International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I11P103

Volume 74 Issue 11, 32-50, November 2026
© 2026 Seventh Sense Research Group®

Original Article

Adaptive Thermal Image Encryption using a Generalized Irrationality-Driven Chaotic Map (GIDCM)

Vinay Kumar Sharma[1], Janki Ballabh Sharma[2]

[1,2]*Department of Electronics Engineering, Rajasthan Technical University, Kota, Rajasthan, India.*

[1]*Corresponding Author: vksharma.phd17@rtu.ac.in*

Received: 24 April 2026 Revised: 18 August 2026 Accepted: 26 August 2026 Published: 25 November 2026

Abstract - *The paper introduces a new thermal image encryption algorithm that is built on a two-dimensional Generalized Irrationality-Driven Chaotic Map (GIDCM). The suggested map builds on the conventional irrational-number-based chaotic systems by providing generalized irrational parameters, enhancing dynamical complexity and flexibility of parameters. An adaptive key-generation mechanism is used to produce image-specific secret parameters, which increases sensitivity to the input image and secret keys. The proposed GIDCM generates three chaotic sequences, which are used in a multi-stage encryption scheme that consists of pixel-level scrambling, block-level permutation, and substitution. Because thermal images have continuous intensity changes and high inter-pixel correlation, the proposed approach is particularly aimed at successfully disrupting their spatial information, which is temperature-based. The bifurcation analysis, trajectory plots, sample entropy, permutation entropy, 01 tests and Lyapunov exponent are used to validate the chaotic characteristics of the proposed GIDCM. Comprehensive security evaluations demonstrate that the proposed scheme achieves high information entropy, negligible correlation between adjacent pixels, a large key space, strong key sensitivity, and robust resilience against statistical, differential, cropping, and noise attacks. The experimental findings confirm that the proposed method offers a secure and computationally efficient approach for thermal image encryption.*

Keywords - *Adaptive key generation, Generalized Irrationality-Driven Chaotic Map (GIDCM), Multistage image encryption, Pixel permutation and substitution, Thermal image encryption.*

1. Introduction

As the infrared sensing and thermal imaging technologies have rapidly developed, thermal images are becoming more commonly utilized in surveillance, military surveillance, intelligent transportation, industrial inspection, medical diagnosis, and border security systems [1]. In contrast to the common visible images, thermal images are the representation of the temperature distribution of a scene and are typically defined by the smooth intensity variations, reduced contrast, and high inter-pixel correlation [2]. Although these characteristics improve object detection under poor lighting and adverse weather conditions, they also make thermal images more vulnerable to unauthorized access and statistical attacks during storage and transmission. Thus, the design of secure thermal image encryption algorithms has been a significant research issue in recent years [3].

Over the last decade, there have been considerable advances in the creation of new chaotic maps to securely encrypt images. Researchers have proposed one-dimensional, two-dimensional, and hyperchaotic systems that are more random and have larger parameter space [4, 5]. Several nonlinear models have been proposed that are logistic maps, sine maps, tent maps, Henon maps, fractional-order systems, coupled maps, and irrational-number-driven systems to increase the security and complexity of image encryption techniques [6]. Specifically, 2D eπ-map [7] proposed the application of irrational numbers as a useful method of enhancing unpredictability and parameter variety of chaotic systems.

Inspired by these advancements, this work introduces a new two-dimensional Generalized Irrationality-Driven Chaotic Map (GIDCM) to encrypt thermal images in a secure manner. The suggested map builds on the conventional chaotic structure of irrational numbers, adding generalized irrational parameters, which enhance the flexibility and the dynamical complexity of the system. Moreover, an adaptive key-generation scheme [8] is used to generate image-dependent secret parameters and thus increase the resistance to brute-force and chosen-plaintext attacks [9].

The proposed encryption framework integrates chaotic-sequence generation with multi-stage permutation and substitution. Firstly, the Arnold cat map and chaotic sequences computed through the proposed GIDCM are used to perform


This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

pixel-level and block-level scrambling. Afterward, diffusion processes are performed with the help of bitwise substitution to remove statistical data in the encrypted image. Given that thermal images have very correlated structures of temperature, the proposed method is specifically aimed at disrupting the spatial dependency and intensity distribution of thermal images.

The major contributions of this work are summarized below:

1. A new two-dimensional Generalized Irrationality-Driven Chaotic Map (GIDCM) is proposed by extending conventional irrational-number-based chaotic systems.
2. An adaptive image-dependent key-generation mechanism is developed to improve key sensitivity and security.
3. A multi-stage thermal image encryption framework is introduced, in which each encryption operation is adaptively derived from the characteristics of the input image.

The experimental results demonstrate that the proposed encryption algorithm provides strong randomness, low correlation, high key sensitivity, and robust resistance against statistical, differential, cropping, and noise attacks. Therefore, the proposed method offers an effective and secure solution for thermal image encryption.

Furthermore, the subsequent sections are structured as follows: Section 2 reviews the recently proposed chaotic maps-based image encryption algorithms, Section 3 outlines the proposed GIDCM, while Section 4 describes the adaptive image encryption scheme. The numerical simulation results are summarized in Section 5, and the comprehensive security analysis of the proposed method is provided in Section 6. Finally, the study is concluded in Section 7.

2. Review of Recently Proposed Chaotic Maps based Image Encryption Algorithms

Recently, many new chaotic maps are proposed for utilizing in cryptographic applications and having competitive performance in terms of security metrices [7, 10-18]. Brief summary of these chaotic maps is presented in Table 1. In study [17], introduce an image encryption algorithm that employs a novel 2D One-Dimensional Cosine Logistic Compound Chaotic map (1DCLC). This algorithm uses a layered scrambling approach to encrypt images, delivering exceptional results in security metrics and offering a highly reliable solution for safeguarding digital images.

A new 1D chaotic map, named the fractional chaotic map, is introduced by integrating the sine map with fractional operations [15]. This map exhibits an expanded range of chaotic parameters and enhanced chaotic properties, making it particularly well-suited for information encryption applications. Conventional chaotic map-based image encryption algorithms often struggle with limited scrambling capability, suboptimal dynamic behavior, and insufficient sensitivity. To overcome these issues, a new cross-channel color image encryption method is proposed that utilizes a 2D Rastrigin-Griewank (RG) hyperchaotic map. This method enhances encryption effectiveness through diagonal permutation and bi-directional sequential diffusion [11].

A new chaotic map, known as the Bessel map, is introduced based on the Bessel function. This map features three control parameters, offering enhanced ergodicity and diversity [10]. A novel 2D chaotic ep-map, by utilizing the infinite diversity of Euler and Pi numbers, is introduced in paper [7]. This map demonstrates exceptional hyperchaotic performance, excelling in ergodicity, complexity, and randomness.

In the study [16], A novel Two-Dimensional Chebyshev-Logistic-Infinite Collapse Map (2D-CLICM) is proposed, providing a larger chaotic region, enhanced randomness, and more complex chaotic behavior. A new hyperchaotic system, termed the 2D Rosenbrock map, is developed using the Rosenbrock function. This system features outstanding modular swinging characteristics, along with excellent ergodicity and diversity [14].

A novel Modular Integrated Logistic Exponential (MILE) map is introduced to address the limitations of existing chaotic maps, including their low performance and smaller ranges [12]. A new 2D hyperchaotic system, called the Schaffer map, showing superior ergodicity compared to existing methods [13]. To address the limitations of current chaotic maps, a new 2D Logistic Tent Modular Map (2DLTMM) is introduced to utilize in the development of a novel color image encryption algorithm named LTMM-CIEA [18].

All these newly developed chaotic maps depict the excellent chaotic behavior in a wider range of control parameters and have shown competitive, robust and reliable security performance in the image encryption algorithms.

However, these algorithms have been proven to be vulnerable to attacks and successfully cracked by researchers using plain text and cipher text attacks [9, 19-25]. The major problem of these compromised encryption algorithms is their fixed initial values and control parameters, which prevents them from adapting to variations in original images.

Consequently, these algorithms fail to achieve optimal encryption performance in terms of security metrics such as entropy, correlation coefficients, Net Pixel Change Ratio (NPCR) and Unified Average Change in Intensity (UACI) values evaluated across all original images. As a result, attackers can easily derive plaintext/ciphertext pairs and potentially predict the key [9].

Table 1. Recently developed chaotic maps and their properties

Ref.	Pub. Year	Chaotic map	Dimension	Control parameter range
[10]	2024	Bessel map	1D	$t, u, v \in [0, +\infty)$
[11]	2024	Rastrigin-Griewank (RG) map	2D	$a, b \in [0, 10]$
[12]	2024	Modular Integrated Logistic Exponential (MILE)	1D	$u, t \geq 0$
[14]	2023	Rosenbrock map	2D	$a \in (0,\infty)$, $b \in (3.1,\infty)$
[13]	2023	Schaffer map	2D	$a, b \in (0,\infty)$
[15]	2023	Fractional Chaotic Map	1D	$\mu > 1.063\times 10{-}4$
[16]	2023	Chebyshev-Logistic-Infinite Collapse Map	2D	$n \in [0, 4]$
[17]	2022	Cosine logistic compound chaotic map	1D	$\alpha \in [0, 6]$, $\beta \in [0, 1]$
[7]	2022	eπ-map	2D	$u \in [0, +\infty)$
[18]	2021	Logistic tent modular map	2D	$r \in [0, 1]$

3. Proposed Generalized Irrationality-Driven Chaotic Map (GIDCM)

In this work, a new two-dimensional Generalized Irrationality-Driven Chaotic Map (GIDCM) is introduced, inspired by eπ-map [7], which exhibits hyperchaotic behavior over a wide control range. A closer analysis of the eπ-map shows that its nonlinear dynamic behavior is not limited to two specific irrational constants, Euler and Pi numbers.

In fact, other irrational numbers can also be incorporated into the same mathematical structure to generate highly complex chaotic sequences with similar dynamical characteristics.

The proposed model, defined by Equation (1), extends the conventional eπ-map by replacing the fixed irrational constants with two generalized irrational parameters, denoted by γ_1 and γ_2. This generalization increases the flexibility of the system and provides a nonlinear framework for producing diverse and highly unpredictable random sequences, makes it suitable for secure image encryption applications.

The state variables X_i and Y_i represent the initial conditions of the map, while $u \in (0,\infty)$ is the control parameter. The modular operation is used to keep the generated outputs bounded within the interval [0, 1].

$$\begin{cases} X_{i+1} = \left((X_i)^{\gamma_2{}^3}\gamma_1{}^4 + uY_i\gamma_1{}^{10}\right) mod\ 1 \\ Y_{i+1} = \left((Y_i)^{\gamma_2{}^3}\gamma_1{}^4 + uX_{i+1}\gamma_2{}^9\right) mod\ 1 \end{cases} \quad (1)$$

3.1. Chaotic Performance Evaluation of Proposed 2D GIDCM

The performance of a chaotic map must be carefully examined to strengthen the security of the image encryption algorithm. Therefore, in this work, bifurcation analysis, trajectory plots, sample entropy, permutation entropy, 01 tests and Lyapunov exponent are employed to assess its dynamical behavior. For the experimental analysis, the irrational parameters γ_1 and γ_2 are selected as: $\gamma_1 = \sqrt{2} = 1.41421356237309504880$, $\gamma_2 = \sqrt{5} = 2.23606797749978969640$. These irrational values are used throughout all simulations and performance evaluations of the proposed GIDCM.

3.1.1. Bifurcation and Trajectory Diagrams

The bifurcation diagram describes the evolution of the values generated by a chaotic map with respect to the control parameter [13]. Bifurcation diagrams of proposed GIDCM, in comparison with classical logistic map, are shown in Figure 1.

It is apparent from the figure that the sequence points remain widely and irregularly distributed over a broad parameter range, without noticeable concentration in any specific region, indicating strong chaotic behavior.

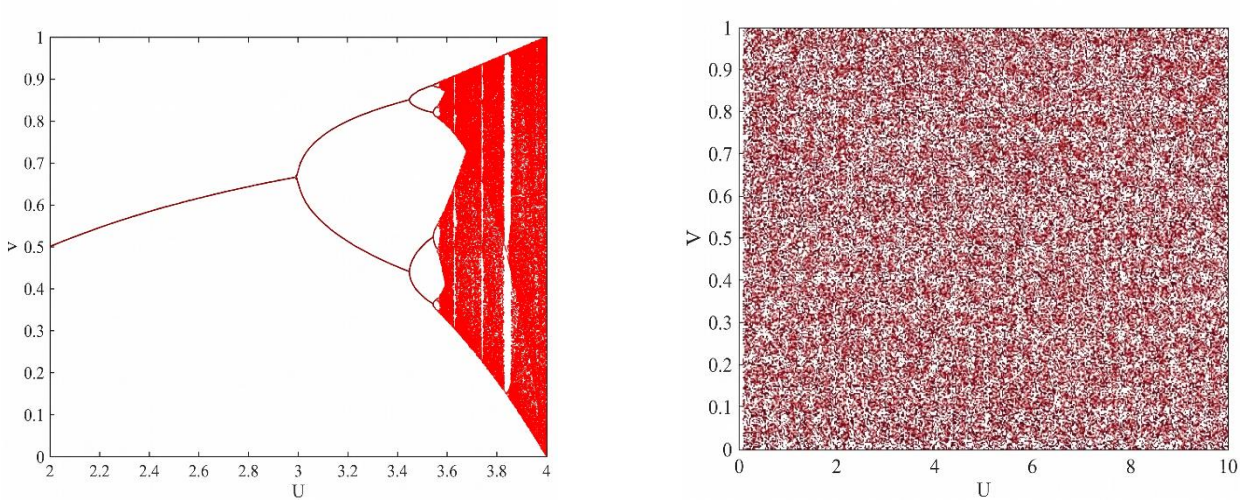
Furthermore, 2D and 3D trajectories of proposed GIDCM are also depicted in Figure 2. The 2D trajectory represents the points of sequence. Y_i versus X_i, while the 3D trajectory depicts the points of combined sequence v_{i+2} with v_{i+1} and v_i.

The distribution clearly shows that the points are uniformly distributed across the entire phase space, which further verifies the high dynamical complexity and effectiveness of the proposed map.

3.1.2. Lyapunov Exponent (LE)

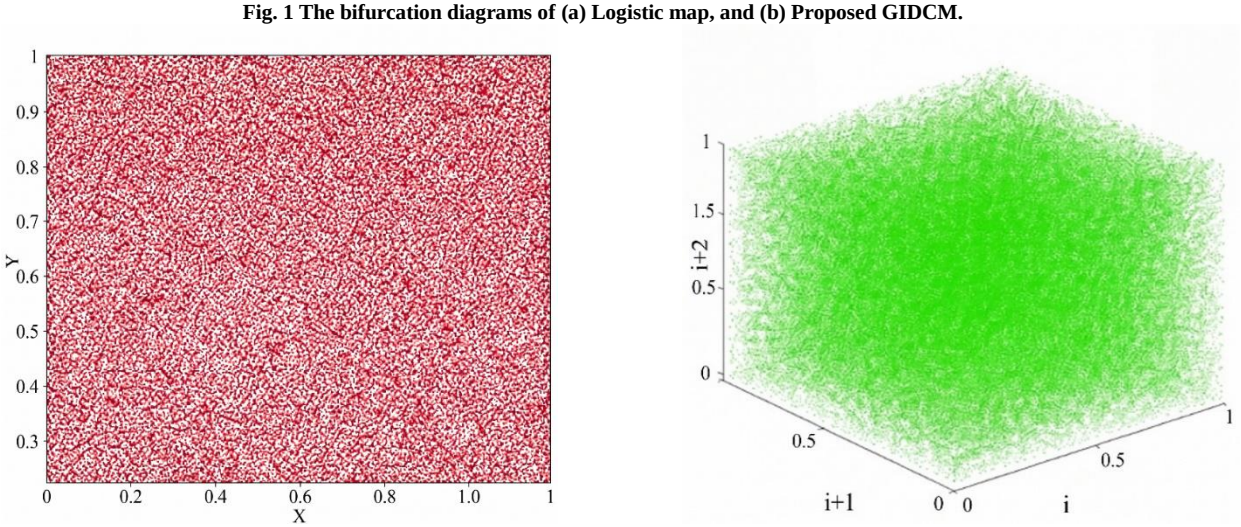
The Lyapunov Exponent (LE) [10] is a measure of the average rate of separation between two nearby trajectories as the system is driven. A positive LE signifies sensitivity to initial conditions and is a measure of chaotic behavior. Figure 3 is a comparison of the LE values of the proposed GIDCM and classical Henon and logistic maps.

The suggested map has positive LE values within a wider range of control parameters, showing more chaos and more sensitivity to the change of parameters. In comparison, the Henon and logistic maps have positive Lyapunov exponents only in smaller areas. These results confirm the superior chaotic dynamics of the proposed GIDCM, validating its suitability in secure image encryption applications.



(a) **(b)**

Fig. 1 The bifurcation diagrams of (a) Logistic map, and (b) Proposed GIDCM.



(a) **(b)**

Fig. 2 The trajectory diagrams of proposed GIDCM (a) 2D trajectory, and (b) 3D trajectory.

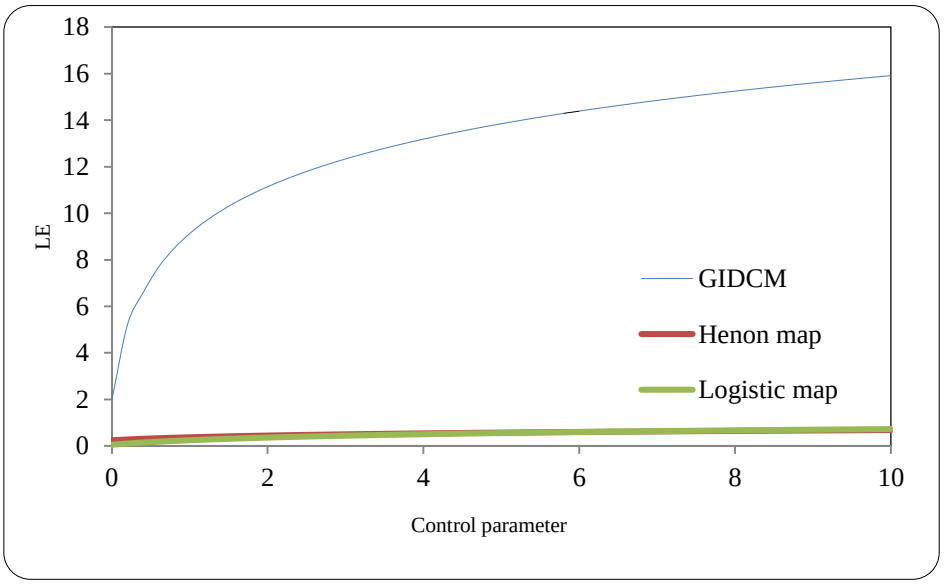


Fig. 3 Comparison of the largest Lyapunov Exponent (LE) of the proposed GIDCM with the Henon map and logistic map

3.1.3. Sample Entropy (SE)

Sample Entropy (SE) [14] is a measure of the irregularity and randomness of a chaotic sequence, with larger values of SE indicating greater complexity. Figure 4 compares the SE values of the GIDCM with the Henon map. It is possible to note that the proposed GIDCM has much higher values of SE over the whole range of control parameters, with an average of about 2.19, compared to much lower values of the Henon map with an average of about 0.46. These findings suggest that GIDCM produces more complex and unpredictable random sequences, making it effective for secure image encryption.

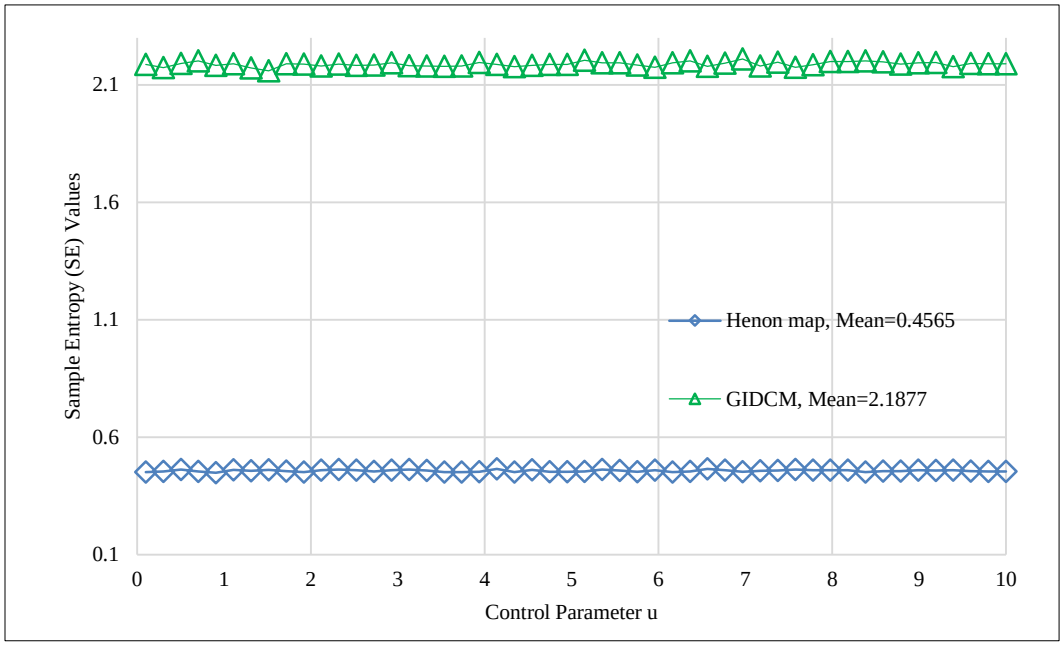


Fig. 4 The comparison of Sample Entropy (SE) values of proposed GIDCM with state-of-the-art Henon map

3.1.4. Permutation Entropy (PE)

Permutation Entropy (PE) [14] is used to measure the complexity and randomness of a chaotic sequence, where higher values indicate greater irregularity. Figure 5 compares the PE values of the GIDCM with the Henon map. The results indicate that the proposed GIDCM maintains PE values close to 1, with an average of about 0.9975, whereas the Henon map exhibits lower values with an average of approximately 0.6150. These results confirm the stronger randomness and higher complexity of the proposed GIDCM.

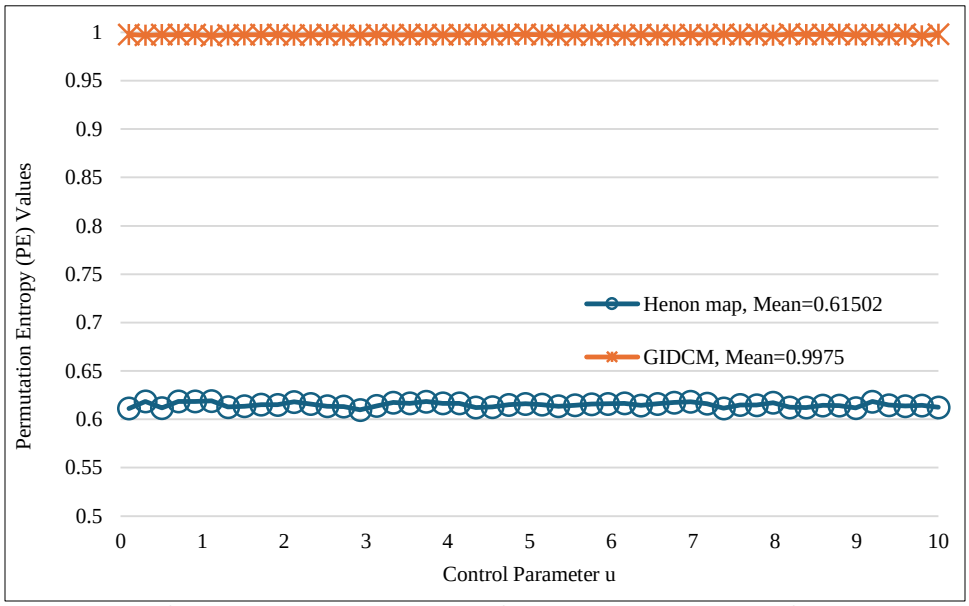


Fig. 5 The comparison of Permutation Entropy (PE) values of proposed GIDCM with state-of-the-art Henon map

3.1.5. The 0-1 Test

The 0-1 test [14] is widely used to distinguish chaotic dynamics from regular behavior, where values close to 1 indicate chaos and values near 0 correspond to periodic motion. Figure 6 compares the 0-1 test values of the GIDCM with those of the Henon map. The observations indicate that both maps maintain values close to 1 over the entire control-parameter range, confirming their chaotic nature. However, the proposed GIDCM exhibits slightly higher and more stable values, with an average of approximately 0.9966 compared with 0.9963 for the Henon map. This result indicates that the proposed map possesses strong and consistent chaotic behavior, well-suited for secure image encryption applications.

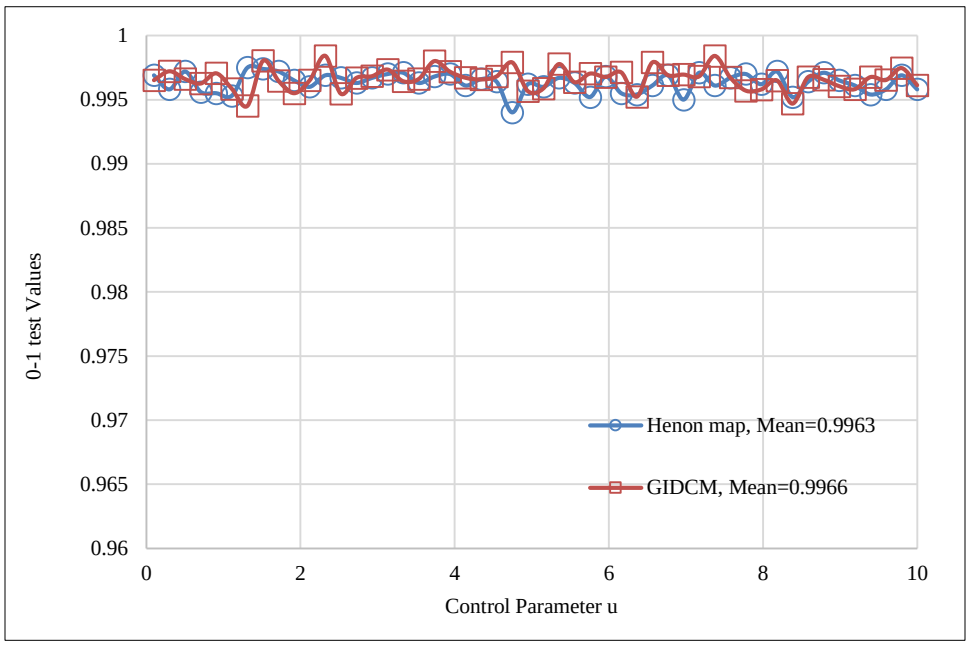


Fig. 6 The comparison of 0-1 test values of proposed GIDCM with state-of-the-art Henon map

4. The Proposed Adaptive Image Encryption Scheme

The adaptive image encryption scheme proposed in this study, composed of three main stages. First, an adaptive secret key is generated for the proposed GIDCM based on the properties of the input image, ensuring image-dependent key generation. Next, the generated key is used to initialize the GIDCM and produce highly random chaotic sequences. Finally, using these chaotic sequences, the encryption process is implemented using pixel permutation and substitution operations, where the permutation stage disrupts the spatial distribution of pixels and the substitution stage modifies their intensity values. This combined process enhances both confusion and diffusion in the encrypted image. The entire process can be implemented through three main algorithms, that is:

Algorithm 1: Computing of adaptively selected secret key of GIDCM

Algorithm 2: Generation of chaotic sequences for encryption

Algorithm 3: Encryption operations composed of pixel permutation and substitution

4.1. Computing of Adaptively Selected Secret Key of GIDCM

The suggested secret key computation scheme extracts all secret parameters out of the input plaintext image, thus creating a high dependency between the encryption keys and the image content. The pixel values of the 256×256 input image are first organized into a 1D vector and subjected to cumulative weighted operations [26]. The resultant sequence is then normalized to the valid gray level range $[0, 255]$ and rearranged into an image of the original dimensions. This preprocessing stage increases the irregularity of the image data before key extraction.

The 256×256 image is then transformed into a 1D sequence of bytes and then processed by the hash function SHA-256 to get a 256-bit digest. Due to the avalanche property of SHA-256, even a minor change in the image leads to an entirely different hash value, and this property greatly increases the sensitivity of plaintext.

Thereafter, three 64-bit segments of the generated digest are extracted and normalized to produce the initial chaotic seeds X, Y, and the control parameter u. Specifically, X and Y are mapped into the interval $(0, 1)$, whereas u is mapped into $(0, 10)$. These parameters are subsequently served as the initial conditions for the chaotic system.

To further expand the key space, six more parameters are obtained by using cyclic overlapping segments of the same hash sequence. The segments are transformed into a decimal integer, scaled to a set range, and rounded to an odd number prior to the next-prime operation. The resulting prime numbers are then square root mapped to produce the irrational parameters $\gamma_1, \gamma_2, \ldots, \gamma_6$. Since the square roots of prime numbers are irrational and non-repeating, these parameters are highly unpredictable and add to greater diffusion ability.

Therefore, the resulting secret key set can be expressed as: $\{X, Y, u, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$ that is entirely dependent on the input image. This type of initialization strategy increases the key space and enhances the security against brute-force, differential, and chosen-plaintext attacks.

4.2. Generation of Chaotic Sequences for Encryption

In Algorithm 2, the secret parameters obtained in Algorithm 1 are used to create three chaotic sequences, which are denoted by S_1, S_2, and S_3. The proposed GIDCM is used to generate three independent chaotic outputs using the initial states (X, Y), control parameter u and irrational parameter pairs (γ_1, γ_2), (γ_3, γ_4), and (γ_5, γ_6). The map is iterated for T successive values to obtain the state sequences. X_i and Y_i. These values are then combined into a middle sequence. q_i with the odd numbers being filled with X_i and the even numbers with Y_i. Finally, the values obtained are multiplied by 10^{15}, then converted into integer form, and then divided by modulo T to derive the chaotic sequences S_1, S_2, and S_3, which are utilized in the subsequent encryption stage.

4.3. Encryption Operations

The encryption procedure described in Algorithm 3 is implemented through permutation and substitution operations. Figure 7 illustrates the whole process of encryption. Firstly, input image I is broken down into B_{block} blocks. First permutation stage involves pixel-level scrambling of each block with the Arnold cat map. Subsequently, block-level permutation is performed using chaotic sequence S_1. Second permutation step involves another Arnold cat map operation to again shuffle pixel positions, and block scrambling with the chaotic sequence S_2, to produce the scrambled image $I_{scr}(x, y)$.

Permutation is followed by the substitution stage to increase diffusion. The chaotic sequence S_3 is transformed into random image G, which is subsequently XORed with he scrambled image to determine an intermediate image V and then the input image is used to create another random image E, which is again XORed with V to give D. Finally, D is transformed to U rounds of transformation by Arnold cat map to finally produce the encrypted image E_{dash}.

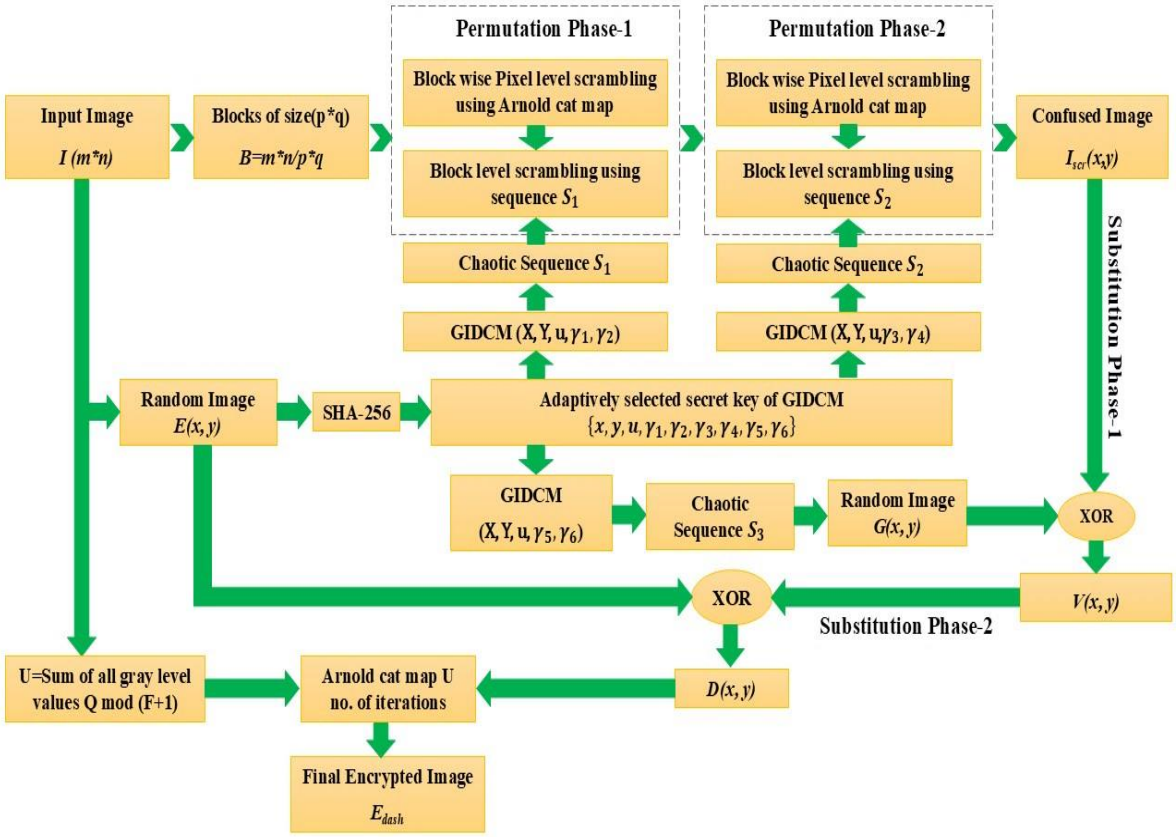


Fig. 7 The adaptive encryption operations composed of pixel permutation and substitution

5. Numerical Simulation Results

This section presents the numerical simulation results obtained for the proposed scheme. All experiments were conducted using MATLAB 2016b on a computer equipped with a 2.00 GHz Intel Core i3 processor and 4 GB of RAM.

Three thermal images, namely Car, Cat, and Man, selected from the Kaggle database, are used for evaluation. Since thermal images contain smooth intensity variations and strong inter-pixel correlation, they provide a suitable test for the proposed encryption scheme. Each image has a size of 256×256pixels and is shown in Figure 8.

https://www.kaggle.com/datasets/deepnewbie/flir-thermal-images-dataset?rvi=1

Initially, the image-dependent secret parameters $\{X, Y, w, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$are generated using Algorithm 1. The corresponding secret keys generated for each test image are listed in Table 2. These parameters are then employed in Algorithm 2 to produce the chaotic sequences S_1, S_2, and S_3, which are subsequently utilized in the encryption process described in Algorithm 3. The simulation results of permutation phase-1, permutation phase-2, substitution phase-1, and substitution phase-2, together with the original and final encrypted images, are presented in Figure 9.

Table 2. Adaptive secret keys computed through algorithm 1

Test Image	Adaptive Secret Keys computed through Algorithm 1								
	X	**Y**	**u**	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6
Car	0.0709	0.8279	0.8195	$\sqrt{513167}$	$\sqrt{994717}$	$\sqrt{609437}$	$\sqrt{140407}$	$\sqrt{737327}$	$\sqrt{103573}$
Cat	0.8672	0.2686	3.1583	$\sqrt{696961}$	$\sqrt{864979}$	$\sqrt{479771}$	$\sqrt{773533}$	$\sqrt{853217}$	$\sqrt{908863}$
Man	0.4888	0.1133	0.5218	$\sqrt{186041}$	$\sqrt{814139}$	$\sqrt{977761}$	$\sqrt{801817}$	$\sqrt{240701}$	$\sqrt{899903}$

Algorithm 1: Computing of adaptively selected secret key of GIDCM

Input: Plain image I of size 256 × 256

Output: $\{X, Y, u, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$,

//Read image I

//Convert the pixel values of I into a 1D vector and apply cumulative weighted operations on it.

//Map the obtained sequence into the range [0, 255].

//Reshape the sequence into an image of original size.

//Convert the transformed image into a 1D byte stream B.

//Compute SHA-256 hash:

H = SHA-256(B);

//Represent H as

H = {h_1, h_2, ..., h_{32}};

//Compute chaotic seed integers

$$X_1 = \sum_{i=1}^{8} h_i * 256^{(8-i)}; Y_1 = \sum_{i=9}^{16} h_i * 256^{(16-i)}; U_1 = \sum_{i=17}^{24} h_i * 256^{(24-i)}$$

//Normalize

$$X = \frac{X_1+1}{2^{64}+1}; Y = \frac{Y_1+1}{2^{64}+1}; u = \frac{U_1+1}{2^{64}+1};$$

for (k = 1 to 6)

$$S_k = 1 + 4(k-1);$$

$$A_k = \sum_{j=0}^{7} h_{[((S_k+j-1) mod 32)+1]} * 256^{(7-j)};$$

$$N_k = mod(A_k, 900000) + 100000;$$

if (N_k is even)

$$N_k = N_k + 1;$$

end

$$P_k = NextPrime(N_k);$$

$$\gamma_k = Sqrt(P_k);$$

end for

//If any repeated γ values occur, increment repeated candidate by 2, recompute P_k and γ_k, until all γ values are distinct.

//Return: $\{X, Y, u, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$

Algorithm 2: Generation of chaotic sequences for encryption
Input: Secret Key of GIDCM $\{X, Y, u, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$, Sequence length T
Output: chaotic sequence S_1, S_2, S_3

//Generate sequence for GIDCM
for i=1 to T/2-1
// Set the initial values and control parameters (x, y, u).
//Set (γ_1, γ_2), (γ_3, γ_4), (γ_5, γ_6) for three for three different chaotic sequences S_1, S_2, S_3 respectively.
// Iterate the Equation (2) for T no. of successive values.
end for

for j=0 to $\frac{T}{2} - 1$ $q_{2j+1} = X_{j+1}$; $q_{2j+2} = Y_{j+1}$; end for
$d_i = floor(q_i \times 10^{15})$; $S = d_i \, mod \, T$; // generate S_1, S_2, S_3
Return chaotic sequence S_1, S_2, S_3.

Algorithm 3: Encryption operations composed of pixel permutation and substitution
Input: Plain text image *I*, chaotic sequence S_1, S_2, S_3.
Output: Encrypted image E_{dash}
//Pixel permutation Phase: Convert image I into B_{block} blocks.

//phase-1
for i=1:B_{block}
Pixel level scrambling Arnold cat map;
end
// Block scrambling using chaotic sequence S_1 from GIDCM.

//phase-2
for i=1:B_{block}
Pixel level scrambling using Arnold cat map;
end
// Block scrambling using chaotic sequence S_2 from GIDCM;
// scrambled image $I_{scr}(x,y)$;

//Pixel Substitution Phase: //Random Image *G* generated from scrambling sequence S_3 from GIDCM;
//Phase 1: $V=bitxor(I_{scr}, G)$;
//Random image *E* generated from plain text image
//Phase 2: $D=bitxor(V, E)$;
//U no. of iteration using Arnold cat. Map: $E_{dash}=arnoldscr(D)$;
Return final encrypted image $E_{dash.}$



(a) **(b)**



(c)

Fig. 8 Thermal images for experiments, (a) Car, (b) Cat, and (c) Man.

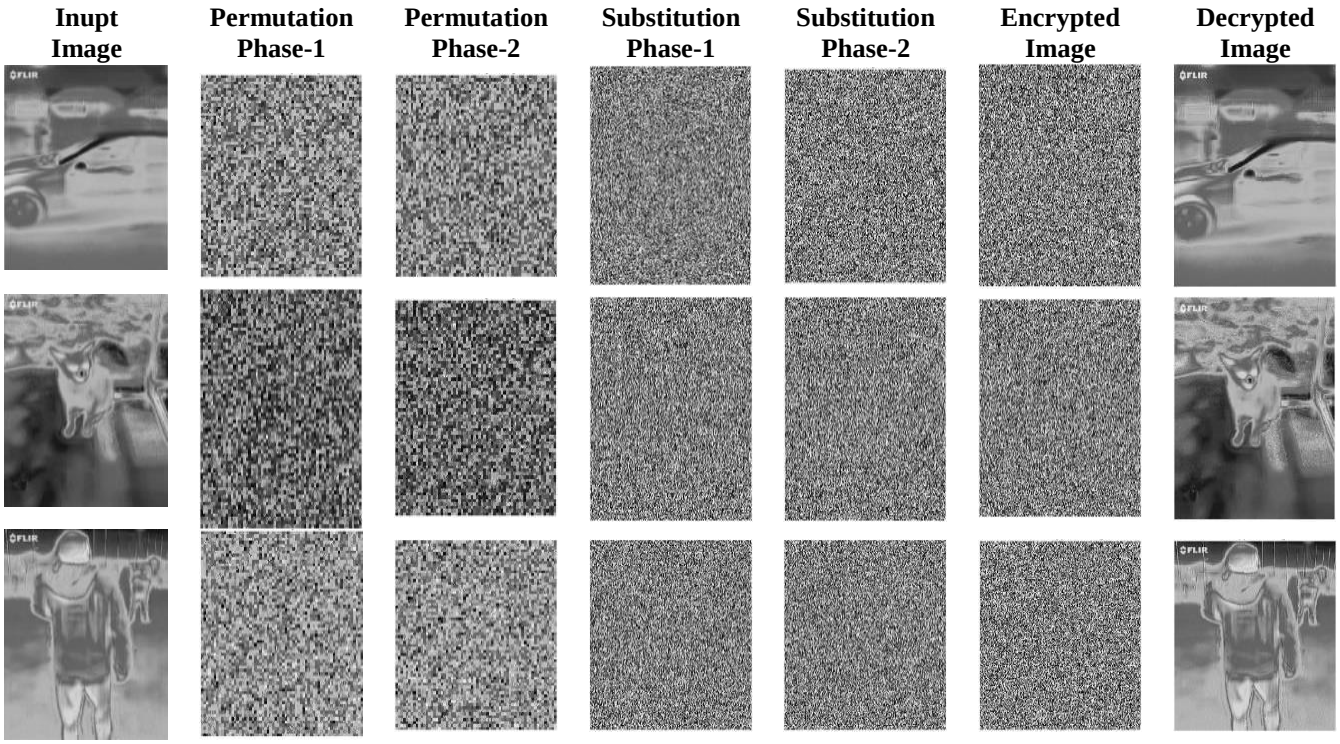


Fig. 9 The output of different phases of encryption process

6. Security Analysis

The security analysis of the proposed image encryption scheme is presented in this section using various statistical and differential attack performance metrices [27].

6.1. Key Space Analysis

The key space of an image encryption scheme reflects the complete range of possible secret keys that could be tested through multiple attempts to obtain the correct key of the encryption [27]. The key space achieved by the proposed encryption scheme is determined by the image-dependent secret keys of the GIDCM, along with the number of Arnold cat map iterations and the number of image blocks. The secret parameters are summarized in Table 3. According to the IEEE floating-point standard [27], the total key space of the proposed scheme is approximately 576 bits. Owing to the high precision of each parameter, the resulting key space is significantly large, making exhaustive brute-force attacks computationally impractical. Therefore, the proposed scheme provides sufficient key space to ensure secure image encryption.

Table 3. Secret keys of the proposed scheme

Secret Keys	Initial value	Parameters
GIDCM	X, Y	$u, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6$
No. of iterations in Arnold Cat Map		U
No. of blocks		B

6.2. Key Sensitivity Analysis

Key sensitivity describes the effect of varying secret key values on security. It involves modifying one or more secret keys and analyzing the effect in encrypted data. The aim is to uncover potential vulnerabilities in the encryption scheme that hackers could exploit by varying different key values [27]. Key sensitivity analysis is carried out here by introducing slight variations in secret parameters.

The results are summarized in Table 4. A small change of 10^{-15} in X_1, Y_1, and u_1, as well as a variation of 10^2in the Arnold cat map iterations U, produces key sensitivity values close to 99.6% for all test images. These results confirm that even a minor change in the secret keys generates a significantly different encrypted image, demonstrating the high sensitivity and security of the proposed scheme.

Table 4. Key sensitivity analysis of the proposed scheme

Parameters	Secret Keys	Inc. /Dec.	Key sensitivity *P(k)%*		
			Input Images		
			Car	Cat	Man
Initial values of GIDCM	X_1	10^{-15}	99.64	99.59	99.64
	Y_1	10^{-15}	99.61	99.62	99.60
Control Parameter of GIDCM	u_1	10^{-15}	99.61	99.61	99.60
No. of iterations in Arnold Cat Map	U	10^2	99.62	99.59	99.62

6.3. Entropy Analysis

The entropy value of an image is defined as a measure of the randomness present in the distribution of pixel values within an image [27]. As shown in Table 5, the entropy values of the original thermal images are relatively low due to the presence of structured temperature information. The entropy remains unchanged during the two permutation phases, indicating that permutation only alters pixel positions without affecting gray level distribution. However, a significant increase is observed after the substitution phases, where the entropy values approach the ideal value of 8. The entropy values of the final encrypted images range from 7.9988 to 7.9995, confirming the high randomness and strong diffusion capability of the proposed scheme.

Table 5. Entropy value analysis

Test Image	Entropy Value					
	Input image	Permutation Phase-1	Permutation Phase-2	Substitution Phase-1	Substitution Phase-2	Encrypted Image
Car	6.8035	6.8035	6.8035	7.9992	7.9995	7.9995
Cat	7.3961	7.3961	7.3961	7.9992	7.9992	7.9992
Man	7.1040	7.1040	7.1040	7.9988	7.9995	7.9995

6.4. Statistical Attack Analysis

Statistical attack analysis is performed in this section by evaluating the correlation of adjacent pixels, autocorrelation and Histogram analysis.

6.4.1. Correlation of Adjacent Pixels

Original plaintext images exhibit strong correlations among adjacent pixels in horizontal, vertical, and diagonal directions.

Attackers often exploit these correlations by analyzing adjacent pixel relationships in encrypted images to collect information of original plaintext.

So, a secure image encryption algorithm must minimize pixel correlation to reduce the correlation coefficient to nearly zero across all three directions [27]. As shown in Table 6, the original thermal images show very high correlation coefficients in the horizontal, vertical, and diagonal directions, with mean values ranging from 0.93340 to 0.97055. After encryption, these values become extremely close to zero across all directions. The mean values of the encrypted images are 40×10^{-5}, 7×10^{-5}, and -7×10^{-4} for the Car, Cat, and Man images, respectively.

Furthermore, the correlation plots of CAR image across all directions are shown in Figure 10 indicates that the pixels of the input images are highly concentrated along a straight line, whereas the encrypted images exhibit a random and widely scattered distribution.

These findings demonstrate that the proposed scheme effectively eliminates the strong correlations among adjacent pixels, thereby providing robust resistance to statistical attacks.

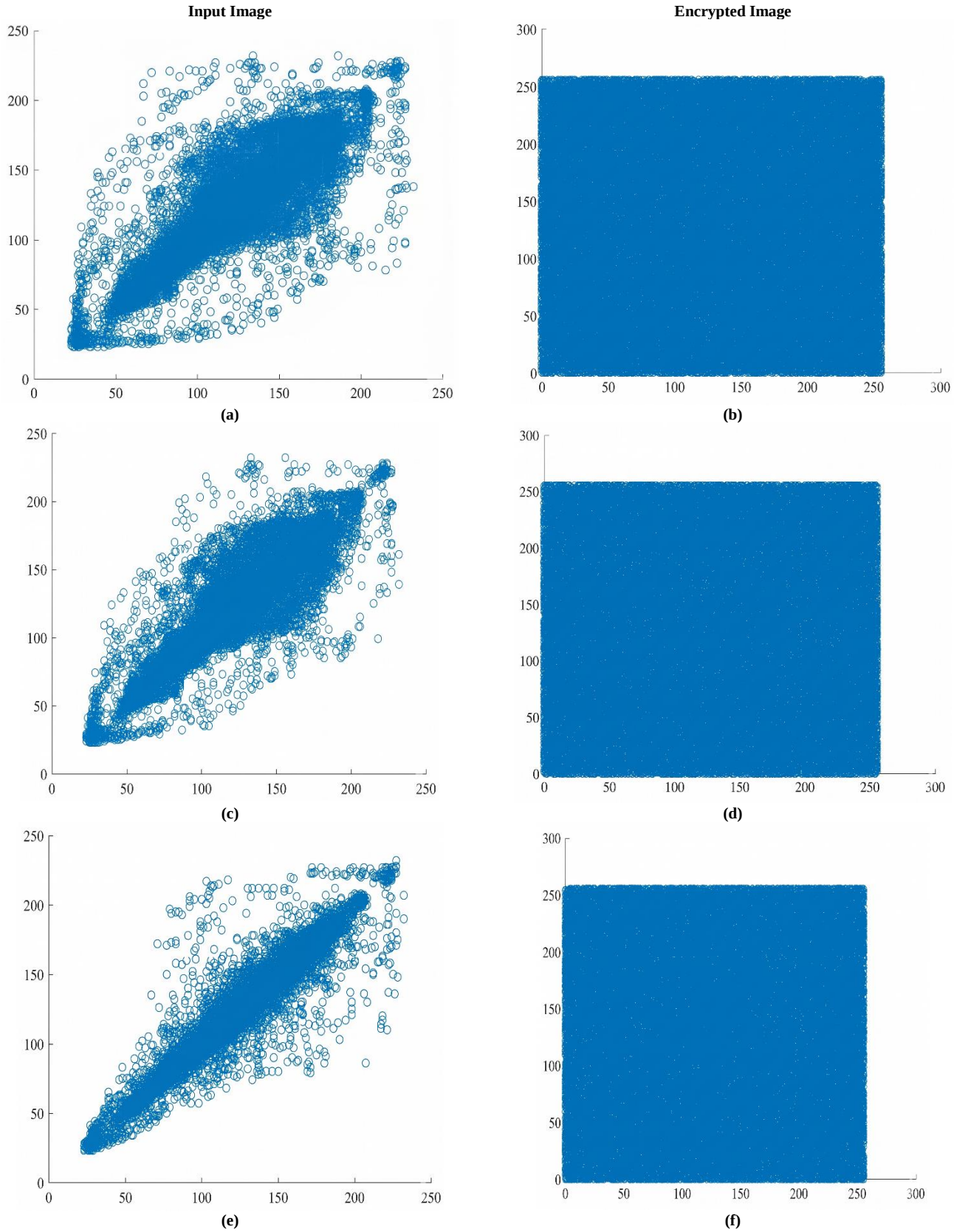


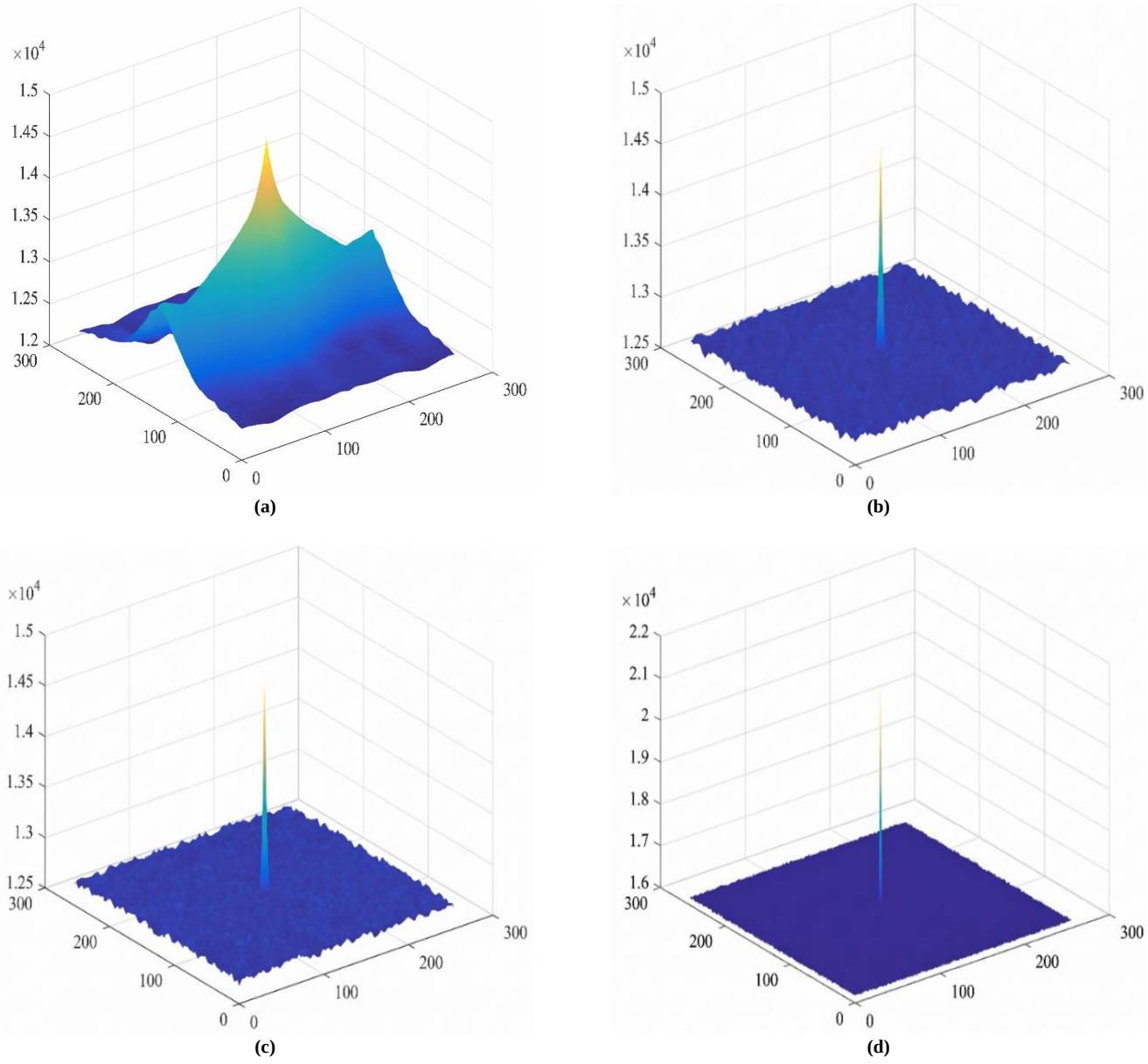
Fig. 10 Correlation plots of test images (CAR) and respective encrypted images in (a)-(b) Horizontal direction, (c)-(d) Vertical direction, and (e)-(f) Diagonal direction.

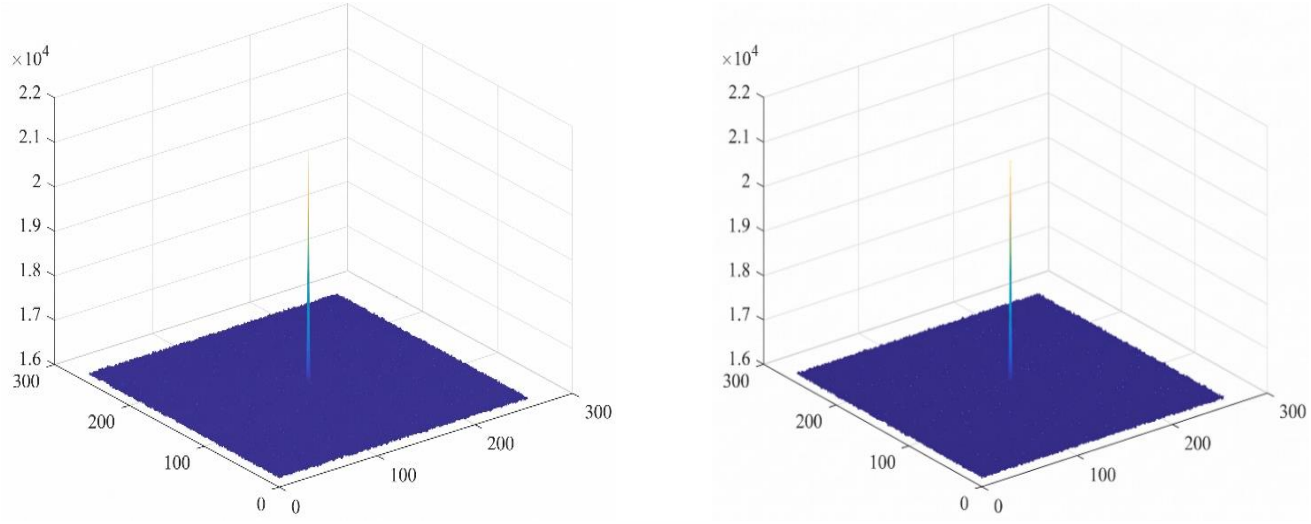
Table 6. Correlation coefficient values of adjacent pixels

Test images	Correlation Coefficients							
	Input Image				Encrypted Image			
	Horizontal	Vertical	Diagonal	Mean	Horizontal	Vertical	Diagonal	Mean
Car	0.98860	0.96786	0.95518	0.97055	0.00118	-0.00002	0.00003	40×10^{-5}
Cat	0.94255	0.93628	0.92400	0.93427	0.00141	0.00074	-0.00193	7×10^{-5}
Man	0.93100	0.96296	0.90623	0.93340	-0.00055	0.00083	-0.00263	-7×10^{-4}

6.4.2. Autocorrelation Analysis

The autocorrelation plot signifies how effectively the encryption process converts the original image into a white noise image distribution [27]. Figure 11 presents the autocorrelation plots of CAT image across different stages. The original images show strong and regular correlation patterns because neighboring pixels have similar intensity values. However, the encrypted images exhibit highly irregular autocorrelation distributions without any noticeable repetitive pattern. This indicates that the proposed encryption scheme successfully removes the strong spatial correlation present in the original images.





(e) **(f)**

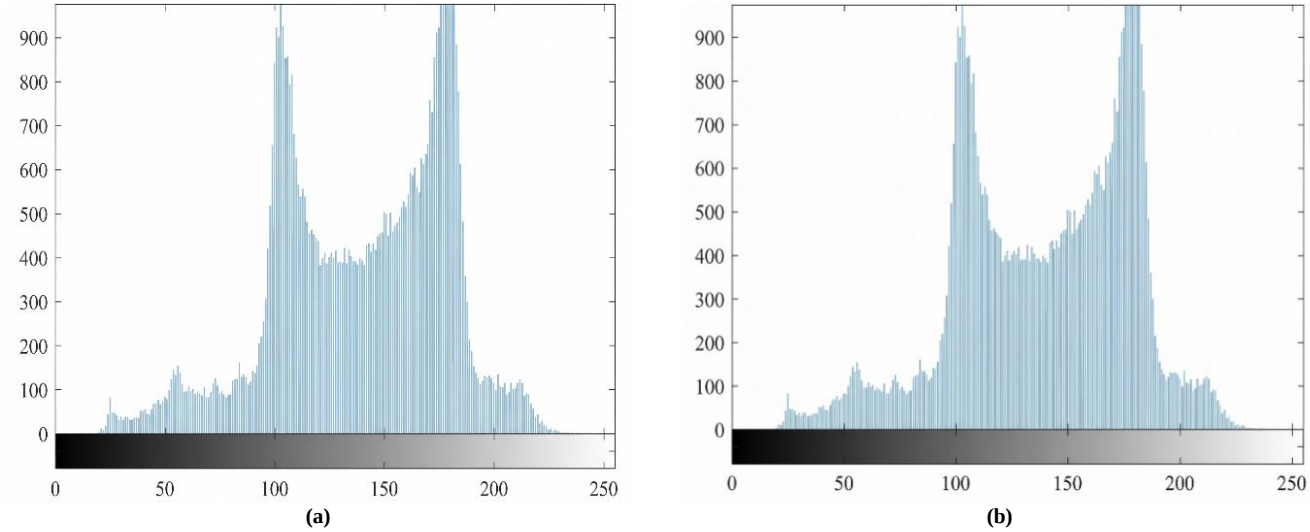
Fig. 11 Autocorrelation plots of test image (CAT) at different phases of encryption process (a) Input image, (b) Permutation phase-1, (c) Permutation phase-2, (d) Substitution phase-1, (e) Substitution phase-2, and (f) Encrypted image.

6.4.3. Histogram Analysis

The histogram of an image displays the information about probability distribution of its pixel values by computing the pixel counts at each intensity level [27]. As reported in Table 7, the χ^2 values remain unchanged during the permutation stages, showing that pixel shuffling only changes the pixel positions without affecting the gray-level distribution. After the substitution stages, the χ^2 values decrease considerably and reach very low levels in the final encrypted images. For the Car, Cat, and Man images, the final χ^2 values are 231.98, 249.54, and 229.95, respectively. In addition, the histogram plots of MAN image in Figure 12 reveal that the original images possess highly uneven pixel distributions, while the encrypted images exhibit nearly uniform histograms. This behavior demonstrates the strong diffusion performance and statistical robustness of the proposed encryption scheme.

Table 7. χ^2 values at different phases of encryption process

Test images	χ^2 Values					
	Input Image	Permutation Phase-1	Permutation Phase-2	Substitution Phase-1	Substitution Phase-2	Encrypted image
Car	144779.96	144779.96	144779.96	251.59	231.98	231.98
Cat	41756.71	41756.71	41756.71	247.66	249.54	249.54
Man	86621.05	86621.05	86621.05	285.78	229.95	229.95



(a) **(b)**

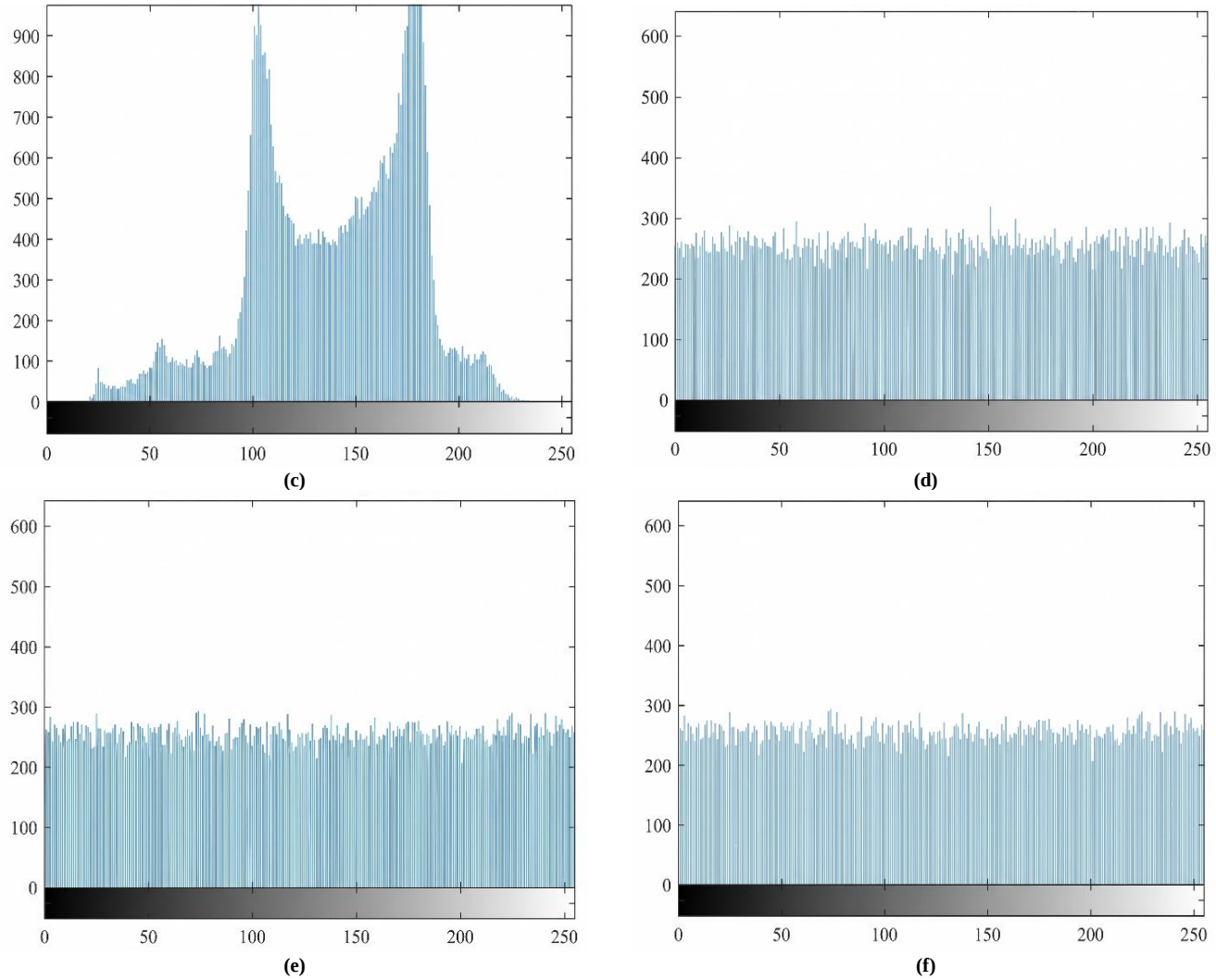


Fig. 12 Histogram plots of test image (MAN) at different phases of encryption process (a) Input image, (b) Permutation phase-1, (c) Permutation phase-2, (d) Substitution phase-1, (e) Substitution phase-2, and (f) Encrypted image.

6.5. Differential Attack Analysis

In differential attacks, Attackers attempt to crack the image encryption algorithm by analyzing the changes in the encrypted image resulting from a slight modification to the original plain-text image [27].

Differential attack performance is evaluated using the NPCR and UACI metrics [27]. NPCR is defined as the percentage of pixels that change in the encrypted image because of a single-pixel modification in the original image. UACI, on the other hand, represents the average intensity difference between the original and encrypted images.

According to Table 8, the proposed scheme attains NPCR values of 99.6445%, 99.6140%, and 99.6750% for the Car, Cat, and Man images, respectively.

The respective UACI values are 33.4673%, 33.6457%, and 33.7990%. These results closely approach the theoretical ideal values, suggesting that even a minor modification in the plain image leads to a substantial variation in the encrypted image. Hence, the proposed encryption scheme exhibits strong resistance to differential attacks.

Table 8. NPCR and UACI values for the proposed encryption scheme

Test Image	Differential Attack Parameters	
	NPCR score	UACI score
Car	99.6445	33.4673
Cat	99.6140	33.6457
Man	99.6750	33.7990

6.6. Robustness Attack Analysis

This section investigates the robustness of the proposed encryption scheme against cropping, salt-and-pepper noise, and Gaussian noise attacks.

6.6.1. Cropping Attack

For cropping attack analysis, the encrypted images are cropped using block sizes of 16×16, 32×32, 64×64, 128×128, and 256×256, followed by decryption of the corrupted cipher images.

Figure 13 shows the cropped encrypted images and respective decrypted results. As the cropped region becomes larger, the recovered image quality gradually decreases. However, even under severe cropping conditions, the decrypted images still preserve sufficient visual information of the original image.

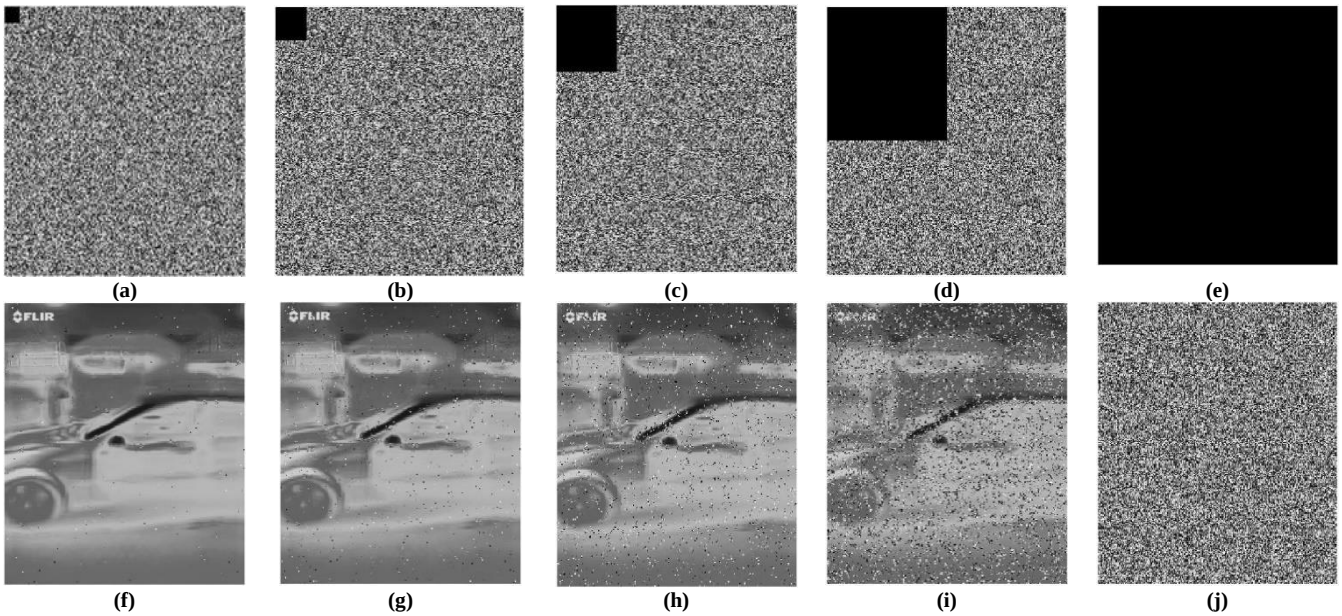


Fig. 13 The encrypted image subjected to cropping attack from 16×16 to 256×256 [(a)-(e)] and corresponding decrypted images [(f)-(j)]

6.6.2. Salt and Pepper Noise Attack

For salt-and-pepper noise attack analysis, noise densities of 2%, 4%, 6%, 8%, 10%, 12%, 14%, 16%, 18%, and 20% are introduced into the encrypted images before decryption. The recovered images obtained under different noise levels are presented in the Figure 14.

With the increasing noise density, the visual information of the decrypted images gradually declines. Even at a noise density of 20%, the major structural features of the original image remain identifiable, highlighting the robustness of the proposed scheme against salt-and-pepper noise attacks.

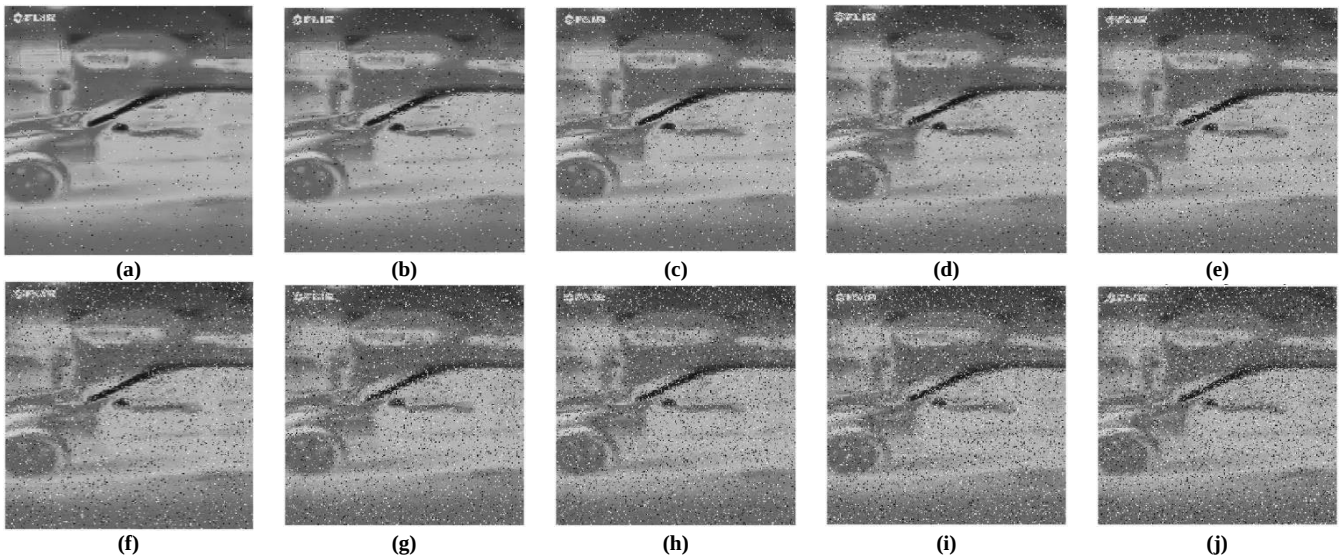


Fig. 14 Decrypted images obtained under different salt-and-pepper noise densities ranging from 2% to 20%

6.6.3. Gaussian Noise Attack

For Gaussian noise attack analysis, Gaussian noise with standard deviation values of 5, 10, 15, 20, 25, 30, 35, 40, 45, and 50 is introduced into the encrypted images prior to decryption. The recovered images obtained under different noise levels are presented on Figure 15.

The visual information of the decrypted images gradually deteriorates as the standard deviation increases. Despite this degradation, the major visual characteristics of the original image remain recognizable even at a standard deviation of 50, confirming the strong resilience of the proposed scheme against Gaussian noise attacks.

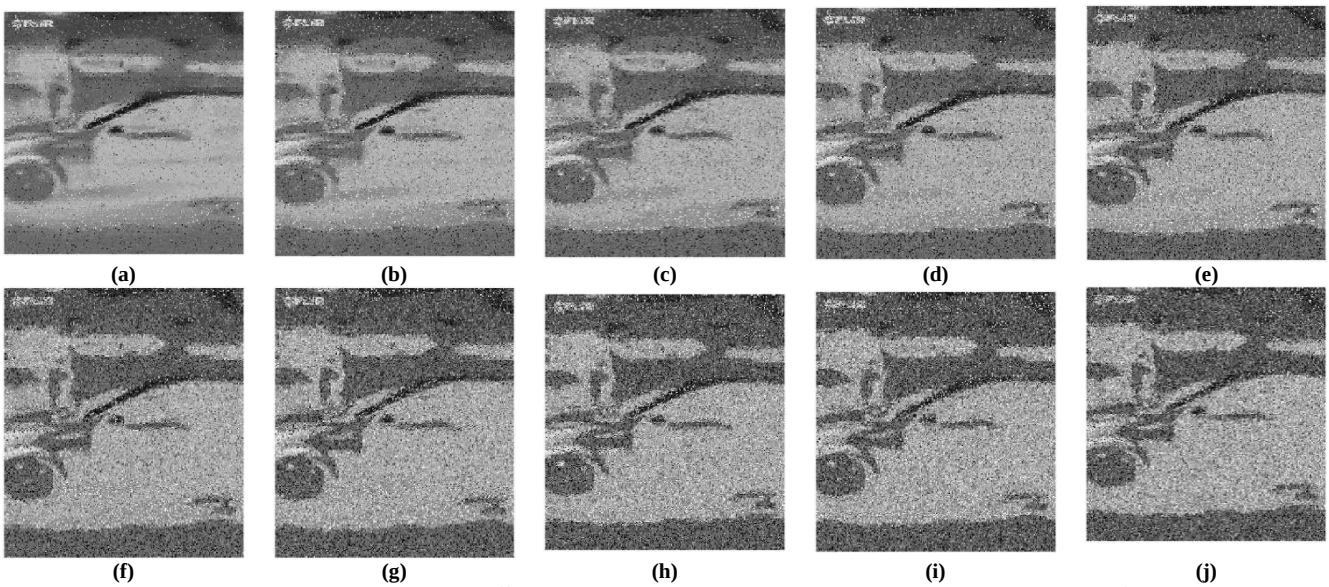


Fig. 15 Decrypted images obtained under different Gaussian noise levels with standard deviation values ranging from 5 to 50

6.7. Comparison with the Recent Image Encryption Schemes

Table 9 presents a comparative analysis between the proposed scheme and several recent image encryption methods based on NPCR, UACI, entropy, key space, and adjacent-pixel correlation coefficients.

The proposed method attains an NPCR of 99.64% and a UACI of 33.64%, both of which are closely aligned with the theoretical ideal values and comparable to those reported in recent studies. The entropy value reaches 7.9994, reflecting the nearly uniform distribution of pixel values in the encrypted image. One of the key advantages of the proposed scheme is its exceptionally large key space of 2^{576}, which is substantially larger than those of the compared methods. In addition, the horizontal, vertical, and diagonal correlation coefficients are 0.00068, 0.00051, and -0.00151, respectively, showing that the encrypted image contains almost no residual pixel correlation. The main factor behind the improved results compared to state-of-the-art techniques lies in the hyperchaotic behavior of proposed GIDCM integrated with a complex two-step pixel permutation and pixel substitution process. The pixel permutation process itself randomly spreads the image pixels using both block-level and pixel-level permutation.

Two rounds of pixel permutation distribute the pixels more uniformly across the image. Next, the two rounds of adaptive pixel substitution completely neutralize the statistical properties present in the input image. That is why the proposed scheme achieves better results than contemporary state-of-the-art techniques. Overall, These findings indicate that the proposed scheme offers strong resistance to brute-force, statistical, and differential attacks, while offering improved security performance compared with existing approaches.

Table 9. Comparison with the recent image encryption schemes

Algorithm	Differential Attack Parameters		Entropy	Key Space	Correlation Coefficients of Encrypted Image		
	NPCR	UACI			Horz.	Vert.	Diag.
Proposed Scheme	99.64	33.64	7.9994	2^{576}	0.00068	0.00051	-0.00151
Ref. [10]	99.60	33.45	7.9994	2^{25675}	0.00038	-0.00030	-0.00028
Ref. [28]	99.61	32	7.9990	2^{850}	0.0013	0.0013	0.0013
Ref. [11]	99.60	33.46	7.9993	2^{398}	-0.00053	0	0.00146
Ref. [16]	99.61	33.45	7.9025	2^{240}	−0.0006	0.001	−0.0012
Ref. [29]	99.62	33.45	7.9993	2^{256}	0.0134	0.0019	0.0243

7. Conclusion

In this work, an adaptive thermal image encryption scheme based on a Generalized Irrationality-Driven Chaotic Map (GIDCM) has been presented. By incorporating generalized irrational parameters, the proposed chaotic map improves the complexity and controllability of the generated chaotic behavior. In addition, an image-dependent key generation mechanism is adopted to increase key sensitivity and strengthen security. The encryption framework integrates chaotic sequence generation with multiple permutation and substitution stages to hide the spatial characteristics of thermal images effectively. The obtained results demonstrate that the scheme achieves high entropy, very low pixel correlation, a large key space, strong resistance to differential attacks, and good robustness against cropping and noise disturbances. These findings suggest that the proposed method can serve as an effective and secure approach for thermal image encryption.

Conflicts of Interest

The authors declare that they have no known conflicts of interest that could have influenced the work reported in this paper.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Majid Khan et al., "A Secure Chaotic Cryptosystem for Thermal Imaging: Logistic Map-based Encryption with Substitution-Diffusion and Spatial Decorrelation," *Journal of Radiation Research and Applied Sciences*, vol. 18, no. 2, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Manu Sudhi et al., "Thermal Imaging Applications in Shock Detection: Technological Advancements and Clinical Implications," *Engineered Science*, vol. 33, pp. 1-13, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] B.S. Lokesh, M.B. Manjunatha, and Panduranga H.T., "Novel Method for Thermal Image Encryption," *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, pp. 1-5, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[4] Muhammad Akraam, Tabasam Rashid, and Sohail Zafar, "A Chaos-based Image Encryption Scheme is Proposed using Multiple Chaotic Maps," *Mathematical Problems in Engineering*, vol. 2023, no. 1, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mingfang Jiang, and Hengfu Yang, "Image Encryption using a New Hybrid Chaotic Map and Spiral Transformation," *Entropy*, vol. 25, no. 11, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Wassim Alexan et al., "A Secure and Efficient Image Encryption Scheme based on Chaotic Systems and Nonlinear Transformations," *Scientific Reports*, vol. 15, no. 1, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Uğur Erkan et al., "2D eπ-Map for Image Encryption," *Information Sciences*, vol. 589, pp. 770-789, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Rohan Tuli, Hitesh Narayan Soneji, and Prathamesh Churi, "PixAdapt: A Novel Approach to Adaptive Image Encryption," *Chaos Solitons and Fractals*, vol. 164, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Feng Yu et al., "Differential Cryptanalysis of Image Cipher using Block-based Scrambling and Image Filtering," *Information Sciences*, vol. 554, pp. 145-156, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Abdurrahim Toktas et al., "A Robust Bit-Level Image Encryption based on Bessel Map," *Applied Mathematics and Computation*, vol. 462, pp. 1-31, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Feyza Toktas, Uğur Erkan, and Zeki Yetgin, "Cross-Channel Color Image Encryption through 2D Hyperchaotic Hybrid Map of Optimization Test Functions," *Expert Systems with Applications*, vol. 249, pp. 1-24, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Omer Kocak et al., "PSO-based Image Encryption Scheme using Modular Integrated Logistic Exponential Map," *Expert Systems with Applications*, vol. 237, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Uğur Erkan, Abdurrahim Toktas, and Qiang Lai, "2D Hyperchaotic System based on Schaffer Function for Image Encryption," *Expert Systems with Applications*, vol. 213, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Uğur Erkan, Abdurrahim Toktas, and Qiang Lai, "Design of Two Dimensional Hyperchaotic System through Optimization Benchmark Function," *Chaos Solitons and Fractals*, vol. 167, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Shenli Zhu et al., "Image Encryption Scheme based on Newly Designed Chaotic Map and Parallel DNA Coding," *Mathematics*, vol. 11, no. 1, pp. 1-22, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Xiaoman Jiang et al., "Image Encryption Algorithm based on 2D-CLICM Chaotic System," *IET Image Process*, vol. 17, no. 7, pp. 2127-2141, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jianeng Tang et al., "An Image Layered Scrambling Encryption Algorithm based on a Novel Discrete Chaotic Map," *IET Image Process*, vol. 17, no. 2, pp. 518-532, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zhongyun Hua et al., "Cross-Plane Colour Image Encryption using a Two-Dimensional Logistic Tent Modular Map," *Information Sciences*, vol. 546, pp. 1063-1083, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Fan Haiju et al., "Cryptanalysis of a Colour Image Encryption using Chaotic APFM Nonlinear Adaptive Filter," *Signal Processing*, vol. 143, pp. 28-41, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[20] Sakshi Dhall, Saibal K. Pal, and Kapil Sharma, "Cryptanalysis of Image Encryption Scheme based on a New 1D chaotic System," *Signal Processing*, vol. 146, pp. 22-32, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[21] S.N. Manoharan, "Cryptanalysis and Security Evaluation of Optimized Algorithms for Image Encryption in Deep Optimal Network," *International Journal of Information Technology*, vol. 16, no. 5, pp. 2883-2889, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Haiju Fan et al., "Cryptanalysis of a New Chaotic Image Encryption Technique based on Multiple Discrete Dynamical Maps," *Entropy*, vol. 23, no. 12, pp. 1-17, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jiahui Wu, Xiaofeng Liao, and Bo Yang, "Cryptanalysis and Enhancements of Image Encryption based on Three-Dimensional Bit Matrix Permutation," *Signal Processing*, vol. 142, pp. 292-300, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Guiqiang Hu et al., "Cryptanalysis of a Chaotic Image Cipher using Latin Square-based Confusion and Diffusion," *Nonlinear Dynamics*, vol. 88, no. 2, pp. 1305-1316, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ming Li et al., "Cryptanalysis and Improvement in a Chaotic Image Cipher using Two-Round Permutation and Diffusion," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 31-47, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Brindha Murugan, and Ammasai Gounden Nanjappa Gounder, "Image Encryption Scheme based on Block-based Confusion and Multiple Levels of Diffusion," *IET Computer Vision*, vol. 10, no. 6, pp. 593-602, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[27] Yousef Alghamdi, and Arslan Munir, "Image Encryption Algorithms: A Survey of Design and Evaluation Metrics," *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 126-152, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] He Zhiqiang et al., "Design and Analysis of a Secure Image Encryption Algorithm using Proposed Non-Linear RN Chaotic System and ECC/HKDF Key Derivation with Authentication Support," *Scientific Reports*, vol. 15, no. 1, pp. 1-22, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[29] Yingjie Su et al., "A Novel One-Dimensional Chaotic System for Image Encryption through the Three-Strand Structure of DNA," *Entropy*, vol. 27, no. 8, pp. 1-20, 2025. [CrossRef] [Google Scholar] [Publisher Link]