrypted images using the 2D-TentCM algorithm.

Test	Proportion	p-value	Result
Frequency monobit	97/100	0.0812	✓
Block frequency	98/100	0.3607	✓
Runs	100/100	0.7483	✓
Longest runs	98/100	0.2662	✓
Rank	97/100	0.4115	✓
FFT	100/100	0.7180	✓
Cumulative sums	97/100	0.1903	✓
Random excursion	50/51	0.4194	✓
Random excursion variant	51/51	0.2691	✓
Approximate entropy	99/100	0.3152	✓
Universal	97/100	0.2913	✓
Serial	97/100	0.3709	✓
Linear complexity	98/100	0.2631	✓
Non-Overlapping templates	98/100	0.3001	✓
Overlapping templates	99/100	0.5207	✓

4.4. Key space analysis

A sufficiently vast key space is a critical factor in increasing protection against brute force attacks. In the case of the suggested 2D-TentCM algorithm, secret keys are obtained through the key mixing proportion technique, which contributes to a significantly vast key space. There are about 10^{14} possible values for each of the five parameters, resulting in a total key space of $(10^{14})^5 \approx 10^{70}$. Converting this to a binary representation yields $log_2\ 10^{70} \approx 232.5$ bits , or roughly 2^{232}. It is much greater than 2^{128}. According to field research, a key space of no less than 2^{128} is essential to ensure adequate resistance to such attacks [11].

4.5. Adjacent Pixel Correlation Analysis

A correlation analysis in image encryption usually measures how well the encryption has decorrelated neighboring pixel values (horizontal, vertical, and diagonal). If encryption is strong, it should be near zero. High correlation is observed between adjacent pixels in the source image. So, an effective encryption algorithm must minimize this correlation. Performance is evaluated by computing the correlation coefficients in the three known directions. The correlation coefficient cc for adjacent pixels is computed using the formula given in [12]: $cc = \frac{E[(c_1 - E(c_1))(c_2 - E(c_2))]}{\sqrt{D(c_1)}\sqrt{D(c_2)}}$ (5)

where $E(c_1)$ and $E(c_2)$ are the expected values of c_1 and c_2, and $D(c_1)$, $D(c_2)$ are their variances.

A total of 3000 adjacent pixel pairs were drawn at random from the two images, the source and encrypted images. The cc is calculated in all directions to analyze the relationship among neighboring pixels. As shown in Table 4, high correlation coefficients are observed in the source image, indicating strong pixel dependency, typically close to 1 in all directions, indicating strong pixel similarity. Following encryption via the suggested algorithm utilizing the 2D-TentCM, the correlation coefficients decrease dramatically, approaching zero in all directions. Similarly, as illustrated in Fig. 7, the 'Male' image reveals significant adjacent pixel dependency in the original image (correlation close to 1), whereas this dependency is effectively eliminated in the encrypted image (correlation close to 0). These results verify that the encryption process efficiently disrupts the inherent pixel relationships, thereby improving the security and randomness characteristics of the encrypted image. The near-zero correlation values serve to validate the strong diffusion capability of the suggested algorithm and its protection against statistical attacks.

Table 4. Correlation evaluation of neighboring pixels in the source and encrypted images processed by the suggested algorithm.

Image	Source Image			Encrypted Image		
	H	V	D	H	V	D
Moon Surface (256 × 256)	0.9104	0.9419	0.9095	-0.0457	0.0040	-0.0012
Aerial (512 × 512)	0.9007	0.8593	0.8121	-0.0092	-0.0127	-0.0233
Male (1024 × 1024)	0.9756	0.9778	0.9665	0.0228	-0.0296	0.0009

4.6. Entropy-Based Analysis

Information entropy is a key measure for assessing the randomness and unpredictability of encrypted images. In an ideal case, a perfectly encrypted image should attain an entropy value close to the theoretical upper limit of 8, applicable to 8-bit grayscale images, indicating that each pixel value is uniformly distributed and contains the maximum uncertainty. To quantify the information entropy E(m) of the image, the following formula is employed [13]:

$$E(m) = -\sum_{i=0}^{255} p(m_i) log_2 p(m_i) \quad (6)$$

where $p(m_i)$ indicates the probability that the pixel value mi occurs in the image.

To evaluate the efficiency of the proposed algorithm using 2D-TentCM, source image and encrypted image entropies were measured. The results, presented in Table 5, demonstrate that the source images have entropy values significantly lower than 8, due to the inherent redundancy and structure of natural images. In contrast, the encrypted images exhibit entropy values very close to 8, implying a nearly uniform spread of pixel intensity values. A comparative analysis of the entropies for the two standard test images, encrypted with the suggested 2D-TentCM algorithm and several recent algorithms, is presented in Table 6. The results demonstrate that the suggested algorithm reliably gives entropies closest to the maximum of 8 for both the 'Lena' and 'Peppers' images. Specifically, our algorithm yields entropy values of 7.9994 for Lena and 7.9993 for Peppers, outperforming the algorithms suggested in [14 - 17]. The increased entropy signifies that the encrypted images exhibit near-uniform pixel intensity distributions, demonstrating the superior randomness and statistical security offered by our approach.

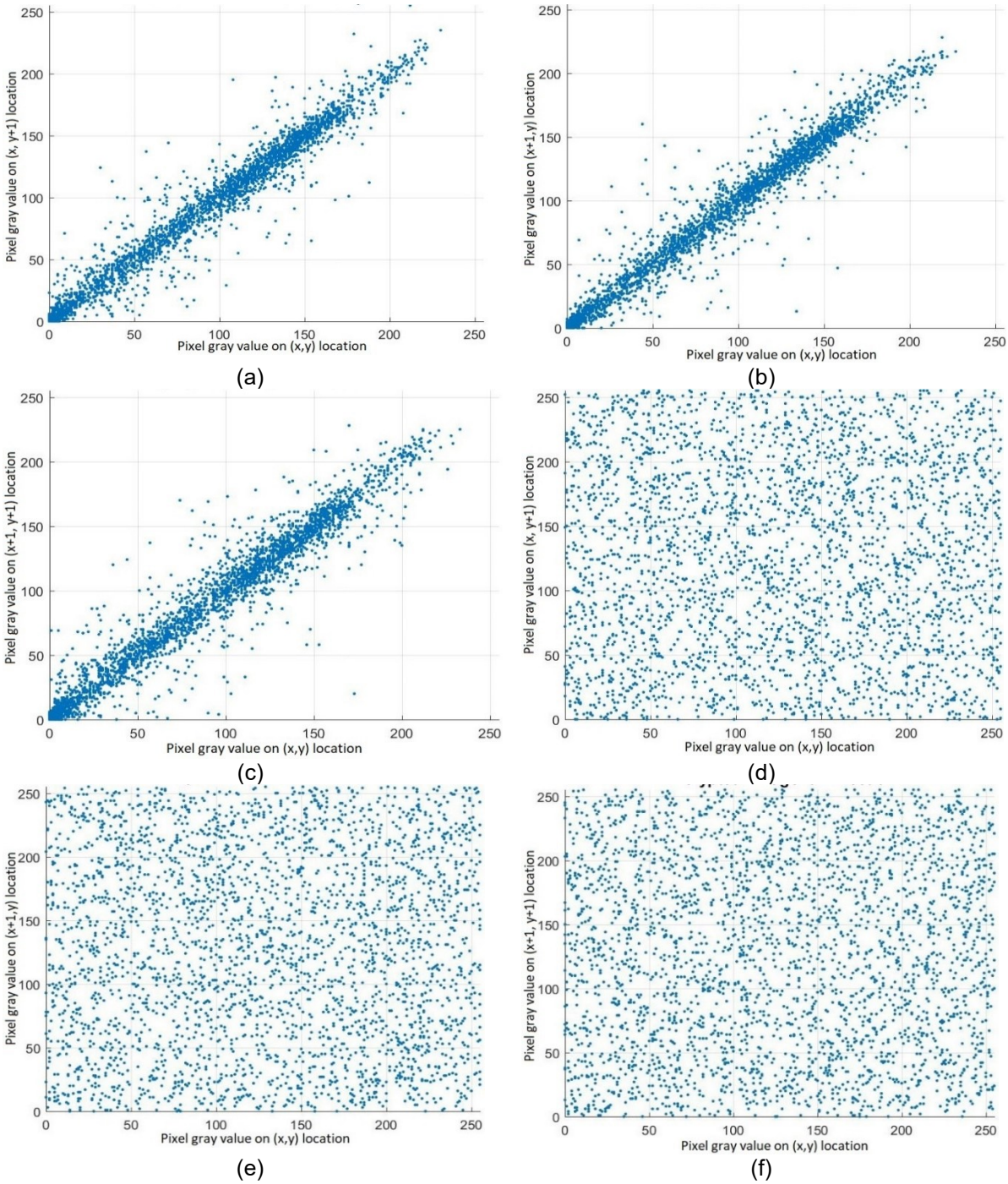


Fig. 7. Correlation analysis: The correlation coefficients between neighboring pixels for the 'Male' image in a) horizontal; b) vertical; and c) diagonal directions, and for its encrypted version in d) horizontal; e) vertical; and f) diagonal directions.

Table 5. Results of information entropy for the source and encrypted images evaluated via Algorithm 1.

Image	Source Image	Encrypted Image
Moon Surface	6.7093	7.9972
Aerial	6.9940	7.9994
Male	7.5237	7.9998

Table 6. Comparison of information entropy performance between the suggested algorithm and recent algorithms.

Image	Suggested algorithm	[17]	[16]	[15]	[14]
Lena$_{(512\times512)}$	**7.9994**	7.9989	7.9977	7.9970	7.9914
Peppers$_{(512\times512)}$	**7.9993**	7.9987	7.9976	7.9971	7.9915

4.7. Sensitivity to Key Variations

Key sensitivity analysis examines the robustness of an encryption algorithm by contrasting the decrypted image obtained with the correct key against that produced using a slightly altered key on the same encrypted image. This test verifies that minor changes to the correct key lead to noticeably inconsistent decryption results, confirming the algorithm's sensitivity to key variations. Two commonly employed metrics for this assessment are the number of pixels change rate (NPCR) and the unified average change intensity (UACI). These metrics quantitatively measure how sensitive the decryption process is to small key variations and can be computed mathematically as described in [18].

$$NPCR = \frac{1}{M \times N} \sum_{i,j} D(i,j) \times 100\% \quad (7)$$

$$UACI = \frac{1}{255 \times M \times N} \sum_{i,j} |E_1(i,j) - E_2(i,j)| \times 100\% \quad (8)$$

Where

$$D(i,j) = \begin{cases} 0 & if\ E_1(i,j) = E_2(i,j) \\ 1 & if\ E_1(i,j) \neq E_2(i,j) \end{cases} \quad (9)$$

The images E_1 and E_2 are produced using the suggested 2D-TentCM algorithm, applied to the source image and to a version modified by a single-pixel change, respectively. An analysis is conducted on the suggested Algorithm 1 to assess its key sensitivity and resistance to differential cryptanalysis. NPCR and UACI metrics were measured using various standard test images, such as 'Moon surface', 'Aerial', and 'Male'. Each original image was modified by a single-pixel change, and the resulting encrypted outputs were compared. Table 7 shows that the mean NPCR for all images is roughly 99.60%, and the mean UACI consistently aligns with the ideal theoretical value of 33.46%. The average NPCR and UACI values achieved by the suggested algorithm, along with those from various existing encryption techniques, are summarized in Table 8. These findings indicate that even a minimal alteration in the input image propagates to produce considerable and widespread effects on the encrypted result. Consequently, the suggested algorithm demonstrates strong diffusion capability and provides robust resistance against differential attacks.

Table 7. Key sensitivity results.

Image	NPCR [%]	UACI [%]
Moon Surface	99.63	33.44
Aerial	99.59	33.45
Male	99.60	33.49
Average	**99.61**	**33.46**

Table 8. Average NPCR and UACI values for encrypted images: performance of the suggested algorithm compared with other state-of-the-art algorithms.

Image	NPCR [%]	UACI [%]
Ours	99.61	33.44
[19]	100	33.37
[20]	99.61	33.29
[21]	99.58	33.11

4.8. Randomness Assessment Using the Run Test

It is a statistical technique employed to determine whether a binary sequence exhibits truly random behavior [22]. In image encryption, this test is commonly employed to examine

the statistical randomness within pixel intensity distributions or binary patterns in encrypted images. The term ”run” refers to a consecutive sequence of identical bits (either 0s or 1s) bounded by differing bits or the ends of the sequence. The test compares the observed number of runs to the expected value under the hypothesis of randomness. A notable deviation can not only imply a nonrandom property, but also infer the weakness of the encryption scheme. Successfully passing the Run’s test implies that the encrypted data closely resembles random noise, which is a critical feature to ensure encryption security. In MATLAB, the runstest function is used to perform this analysis. The results of several standard test images, summarized in Table 9, show that the encrypted outputs consistently pass the Run’s Test. This confirms that the suggested algorithm effectively produces encrypted images with significant randomness, enhancing resistance to statistical and pattern-based attacks.

Table 9. Analysis of the Run Test applied to test images.

Image	Moon surface	Aerial	Male
Test results	0	0	0
Randomness	Pass	Pass	Pass

4.9. Noise Attack Analysis

In practical encrypted image communication, the transmitted images are usually deteriorated by noise (e.g., Salt&Pepper and Gaussian noises). A practical secure image encryption algorithm should be robust under these cases, that is the recovered images should be intelligible when partial and/or temporal corruption occurs. To investigate the security performance of the suggested 2D-TentCM algorithm, multiple kinds and intensities of noise were introduced into the encrypted images.

These noisy encrypted images were then decrypted using the original key, and the quality of the resulting images was assessed both visually and quantitatively. Robustness was quantitatively analyzed using two widely adopted metrics: Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). MSE evaluates the squared pixel differences between source and decrypted images, where reduced values correspond to improved reconstruction fidelity. Expressed in dB, PSNR quantifies the effect of noise on an image, with larger values corresponding to improved visual quality. As shown in Table 10 and Fig. 8, although the visual quality of decrypted images degrades as noise intensity increases, the structural content and essential features remain largely intact. The relatively low MSE and consistently acceptable PSNR values under various noise scenarios demonstrate the robustness of the supposed algorithm. This property is important in practical applications where images may be sent over noisy channels or stored on imperfect media.

Table 10. MSE and PSNR comparison of decrypted images produced by the suggested algorithm and selected existing methods under noise attacks.

Noise	Ours		[23]		[24]	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Gaussian ($\mu = 0$, $\sigma^2 = 0.1$)	4684.6	11.4	5201.2	11.0	5272.1	10.9
Gaussian ($\mu = 0$, $\sigma^2 = 0.01$)	1994.7	15.1	2321.4	14.5	2348.4	14.4
Salt&Pepper (d=0.1)	793.2	19.1	893.1	18.6	909.3	18.5
Salt&Pepper (d=0.05)	390.8	22.2	437.9	21.7	444.1	21.7

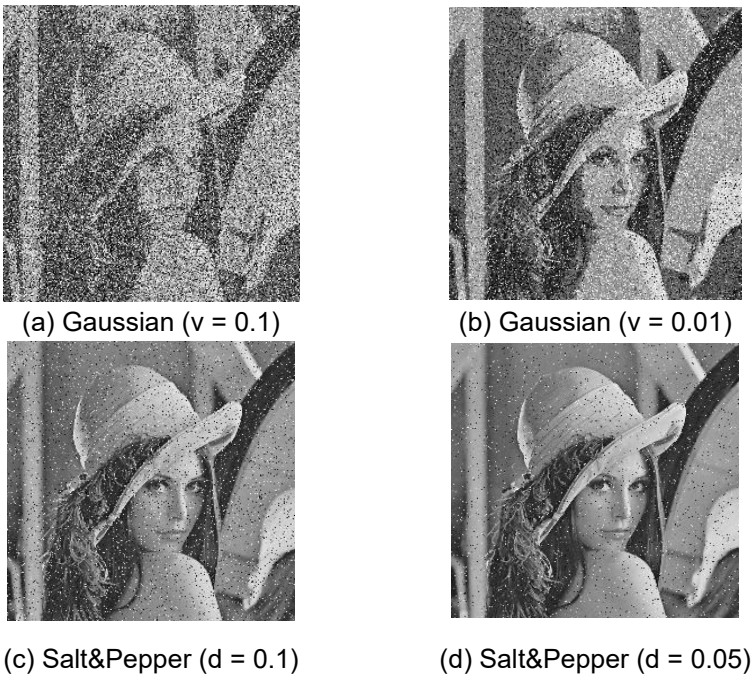


Fig. 8. Lena (256 × 256) images retrieved after decryption when the encrypted image is corrupted with multiple kinds of noise.

4.10. Analysis of Known/Chosen Plaintext Attack via Structured Pattern Encryption

Known-plaintext attacker (KPA): The attaker has obtained one or more plaintext-ciphertext pairs and uses them to determine the secret key or otherwise break future encryptions. In our scheme, the session keys/initial conditions are derived from the plaintext itself (besides secret parameters). Hence, each plaintext produces a different effective keystream even if the underlying secret parameters are the same. This design makes direct key recovery from a single plaintext-ciphertext pair ineffective.

To verify the chosen plaintext attack (CPA) resistance of the suggested 2D-TentCM encryption method, a pattern-oriented analysis is performed. This method tests whether predictable or structured patterns in the input images lead to detectable patterns in the corresponding ciphertexts. In this experiment, several structured test images were used, including all-zero, all-one, horizontal gradient, and checkerboard patterns. These images are specifically designed to reveal any potential structural leakage during encryption. If the ciphertext (encrypted image) preserves any visual or statistical traces of the input structure, the algorithm may be vulnerable to CPA. Structured images were encrypted via the suggested algorithm, and the resulting ciphertexts were visually inspected and statistically analyzed. Histograms corresponding to the encrypted images were also examined to assess the uniformity of the pixel value distributions. The experiment results show that the noise-like feature of the source image can be retained in the encrypted images irrespective of the shape of its configuration. Besides, the histograms of all encrypted images are relatively uniform, which means that the encryption algorithm can make most clear structures in the source image undetectable to the eye. This analysis provides additional evidence for the resistance of the suggested algorithm against CPA and its power to produce encrypted images with high randomness and lack of distinguishable patterns. To verify the resistance of the suggested 2D-TentCM algorithm to CPA, multiple structured test images- specifically, an all-zero image, an all-one image, a horizontal gradient, and a checkerboard pattern were encrypted and

analyzed. These images were deliberately selected to expose potential structural vulnerabilities in the encryption scheme. Visual inspection of the resulting ciphertexts reveals completely noise-like patterns, with no observable remnants of the original structures. Moreover, histogram analysis, as illustrated in Fig. 9, confirms that the pixel intensity distributions in the encrypted images are nearly uniform. This evidence supports that the algorithm successfully hides the statistical features of the input data. Collectively, the results confirm the robustness of the suggested algorithm against CPA scenarios, as it prevents even highly structured plaintexts from producing predictable or exploitable patterns in the ciphertext.

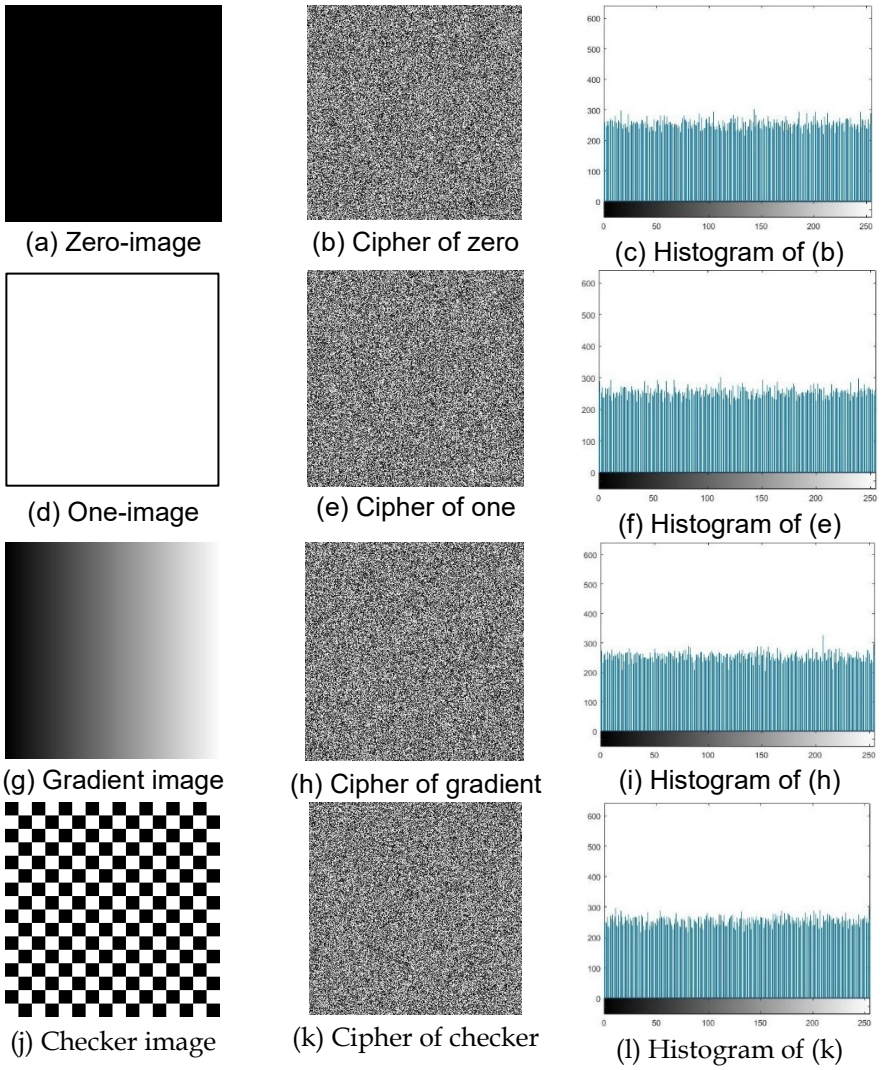


Fig. 9. CPA analysis for several structured test images.

4.11. Computational Cost

The computational efficiency of an encryption algorithm is very essential for its real-world applications, such as in medical imaging, wireless communication and embedded systems. Thereby, the metric includes both the ability to order things in time and to allocate resources that would influence its scalability and usability. To check the computational efficiency of the suggested algorithm, encryption/decryption time was computed for typical grayscale images with different sizes. The experiments were conducted on a computer (Intel Core i5 2.20GHz, 8GB RAM, MATLAB R2016b) and each experiment was repeated sufficiently

to ensure reliable average performance. The results are summarized in Table 11, which shows that the suggested algorithm is computationally least expensive in terms of encryption/decryption. The efficiency of the suggested cryptosystem is due to the lightweight nature of the considered chaotic map and the efficient implementation of the confusion and diffusion processes. In general, based on strong security and low computational complexity, the suggested algorithm is suitable for high-level security applications, even performance-critical ones.

Table 11. Time taken by the suggested 2D-TentCM algorithm to encrypt/decrypt images (cameraman) of varying sizes.

Image size	Enc. Time [s]	Dec. Time p[s]
256 × 256	0.0357	0.0434
512 × 512	0.1422	0.1809
1024 × 1024	0.5692	0.7580

5. BENCHMARKING AGAINST AES AND CHAOS-BASED ALGORITHMS

For performance and security evaluation, the proposed 2D-TentCM image encryption scheme is compared with AES-128 (CBC mode with random IV) and two representative recent chaos-based image encryption schemes with the same test images and metrics. The comparison was made on a standard image set and evaluated using: (i) peak signal-to-noise ratio (PSNR); (ii) histogram uniformity, correlation coefficients of adjacent pixels, information entropy, and NPCR/UACI to measure resistance to statistical and differential attacks; and (iii) encryption/decryption throughput (MB/s). Table 12 shows the performance comparison of the proposed algorithm, AES and two recent chaos-based algorithms [17] and [25]. As can be seen from Table 12, the proposed algorithm can generate the cipher images with very strong statistical properties for all the three test images. The entropy values are near to 8 and the adjacent-pixel correlation coefficients are near to zero, which shows that the cipher images are highly random and the visible structural information of the plain image has been removed successfully. Also, after decryption by the proposed method, MSE = 0 is achieved which proves the perfect reversibility and lossless recovery of the original images. The results for differential-security are also impressive. The proposed method for Boat, Peppers and Lena achieves NPCR values of 99.6170%, 99.6357% and 99.6216% respectively. The corresponding UACI values are 33.4781%, 33.5677% and 33.4965%. These values are close to the ideal levels in image encryption, which shows that even a very small change in the plain image gives rise to a major change in the cipher image. The proposed method is much more differentially sensitive than AES because AES has significantly lower NPCR and UACI values in this experimental setting. The proposed algorithm is still very competitive compared with the recent chaos-based schemes in [17] and [25]. It compares well or is slightly better in entropy and correlation results. It also keeps the NPCR and UACI values near the theoretical ideals. Although AES is much faster in decryption and encryption, the proposed approach offers better security-computational efficiency tradeoff than the chaos-based references especially for applications where statistical security and the plain image sensitivity are more important than the raw speed. The main limitations of the present work, including the dependence on carefully chosen ranges of parameters.

Table 12. Performance comparison of the proposed algorithm with AES and recent chaos-based schemes using identical test images, showing entropy, adjacent-pixel correlation, NPCR, UACI, and encryption/decryption time.

Image	Metric	Our	AES	[17]	[25]
Boat 512 × 512	Entropy	7.9993	7.9992	--	7.9992
	Correlation	0.00003	-0.0027	--	0.0089
	MSE	0	0	--	0
	NPCR [%]	99.6170	74.5896	--	99.6188
	UACI [%]	33.4781	16.6661	--	33.5461
	Enc./Dec. Time [s]	0.1523/0.1948	0.0053/0.0043	--	0.5589/0.5484
Peppers 512 × 512	Entropy	7.9993	7.9992	7.9987	7.9993
	Correlation	-0.0032	-0.0038	--	0.0084
	MSE	0	0	15.42	0
	NPCR [%]	99.6357	74.3145	--	99.5984
	UACI [%]	33.5677	16.6410	--	33.3374
	Enc./Dec. Time [s]	0.1435/0.1939	0.0043/0.0048	--	0.5660/0.5620
Lena 512 × 512	Entropy	7.9994	7.9993	7.9989	7.9992
	Correlation	0.0003	0.0009	0.0003	0.0189
	MSE	0	0	14.82	0
	NPCR [%]	99.6216	74.3359	--	99.6195
	UACI [%]	33.4965	16.5897	--	33.4312
	Enc./Dec. Time [s]	0.1458/0.1952	0.0057/ 0.0044	--	0.5785/0.5556

6. CONCLUSIONS

In this paper, we have presented an image encryption algorithm based on the 2D-Tent chaotic map and confirmed the effectiveness of our proposal by numerical simulation. Generalized from the Tent map, the suggested algorithm generalizes the one-dimensional Tent map into two dimensions to generate pseudo-random sequences with significantly enhanced complexity, improved randomness, and an increased key space. The suggested algorithm shows strong robustness against brute-force attacks by using the key mixing proportion to enhance system parameter initialization and it has a huge key space of approximately 1070. The correlation coefficients of the ciphertext image are almost zero in three directions; its NPCR is close to 99.60%, and UACI attains approximately 33.46% with the entropy being 7.9994. The theoretical analysis presented here, as well as the extensive sensitivity testing of both key-recovery and modification-based cryptanalysis, establishes that the suggested 2D-TentCM encryption algorithm is secure and computationally strong compared to previous algorithms. In summary, the experimental results illustrate that the suggested algorithm is a good choice for secure and efficient image encryption. Future studies may enhance the suggested encryption algorithm by incorporating a multi-dimensional chaotic system and using quantum-inspired cryptographic techniques for stronger security against advanced cryptanalysis attacks.

Acknowledgement: I wish to extend my heartfelt thanks to Mr. Mohamed Ishtiaq for his significant support in editing and proofreading this paper.

REFERENCES

[1] Y. Alghamdi, A. Munir, "Image encryption algorithms: a survey of design and evaluation metrics," *Journal of Cybersecurity and Privacy,* vol. 4, pp. 126-152, 2024, doi: 10.3390/jcp4010007.

[2] U. Zia, M. McCartney, B. Scotney, J. Martinez, J. AbuTair, J. Memon, A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, pp. 917-935, 2022, doi: 10.1007/s10207-022-00588-5.

[3] N. Pareek, V. Patidar, K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926-934, 2006, doi: 10.1016/j.imavis.2006.02.021.

[4] C. Li, G. Luo, K. Qin, C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, pp. 127-133, 2017, doi: 10.1007/s11071-016-3030-8.

[5] R. Raj, S. Paul, "Image encryption using chaotic maps of various dimensions: review," *International Journal of Engineering Research & Technology*, vol. 5, no. 4, pp. 94-96, 2016, http://ijret.esatjournals.org.

[6] A. JarJar, "Image encryption using hybrid cryptographic system incorporating three improved standards," *Sensing and Imaging*, vol. 22, no. 37, 2021, doi: 10.1007/s11220-021-00358-y.

[7] Y. Ma, C. Li, B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications,* vol. 54, pp. 102566, 2020, doi: 10.1016/j.jisa.2020.102566.

[8] E. Yavuz, R. Yazıcı, M. Kasapbasi, E. Yamac, "A chaos-based image encryption algorithm with simple logical functions," *Computers & Electrical Engineering,* vol. 54, pp. 471-483, 2016, doi: 10.1016/j.compeleceng.2015.11.008.

[9] M. Eltoukhy, F. Alsubaei, Y. Elnabawy, K. Hosny, "Multiple image encryption techniques: Strategies, challenges, and potential future directions," *Alexandria Engineering Journal*, vol. 25, pp. 367-387, 2025, doi: 10.1016/j.aej.2025.04.006.

[10] P. Andono, "Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption," *IEEE Access*, vol. 10, pp. 115143-115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[11] X. Liu, Q. Chen, R. Zhao, G. Liu, S. Guan, L. Wu, X. Fan, "Quantum image encryption algorithm based on four-dimensional chaos," *Frontiers in Physics*, vol. 12, pp. 1230294, 2024, doi: 10.3389/fphy.2024.1230294.

[12] R. Gonzalez, R. Woods, "Digital Image Processing," New York, USA: Pearson, 330 Hudson street. New York, NY 10013, 2018.

[13] X. Wang, Y. Zhang, X. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015, doi: 10.1016/j.optlaseng.2015.03.022.

[14] L. Teng, X. Wang, F. Yang, Y. Xian, "Color image encryption based on cross 2d hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dynamics*, vol. 105, pp. 1859-1876, 2021, doi: 10.1007/s11071-021-06663-1.

[15] X. Yan, X. Wang, Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and dna encoding operation," *Multimedia Tools and Applications*, vol. 80, pp. 10949-10983, 2021, doi: 10.1007/s11042-020-10218-8.

[16] S. Zhou, Y. Qiu, X. Wang, Y. Zhang, "Novel image cryptosystem based on new 2d hyperchaotic map and dynamical chaotic s-box," *Nonlinear Dynamics,* vol. 111, pp. 9571-9589, 2023, doi: 10.1007/s11071-023-08312-1.

[17] M. Liu, C. Ning, C. Zhu, "A secure image encryption scheme based on a new hyperchaotic system and 2d compressed sensing," *Entropy,* vol. 26, no. 7, pp.603, 2024, doi: 10.3390/e26070603.

[18] C. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal,* vol. 27, no. 3, pp. 379-423, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[19] D. Singh, H. Kaur, C. Verma, N. Kumar, Z. Ill´es, "A novel 3-d image encryption algorithm based on sha-256 and chaos theory," *Alexandria Engineering Journal,* vol. 122, pp. 564-577, 2025, doi: 10.1016/j.aej.2025.03.026.

[20] R. Chu, S. Zhang, X. Gao, "A novel 3d image encryption based on the chaotic system and RNA crossover and mutation," *Frontiers in Physics*, vol. 10, pp. 844966, 2022, doi: 10.3389/fphy.2022.844966.

[21] T. Liu, H. Yan, S. Banerjee, J. Mou, "A fractional-order chaotic system with hidden attractor and self-excited attractor and its dsp implementation," *Chaos, Solitons & Fractals*, vol. 145, pp. 110791, 2021, doi: 10.1016/j.chaos.2021.110791.

[22] D. Singh, S. Kumar, "A multiphase encryption scheme using RSA, modified RMAC and CHEN's hyperchaotic map," *Multimedia Tools and Applications*, vol. 83, pp. 57059-57088, 2024, doi: 10.1007/s11042-023-17727-2.

[23] S. Askar, A. Karawia, A. Al-Khedhairi, F. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, no. 1, pp. 1-17, 2019, doi: 10.3390/e21010044.

[24] A. Karawia, "Image encryption based on fisher-yates shuffling and three-dimensional chaotic economic map," *IET Image Processing*, vol. 13, no. 12, pp. 2086-2097, 2019, doi: 10.1049/iet-ipr.2018.5142.

[25] M. Abdul-Hameed, H. El-Metwally, S. Askar, A. Alshamrani, M. Abouhawwash, A. Karawia, "Advanced color image encryption using third-order differential equations and three-dimensional logistic map," *AIP Advances*, vol. 14, no. 7, p. 075024, 2024, doi: 10.1063/5.0214794.