AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(10): 27220–27246.
DOI: 10.3934/math.20241323
Received: 06 May 2024
Revised: 27 August 2024
Accepted: 29 August 2024
Published: 20 September 2024

Research article

An efficient confidentiality scheme based on quadratic chaotic map and Fibonacci sequence

Majid Khan[1],* and Hafiz Muhammad Waseem[2]

[1] Department of Mathematics, College of Science and Humanities in Alkharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[2] Warwick Manufacturing Group (WMG), Warwick University, United Kingdom

* **Correspondence:** Email: mb.khan@psau.edu.sa.

Abstract: In today's rapidly evolving digital landscape, secure data transmission and exchange are crucial for protecting sensitive information across personal, financial, and global infrastructures. Traditional cryptographic algorithms like RSA and AES face increasing challenges due to the rise of quantum computing and enhanced computational power, necessitating innovative approaches for data security. We explored a novel encryption scheme leveraging the quadratic chaotic map (QCM) integrated with the Fibonacci sequence, addressing key sensitivity, periodicity, and computational efficiency. By employing chaotic systems' inherent unpredictability and sensitivity to initial conditions, the proposed method generates highly secure and unpredictable ciphers suitable for text and image encryption. We incorporated a combined sequence from the Fibonacci sequence and QCM, providing enhanced complexity and security. Comprehensive experimental analyses, including noise and occlusion attack simulations, demonstrate the scheme's robustness, resilience, and practicality. The results indicated that the proposed encryption framework offers a secure, efficient, and adaptable solution for digital data protection against modern computational threats.

Keywords: chaotic map; Fibonacci sequence; image encryption; information security
Mathematics Subject Classification: 94A60, 68P25

1. Introduction

In the rapidly advancing landscape of modern society, the significance of secure digital data transmission and exchange is paramount. From personal communications and financial transactions to critical infrastructure management and global business operations, the seamless flow of information underpins virtually every aspect of contemporary life. Ensuring the security of this data is essential, as breaches can lead to personal privacy violations, economic disruptions, and national security threats. Conventional cryptographic algorithms, such as RSA, AES, and DES, have long been the cornerstone of data security, relying on complex mathematical principles and large key sizes for robust protection against unauthorized access. However, they face challenges as computational power grows exponentially, making brute force attacks more viable, and the emergence of quantum computing poses a significant risk, potentially allowing quantum algorithms to decrypt data much faster than classical computers.

Considering these challenges, the relationship between chaos theory and cryptography offers a promising avenue for enhancing data security. Chaos theory, a branch of mathematics focused on complex and dynamic systems that are highly sensitive to initial conditions, provides a novel framework for encryption. The inherent unpredictability and sensitivity in chaotic systems make them extraordinarily difficult to decipher without the correct key. These systems are deterministic yet appear random, making it nearly impossible to predict their behavior without precise knowledge of the initial conditions. This deterministic chaos ensures that even minor changes in input can lead to vastly different outputs, providing a high level of security against attempts to reverse-engineer the encryption process. The behavior of chaotic systems, characterized by their sensitivity to initial conditions, topological mixing, and dense periodic orbits, aligns well with the requirements for secure encryption and digital content exchange.

Researchers have highlighted several advancements in chaos-based cryptosystems, including Logistic Map with DNN, Henon Map with ANN, Arnold Cat Map, JPEG Compatible Encryption, Reverse Zigzag, DNA Diffusion, and Hyperchaotic Attractors. The following are detailed overviews of these methods and their challenges:

- Logistic Map with DNN: The integration of logistic maps with DNNs for image encryption leverages the chaotic properties of logistic maps and the adaptive learning capabilities of DNNs to enhance encryption robustness. Logistic maps generate pseudo-random sequences that are highly sensitive to initial conditions, making them suitable for creating encryption keys. These keys are then processed by a DNN, which has been trained on image data to understand and transform chaotic sequences effectively. This combination ensures that the encryption keys are both unpredictable and complex, significantly improving the security of the encrypted images [1]. Several researchers have demonstrated improved encryption quality, key sensitivity, and robustness against several attacks through various deep learning and neural networks based intelligent mechanisms [2,3,4,5]. However, the integration of logistic maps with DNNs also presents challenges. Training the DNN requires substantial computational resources and large datasets, which can hinder practical implementation. Additionally, the system's security must be rigorously tested against various cryptographic attacks to ensure its robustness. The computational overhead introduced by the DNN processing phase must be balanced with the encryption's efficiency to make the method viable for real-time applications. Researchers are focused on optimizing the balance between security and computational efficiency to fully realize the potential of this innovative encryption approach [6,7].
- Henon Map with ANN: The integration of the Henon map with ANN in image encryption leverages the chaotic nature of the Henon map and the pattern recognition capabilities of ANN to enhance security. In this approach, the Henon map generates chaotic sequences that shuffle pixel positions in the image, introducing a high level of randomness. The ANN is trained with these

transformed images to learn and replicate the complex encryption patterns. During encryption, the ANN uses the chaotic sequences from the Henon map to encrypt new images dynamically, ensuring that each encryption instance is unique and secure [1,8,9]. However, these method faces several challenges, including key sensitivity, computational complexity, and robustness against attacks. Small variations in the Henon map's initial parameters can lead to significant differences in the encrypted output, complicating synchronization between encryption and decryption [10]. Additionally, training the ANN to accurately learn and apply chaotic transformations requires substantial computational resources and time. Ensuring the system's robustness against modern cryptographic attacks and finding optimal parameters for both the Henon map and ANN are crucial for practical implementation [11,12].

- Arnold Cat Map: The Arnold Cat Map is widely used in image encryption due to its ability to thoroughly shuffle pixel positions, creating a seemingly random distribution that enhances security. Statistically, it transforms pixel coordinates using a specific matrix operation, and when iterated multiple times, it effectively disrupts spatial correlations in the image, making it difficult to decode without the correct key [13,14]. However, the map's periodic nature, where the image can revert to its original state after a certain number of iterations, poses a security risk if the number of iterations is known. To mitigate this, it is often combined with other chaotic systems or neural networks, enhancing the complexity and unpredictability of the encryption process [1,15]. Despite its advantages, the Arnold Cat Map faces challenges such as limited key space and statistical predictability due to its deterministic nature [16]. The periodicity can be exploited by attackers to reverse the encryption. Combining the Arnold Cat Map with other chaotic maps or cryptographic techniques can address these issues, offering a more secure and robust encryption solution. For instance, integrating it with the Henon map or Logistic map adds additional layers of security, while hybrid systems incorporating neural networks can further enhance resistance to attacks.
- JPEG Compatible Encryption: JPEG compatible encryption integrates encryption directly into the JPEG compression process, leveraging techniques such as modifying Discrete Cosine Transform (DCT) coefficients and permuting AC and DC coefficients. These methods ensure that the encrypted image retains its JPEG format while enhancing security [17]. For instance, permuting the DCT coefficients or scrambling the blocks of an image based on chaotic sequences disrupts the image content while maintaining the compression efficiency and image quality standards set by JPEG. This approach reduces computational overhead by combining encryption with compression, making it suitable for practical applications [18]. Key management and distribution are critical, as keys must be protected to ensure unauthorized users cannot decrypt the images. Balancing security and compression efficiency is also a concern, as encryption should not degrade the compression ratio or image quality. Additionally, maintaining computational efficiency while providing robust security and ensuring that encrypted images remain compatible with standard JPEG decoders are essential for the practical application of these methods [19]. These challenges necessitate ongoing research to optimize JPEG compatible encryption techniques.
- Reverse Zigzag and DNA Diffusion: The reverse zigzag and DNA diffusion method for image encryption combines advanced traversal and encoding techniques to significantly enhance security. The reverse zigzag algorithm modifies the traditional pixel traversal order, making the scrambling process more unpredictable and resistant to attacks that exploit predictable patterns. Once the pixels are scrambled, DNA diffusion is applied, wherein pixel values are converted into DNA sequences and manipulated using biological operations, such as complementary pairing [20,21]. This adds a layer of complexity and nonlinearity, making the encryption robust against differential and chosen-plaintext attacks. This dual approach leverages the strengths of both methods to provide a high level of security

in image encryption. Despite its strengths, the reverse zigzag and DNA diffusion method faces challenges such as increased computational complexity and resource requirements. The implementation of DNA operations and managing the encryption keys can be intricate and demanding, potentially affecting scalability and compatibility with existing systems [22]. Moreover, the computational overhead might limit its applicability in real-time or large-scale image processing scenarios. These challenges highlight the need for further research and optimization to fully realize the potential of this advanced encryption technique [1].

- Hyperchaotic attractors: Hyperchaotic multi-wing attractors enhance image encryption by leveraging their complex dynamics and high sensitivity to initial conditions, which create highly unpredictable and secure encryption keys. These systems can generate larger key spaces compared to simpler chaotic systems, making them robust against brute-force attacks. The encryption process involves shuffling pixel positions and modifying pixel values based on the key stream derived from the hyperchaotic attractor, ensuring each pixel's value is intricately linked to the entire image content, thus complicating differential attacks [23,24]. However, the implementation of hyperchaotic multi-wing attractors in image encryption faces significant challenges, such as computational intensity and sensitivity to initial parameter variations, which can hinder real-time applications and cause decryption failures if not precisely managed. Additionally, the complexity of accurately solving the associated differential equations and ensuring robustness against noise adds to the implementation challenges [25]. Despite these hurdles, ongoing research aims to optimize these systems to fully leverage their potential for secure image encryption.

In addition to the above several challenges, chaos-based systems also face key sensitivity, periodicity, computational complexity, and resistance to modern attack issues. Although integrating chaotic systems with machine learning techniques, such as Logistic Map with DNN or Henon Map with ANN, offers promising encryption robustness, it introduces significant computational complexity and resource demands. These methods require substantial computational power and large datasets for training, posing a barrier to practical implementation, especially for real-time applications. Achieving a balance between security and computational efficiency remains a key challenge in the development of chaos-based cryptographic systems. While chaos-based encryption methods like the Arnold Cat Map effectively shuffle pixel positions to enhance security, their periodic nature poses a risk. If the periodicity of these systems is known, attackers can exploit it to reverse the encryption.

To address the challenges faced by chaos-based systems, such as key sensitivity, periodicity, computational complexity, and resistance to modern attacks, we propose using a Quadratic Chaotic Map (QCM) with an initial condition generated by the Fibonacci series as a promising solution. Unlike methods that require substantial computational power and large datasets, such as Logistic Map with DNN or Henon Map with ANN, QCM provides robust encryption with lower computational overhead. The QCM generates pseudo-random sequences with high sensitivity to initial conditions, making the encryption phenomenon difficult to predict or decipher, thus defending against brute force and quantum-based decryption attempts [26]. Additionally, QCM mitigates the periodicity issue found in methods like the Arnold Cat Map by ensuring even minor changes in initial conditions lead to vastly different outcomes, reducing the risk of periodicity exploitation. This continuous, non-repetitive behavior enhances the overall security and makes QCM significantly more resistant to reverse-engineering attempts. Therefore, integrating QCM into cryptographic systems addresses key security challenges and offers a more secure, efficient, and robust framework for digital data encryption in the face of modern computational threats.

The article is structured as follows: In Section 2, we cover the preliminaries necessary for understanding the research. In Section 3, we detail the proposed encryption algorithm. We present the experimental results for text and image encryption in Section 4. In Section 5, we discuss the performance analysis, comparing it with existing cryptographic methods. Finally, we with the key findings and implications of the study in Section 6.

2. Preliminaries

This section provides essential derivations that will be utilized in various sections of this article. We compare the chaotic properties of the classical quadratic chaotic map with our proposed one. Additionally, we explore the Fibonacci sequence, key space, and the relationship between the chaotic map and the Fibonacci sequence.

2.1. Quadratic chaotic map

QCMs are used to generate sequences that exhibit sensitive dependence on initial conditions, making them useful for applications requiring pseudo randomness, such as in cryptography and optimization algorithms. These are critical in enhancing evolutionary algorithms by avoiding local optima and speeding up convergence. The classical quadratic chaotic map is given by $X_{n+1} = r - X_n^2$, whereas the proposed modified quadratic chaotic map in this article is:

$$X_{n+1} = r + (1 - aX_n^2), \tag{1}$$

where *n* represents the number of iterations, *r* is the chaotic parameter, and *a* is a scaling factor that introduces a nonlinearity in the map, enabling finer control over the chaotic behaviour, which can be tuned to fit specific requirements in applications where varied levels of unpredictability might be desired. We evaluated several analyses, such as iteration property, bifurcation analysis, and the Lyapunov exponent, for both maps as follows:

2.1.1. Iteration property

These properties highlight how the sequence evolves over iterations at different parameter values, illustrating the map's dynamics graphically. This visualization benefits in understanding the practical implications of the theoretical parameters. For a specific value of *X₀*, the iteration plot defines the relationship between the number of iterations and the chaotic map at different values of *r*. The behavior of the classical and proposed quadratic maps can be categorized into three regions based on *r*, as follows:

- Classical QCM

Non-chaotic region: For $r \in [0,0.74]$, values converge to the same result after several iterations, Figure 1 (a).

Periodic: For $r \in [0.74,1.4]$, system exhibits periodic behaviour, Figure 1 (b).

Chaotic region: For $r \in [1.4,2]$, system exhibits chaotic behaviour, Figure 1 (c).

- Proposed modified QCM

For *a = 2*

Chaotic region: For $r \in \{[0,0.15],[0.55,1.15],[1.55,2.15],\ldots\}$, system exhibits chaotic behaviour, Figure 1 (d).

Periodic: For $r \in \{[0.15,0.27],[1.15,1.27],[2.15,2.27],\ldots\}$, system exhibits periodic behaviour, Figure 1 (e).

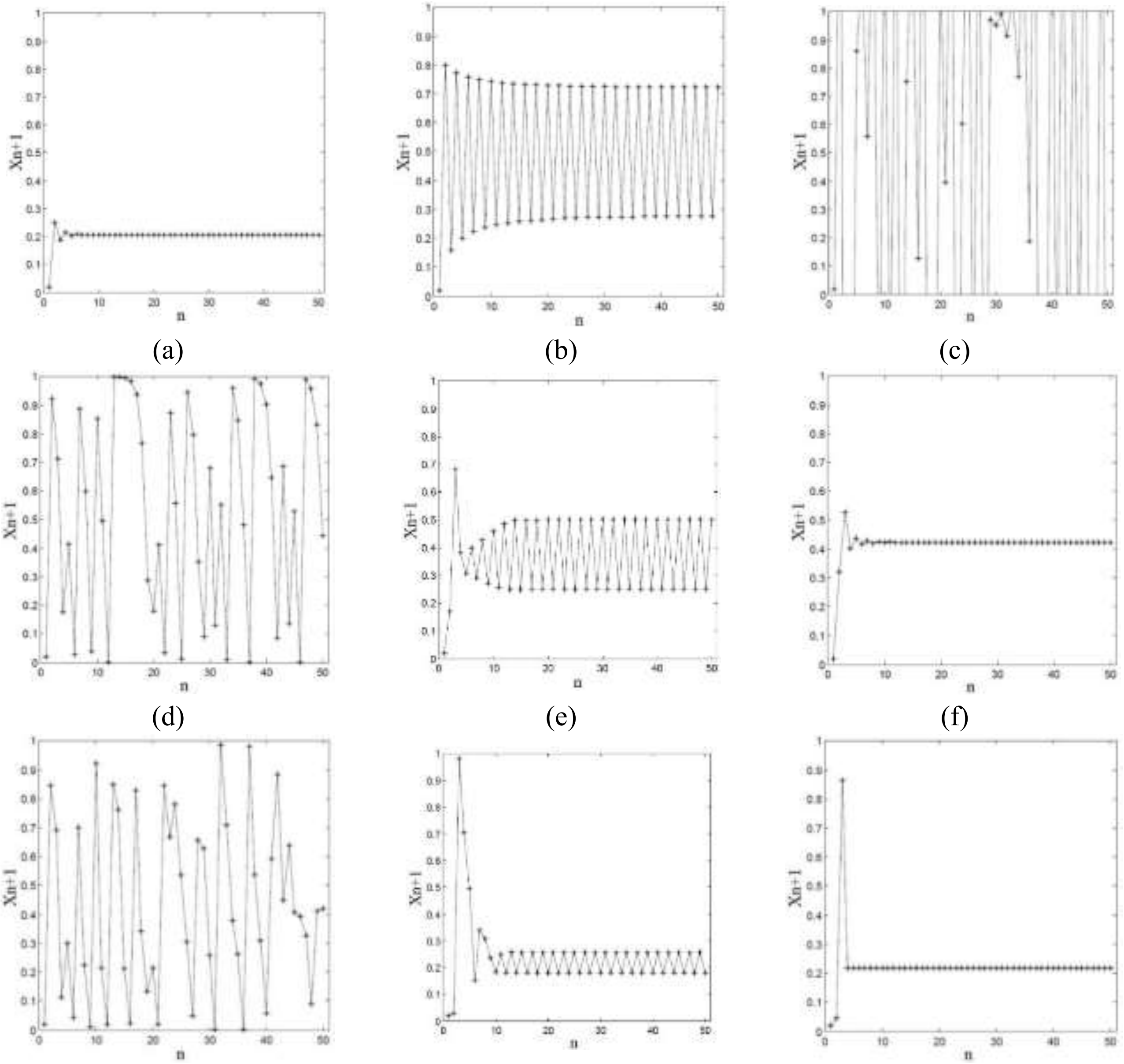
Non-chaotic region: For $r \in \{[0.27,0.55],[1.27,1.55],[2.27,2.55],\dots\}$, values converge to the same result after several iterations, Figure 1 (f).

For *a=4*

Chaotic region: For $r \in \{[0,0.11],[0.27,1.11],[1.27,2.11],\dots\}$, system exhibits chaotic behaviour, Figure 1 (g).

Periodic: For $r \in \{[0.11,0.2],[1.11,1.2],[2.11,2.2],\dots\}$, system exhibits periodic behaviour, Figure 1 (h).

Non-chaotic region: For $r \in \{[0.2,0.27],[1.2,1.27],[2.2,2.27],\dots\}$, same result produced after several iterations, Figure 1 (i).



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 1. Iteration analyses of classical and proposed QCM at $X_0 = 0.02$: (a-c) Iteration analysis of classical map at $r = 0.25, 0.8,$ and 1.9; (d-f) Iteration analysis of proposed QCM at a = 2 and r = 0, 0.25, and 0.4; (g-i) Iteration analysis of proposed QCM at a = 4 and r = 0, 0.18, and 0.2.

2.1.2. Bifurcation analyses

By systematically varying r and observing changes in the system's dynamics, we can identify regions of stability, periodicity, and chaos. This analysis is critical for tuning the parameters in applications to ensure the desired behavior is achieved consistently. The observed behaviors for parameter *r* were as follows:

- Classical QCM

In a classical map, as presented in Figure 2 (a); for the convergence region $r \in [0, 0.74]$, Bifurcation region $r \in [0.74,1.4]$, and Chaos region at $r \in [1.4,2]$.

- Proposed modified QCM

The modified quadratic map with scaling factor a = *2* produces convergence region $r \in \{[0.27,0.55], [1.27,1.55], [2.27,2.55], \dots\}$, bifurcation region $r \in \{[0.15,0.27]$, $[1.15,1.27]$, $[2.15,2.27], \dots\}$ and chaos region $r \in \{[0,0.15], [0.55,1.15], [1.55,2.15], \dots\}$, as presented in Figure 2 (b).

The modified quadratic map with scaling factor a = *4* produces convergence region $r \in \{[0.2,0.27], [1.2,1.27], [2.2,2.27], \dots\}$, bifurcation region $r \in \{[0.11,0.2], [1.11,1.2], [2.11,2.2], \dots\}$ and chaos region $r \in \{[0,0.11], [0.27,1.11], [1.27,2.11], \dots\}$, as presented in Figure 2 (c).

2.1.3. Lyapunov exponent

The Lyapunov exponent, λ, quantifies the rate of separation of infinitesimally close trajectories, providing a measure of the chaotic nature of the map. It measures sensitive dependence for initial conditions as follows [15,16]:

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{\infty} ln|f'(x_i)|. \tag{2}$$

where f' is the derivative of the function f. A positive λ indicates chaos, $\lambda = 0$ indicates stability, and a negative λ indicates non-chaotic behavior. The maximal Lyapunov exponent (MLE) is the largest λ.

- Classical QCM

Positive and chaotic behavior for $r \in [1.4,2]$, with MLE = 0.67, Figure 2 (d).

- Proposed modified QCM

Positive and chaotic behavior for $r \in \{[0,0.15], [0.55,1.15], [1.55,2.15], \dots\}$, with MLE = 0.673 at a given value of $a = 2$, Figure 2 (e).

Positive and chaotic behavior for $r \in \{[0,0.11], [0.27,1.11], [1.27,2.11], \dots\}$, with MLE = 2.025 at a given value of $a = 4$, Figure 2 (f).

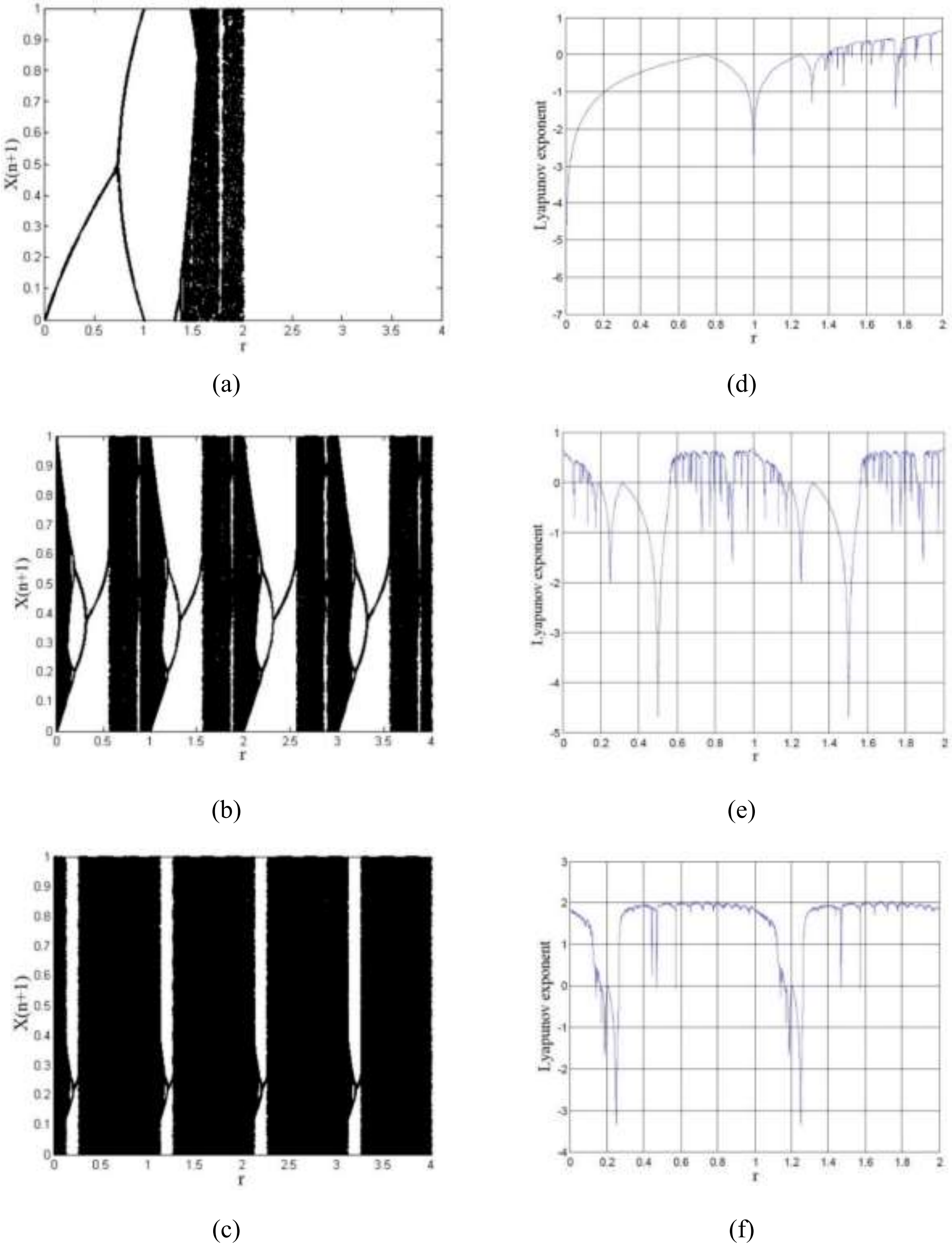


Figure 2. Bifurcation and Lyapunov exponent analyses for classical and proposed QCM at $X_0 = 0.02$: (a) Bifurcation analysis of classical QCM, (b-c) Bifurcation analysis of proposed QCM at $a = 2$ and $a = 4$, (d) Lyapunov exponent of classical QCM, and (e-f) Lyapunov exponent of proposed QCM at $a = 2$ and $a = 4$.

2.2. Fibonacci sequence and key space integration

Utilizing Fibonacci numbers as part of the key space provides a mathematical and natural sequential foundation that can enhance the complexity and security of the key generation process. In cryptography, selecting indications from the Fibonacci sequence based on portions of a key can generate a sequence that is less predictable than linear congruential generators or simple pseudorandom number generators.

In practical implementation, we split a binary key into two parts where one governs the starting point in the Fibonacci sequence and the other adjusts the parameters in the chaotic map, offering a high degree of unpredictability and customization in cryptographic applications. However, the Fibonacci sequence is defined as $X_n = X_{n-1} + X_{n-2}$. The initial numbers are 0 and 1, and each subsequent number is the sum of the previous two.

The key space involves using the Fibonacci sequence and the sequence generated by the proposed chaotic map. For a 16-bit key, the first 8 bits select the Fibonacci series, and the remaining 8 bits select the range of the proposed quadratic chaotic map. For example, the key '35884' converts to binary '1000110000101100'. Splitting it into '10001100' and '00101100' and converting to decimals gives 140 and 44, respectively. The Fibonacci series starts from m140 and the quadratic map from n44 up to the required range.

3. Methodology

We proposed the structure in Figure 3 and explained the methodology steps, which integrate the Fibonacci sequence and the quadratic chaotic map for encryption purposes as follows:

Input Key: The process starts with a cryptographic key, which is used to initialize the system. The key is split into two parts: one for the Fibonacci sequence and the other for the quadratic chaotic map, enhancing the unpredictability and complexity of the system.

Sequence Generation: Using part of the key, a starting point is selected in the Fibonacci sequence. The sequence acts as a source of pseudorandom numbers that are less predictable than traditional linear congruential generators.

Map Initialization: The other part of the key is used to set the parameters of the quadratic chaotic map. The map's equation generates a chaotic sequence based on the initial condition and parameters. The chaotic sequence provides randomness needed for cryptographic security by exploiting the map's sensitivity to initial conditions.

Combining Sequences: The Fibonacci sequence and the quadratic chaotic map sequence are multiplied. This operation combines the characteristics of both sequences to generate a new sequence with enhanced chaotic properties.

Modulo Operation: The modulo operation ensures that the numbers are within the valid range for the specific data type (alphabet for text, color values for images). For text data, the resulting sequence is reduced modulo 26 (the number of letters in the English alphabet) to produce numerical equivalents of letters. For image data, the sequence is reduced to modulo 256 to fit the 8-bit range of RGB color values.

Text and Image Input: The system accepts both text and image inputs for encryption. Text is converted to numerical form based on its alphabet position, while images are broken down into their RGB components.

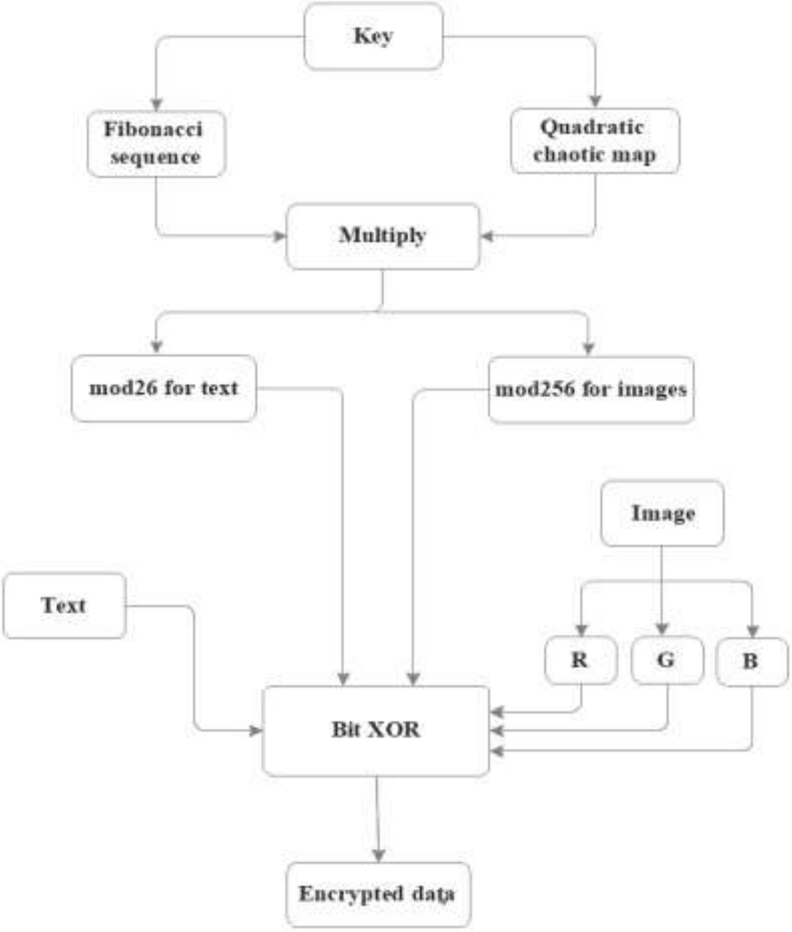


Figure 3. Proposed methodology for data encryption.

Encryption Process: The bitwise XOR operation is performed between the modulo result and the numerical representation of the input data (text or image). XOR is a common cryptographic technique due to its reversibility. It scrambles the data, making it difficult to retrieve without the correct key.

Result: The final output is the encrypted version of the input data, whether it is text or image. This encrypted data is secure and can be decrypted using only the correct key.

The combination of the Fibonacci sequence and the quadratic chaotic map ensures that the encryption is robust, leveraging both mathematical sequences and chaotic dynamics for enhanced security. Moreover, by adjusting the key and map parameters, the system can be tailored to meet specific security requirements or constraints; this methodology is also applicable to both text and image data, making it suitable for various cryptographic applications.

4. Experimental results

The experimentation section evaluates the robustness and sensitivity of the proposed encryption scheme by analyzing its behavior when there is a 1-bit change in the key. The experiments are performed on both texts, in Table 1, and images, in Table 2, by applying the proposed scheme, with key $1000110000101100,\ X_0 = 0.02,\ r = 0$, and $a = 4$, to illustrate the effectiveness and security of the encryption and decryption processes.

4.1. Text analysis

The encryption of text using the defined key and examining the effects of a 1-bit change in the key during decryption are determined as follows:

- Two different texts are encrypted using the same key, as presented in Table 1, resulting in different cipher texts. The encryption process utilizes the combined sequences generated from the quadratic chaotic map and Fibonacci sequence to create a cipher text that is highly dependent on the initial key. This demonstrates the sensitivity of the chaotic map and Fibonacci sequence integration in generating unique outputs.
- The decryption process is attempted with a 1-bit change in the original key, either affecting the quadratic chaotic map or the Fibonacci sequence. Each 1-bit change results in a new cipher that bears no resemblance to the original cipher text or the original plain text, illustrating the scheme's sensitivity to initial conditions. This highlights the security features of the scheme, as a minor alteration in the key significantly alters the decryption output, preventing unauthorized access to the original message. Successful decryption back to the original text is achieved only when the same key used for encryption is applied, ensuring that the encryption and decryption processes are perfectly reversible and secure with the correct key.

Table 1. Encryption and decryption analysis of a proposed scheme at text.

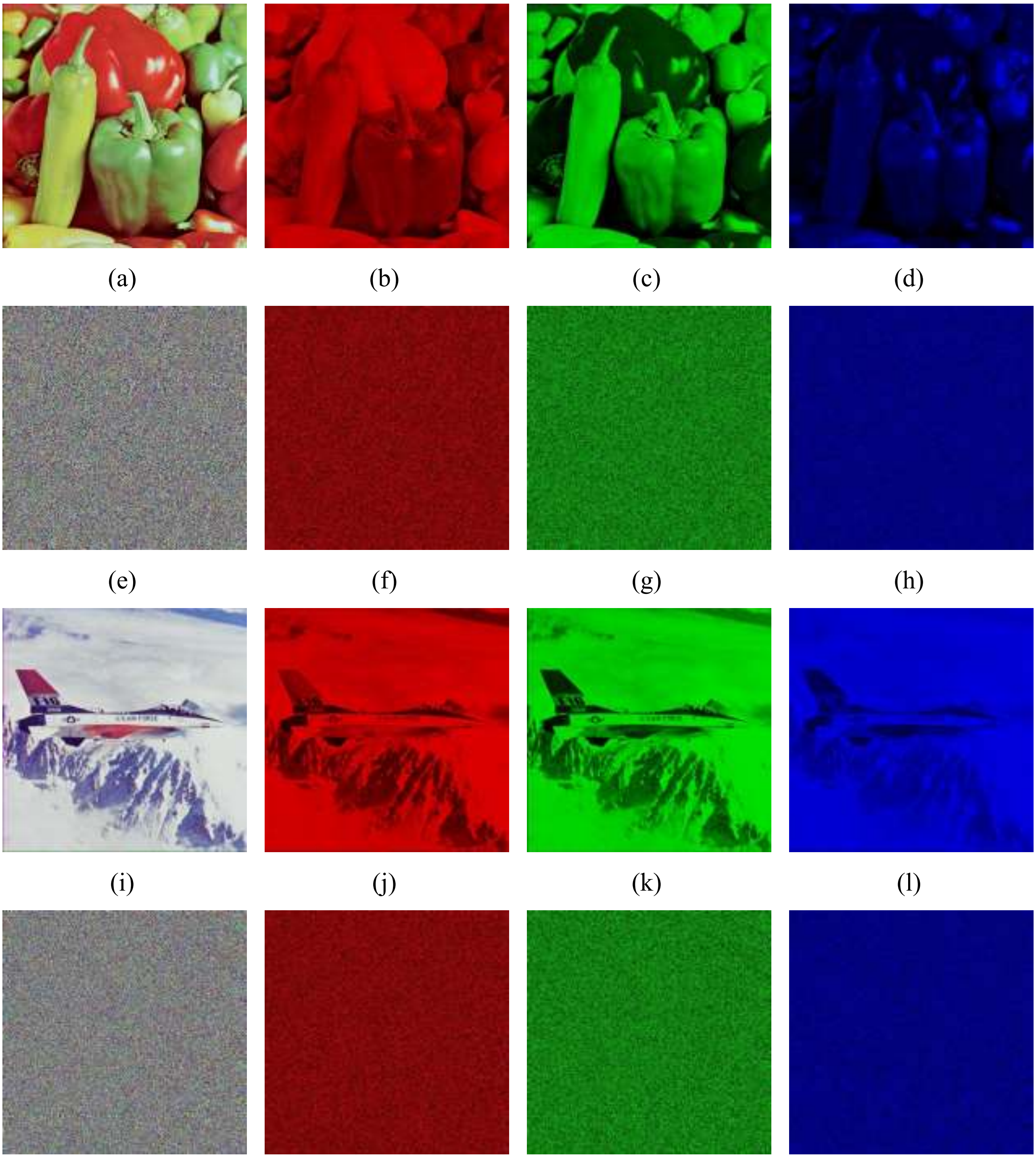
Algorithm	**Text**	**Key**	**Result**
Encryption	UNDIFFERENTIATED	1000110000101100	CDXFTRTYWEQDCVXS
	CHARACTERIZATION	1000110000101100	KHJELBMLHMBFERJG
Decryption	CDXFTRTYWEQDCVXS	1000110000101110	XXTUYBGFFPIDQWQL
	CDXFTRTYWEQDCVXS	1100110000101100	RTNGBHJUEDVCCXOH
	KHJELBMLHMBFERJG	1000110000101101	RHNILKJOSDITGGMI
	KHJELBMLHMBFERJG	1000010000101100	UNHGMYTRSDFEVGER
	CDXFTRTYWEQDCVXS	1000110000101100	UNDIFFERENTIATED
	KHJELBMLHMBFERJG	1000110000101100	CHARACTERIZATION

4.2. Image analysis

The image encryption analysis is performed on samples from the SIPI image database [27], specifically focusing on “pepper” and “airplane” images. The process analyzes the impact on the RGB layers as follows:

- Each pixel's RGB value is processed through the chaotic map and Fibonacci sequence-modulated key to produce an encrypted image. The method encrypts the image by applying the modulo operation (mod 256) to ensure pixel values remain within the valid color range. Different RGB layers are separately encrypted, resulting in scrambled images that reveal no visible information about the original images, depicted in Figure 4.
- Decryption of images is analyzed by altering the key and using the original key to compare results. This process involves testing the sensitivity by altering the 2nd, 5th, 15th, and 16th bits of the key, presented in Table 2. Each alteration results in an image cipher that shows no resemblance to the original image, producing a distinct and scrambled image each time. This test confirms the encryption's resistance to slight changes in the key, ensuring security against brute-force attacks that might attempt

to guess the key. Accurate decryption to the original image is achieved only when the original key is used, confirming that the encryption process is fully reversible and secure when the correct key is employed.



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

Figure 4. Plain and Encrypted layer-wise Pepper and Airplane images: (a-d) Plain Pepper image and its corresponding RGB content, (e-h) Encrypted Pepper image and its corresponding RGB content; (i-l) Plain Airplane image and its corresponding RGB content; and (m-p) Encrypted Pepper image and its corresponding RGB content.

Table 2. Decryption analyses for images with original and 1-bit change in key.

Algorithm	Image	Key	Result
Encryption		1000110000101100	
		1000110000101100	
Decryption		1000110000101110	
		1100110000101100	
		1000110000101101	
		1000010000101100	
		1000110000101100	
		1000110000101100	

The experiments for both text and images demonstrate sensitivity, security, robustness, and practicality. The encryption scheme exhibits high sensitivity to changes in the key. Even a single-bit modification leads to significantly different outcomes, which is a desirable trait in cryptographic applications for preventing unauthorized access. Moreover, the combined use of a quadratic chaotic map and Fibonacci sequence ensures that the encryption process generates highly secure and unpredictable ciphers. The methodology shows robustness in encryption, maintaining data integrity and security even under attempts to use incorrect keys, as well as the ability to apply the same encryption process to both text and images. This highlights the versatility and practical application potential of the proposed scheme in various domains that require secure data transmission and storage.

5. Discussions

To evaluate the performance and sensitivity of the proposed encryption scheme, we conducted a series of tests focusing on encryption and decryption processes. The tests include factual examinations, inconsistency detection, and sensitivity analyses on encrypted images using our developed approach. Various analytical techniques, such as histogram, entropy, correlation, differential attack, pixel similarity and difference, and noise and occlusion attack analyses, were employed to measure the algorithm's performance and resilience against real-world conditions.

5.1. Entropy analysis

Entropy analysis measures the randomness or uncertainty in the pixel distribution of an encrypted image, quantifying the average information content derived from the histogram [28–30]. It can be evaluated as:

$$H = -\sum p(x)\, log_2(p(x)), \tag{3}$$

where $p(x)$ is the probability of a pixel having value x. Higher entropy values suggest a more random pixel distribution and greater security. Ideally, the entropy should be close to 8 for images with 256 gray levels. Table 3 shows entropy values of encrypted images near 8, indicating a high level of randomness and security in the encryption.

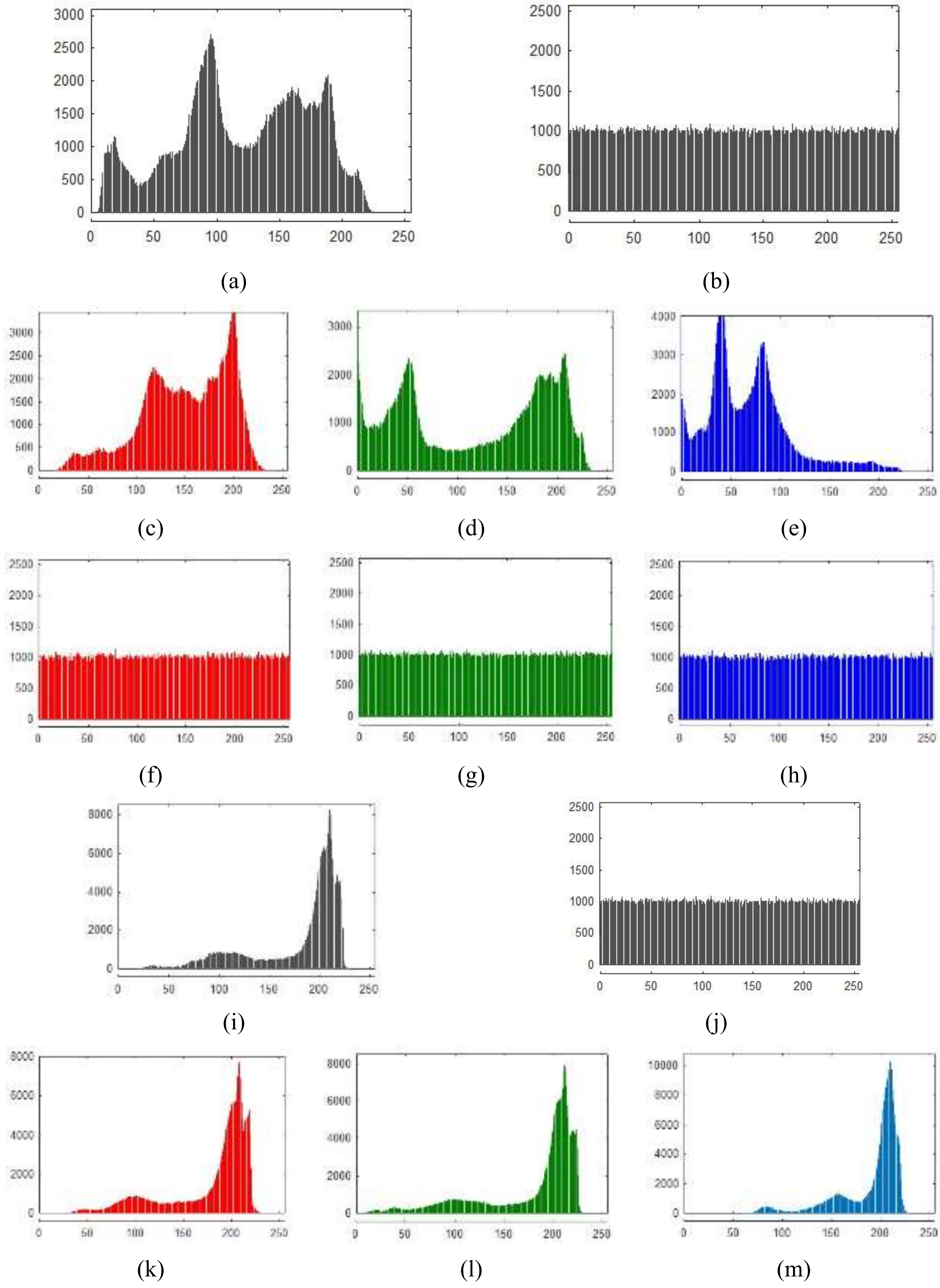
Table 3. Layer wise entropies of plain and encrypted content with the proposed methodology and comparison with SOTA approaches.

Content	Plain (Grey)	Encrypted (Red)	Encrypted (Green)	Encrypted (Blue)	Encrypted (Grey)	Ref. [29]	Ref. [30]
Pepper	7.7253	7.9979	7.9981	7.9989	7.9991	7.9990	7.9993
Airplane	7.6879	7.9980	7.9984	7.9978	7.9993	7.9991	7.9993
Lena	7.7502	7.9984	7.9985	7.9982	7.9992	7.9990	7.9975
Baboon	7.7666	7.9984	7.9981	7.9980	7.9991	7.9991	7.9890
House	7.5112	7.9984	7.9980	7.9982	7.9992	–	–
Sailboat	7.7675	7.9981	7.9983	7.9980	7.9991	7.9989	–

5.2. Histogram analysis

Histogram analysis provides insights into the statistical properties of an image by examining the distribution of pixel intensity values. This analysis detects irregularities, assesses uniformity, and identifies potential weaknesses in the encryption procedure [31,32]. We observed the histograms of the encrypted Pepper and Airplane images (Figure 5) show no discernible patterns or information about the original content, confirming the encryption scheme's robustness against statistical attacks.

Moreover, uniform histograms of encrypted images indicate strong resistance to statistical attacks, as they differ significantly from those of plain images, demonstrating the effectiveness of the proposed algorithm.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

(i)

(j)

(k)

(l)

(m)

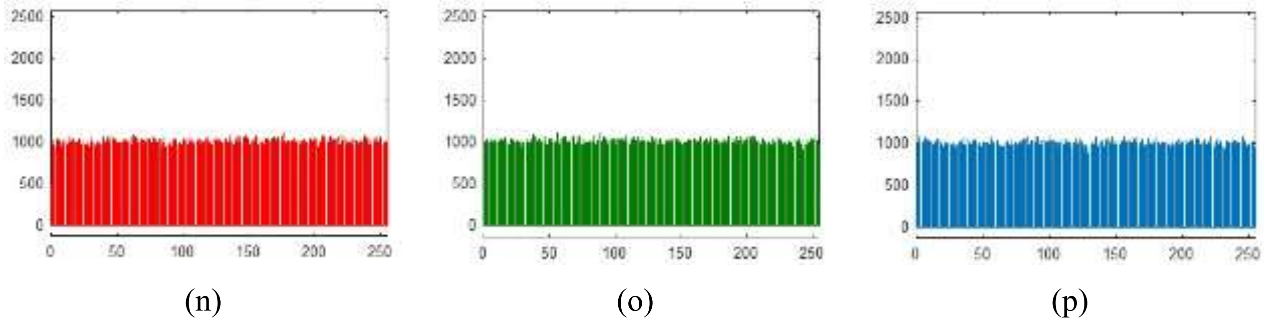


Figure 5. Histograms of plain and encrypted Pepper and Airplane images: (a-b) Histograms of Gray content for pepper image; (c-h) Histograms of RGB content for the pepper image; (i-j) Histograms of Gray content for the Airplane image; and (k-p) Histograms of RGB content for the Airplane image.

5.3. Correlation analysis

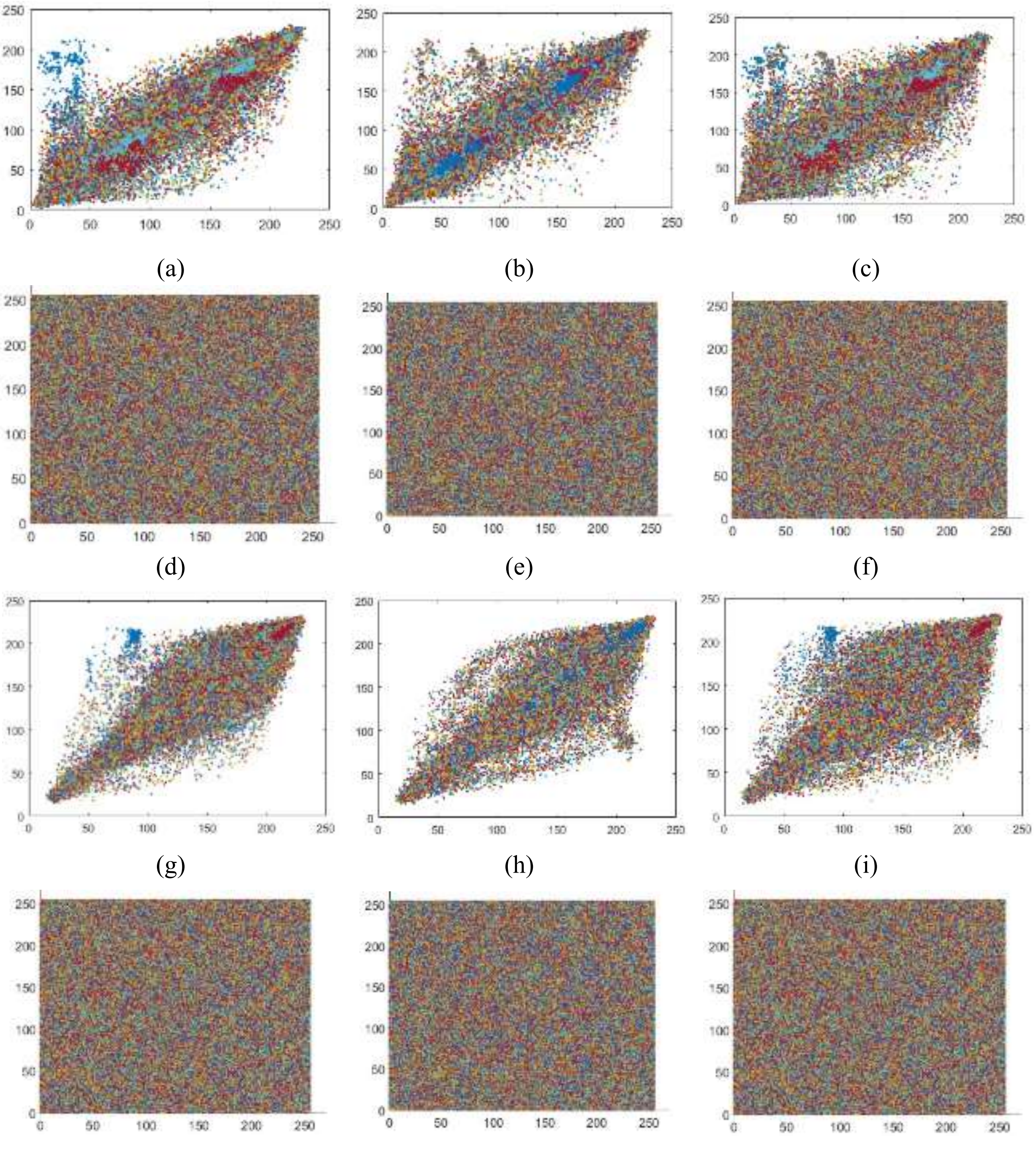
Correlation analysis evaluates the statistical relationships between pixel values within an encrypted image, focusing on how changes in one pixel affect adjacent pixels [33–35]. It can be evaluated as:

$$\rho = \frac{Cov(X,Y)}{\sigma_X \sigma_Y}, \tag{4}$$

where $Cov(X,Y)$ is the covariance, and σ_X and σ_Y are the standard deviations of X and Y. Correlation coefficients for adjacent pixels in encrypted images are close to zero (Table 4), indicating that the encryption scheme effectively disrupts patterns present in the original images. Scatter plots of pixel values in encrypted images (Figure 6 (d–f, j–l)) show no convergence towards a line, demonstrating the encryption's strength.

Table 4. Correlation coefficients for the plain and encrypted contents and comparison with SOTA.

Content	Plain image			Encrypted image (proposed)			Ref. [33]		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Pepper	0.9757	0.9779	0.9635	-0.0111	-0.0133	0.0052	−0.0236	−0.0084	−0.0351
Airplane	0.9662	0.9639	0.9368	-0.0092	-0.0141	0.0052	−0.0057	−0.0246	−0.0034
Lena	0.9719	0.9850	0.9593	-0.0083	-0.0140	0.0023	−0.0054	−0.0236	−0.0535
Baboon	0.8534	0.7598	0.7300	-0.0091	-0.0122	0.0025	−0.0166	−0.0243	−0.1016
House	0.9479	0.957	0.9132	-0.0082	-0.0032	-0.0026	−0.0187	−0.0038	−0.0356
Sailboat	0.9737	0.9700	0.9569	-0.0029	-0.0014	0.0002	−0.0166	−0.0035	−0.0189



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Figure 6. Correlation analysis of horizontal, vertical, and diagonal adjacent pixels for Pepper and Airplane images. (a-f) Correlation analysis for the plain and encrypted content of Pepper image, (g-l) Correlation analysis for the plain and encrypted content of Airplane image.

5.4. *Differential attack analysis*

Differential attack analysis assesses the encryption scheme's resistance to minor changes in the plaintext, using metrics such as NPCR (Number of Pixel Change Rate) and UACI (Unified Average Change Intensity) [36–38]. NPCR and UACI can be evaluated as:

$$NPCR = \frac{N-M}{N} \times 100\% \tag{5}$$

$$UACI = \frac{1}{N}\sum_{i=1}^{N}\frac{|C_i - C_i{}'|}{L} \times 100\% \tag{6}$$

where *N* is the total number of pixels, and *M* is the number of unchanged pixels, C_i and C_i' are pixel values in the original and modified ciphertexts, respectively, and *L* is the maximum pixel value. High NPCR and UACI values (Table 5) indicate strong resistance to differential attacks, with significant changes in ciphertext resulting from minor changes in plaintext.

Table 5. Differential analysis for the encrypted contents with the proposed methodology and comparison with SOTA.

	Proposed	Ref. [36]	Ref. [37]	Ref. [38]				
Content	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Pepper	99.89	33.48	99.60	33.48	99.57	33.26	99.89	33.38
Airplane	99.92	33.47	99.61	33.50	99.63	33.58	99.95	33.34
Lena	99.91	33.49	–	–	–	–	99.91	33.41
Baboon	99.91	33.42	99.60	33.42	99.62	33.26	99.88	33.36
House	99.88	33.43	99.61	33.43	–	–	99.86	33.31
Sailboat	99.92	33.41	99.60	33.45	99.62	33.39	99.89	33.37

5.5. *Pixels' similarity analyses*

Pixel similarity analysis quantifies the resemblance of correlated pixel values across different image regions. This analysis helps to assess how well the encryption scheme obscures the original image information [39]. The following measures were used:

5.5.1. Structural Similarity Index Matrix (SSIM)

SSIM evaluates the similarity between two images based on luminance, contrast, and structure. It provides a comprehensive measure of image quality by considering changes in structural information [40]. It can be evaluated as:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \tag{7}$$

where μ_x and μ_y are means of images *x* and *y,* σ_x and σ_y are standard deviations of *x* and *y,* σ_{xy} is covariance of *x* and *y, and* C_1 and C_2 are Constants for stability.

5.5.2. Normalized Cross-Correlation (NCC)

NCC measures the similarity between two images by assessing the cross-correlation of their pixel values. It is effective for detecting shifts and correlations in the image structure [41]. It can be evaluated as:

$$\mathrm{NCC}(x,y)=\frac{\Sigma(x_i-\mu_x)(y_i-\mu_y)}{\sqrt{\Sigma(x_i-\mu_x)^2\,\Sigma(y_i-\mu_y)}^2}, \tag{8}$$

where x_i and y_i are pixel values at corresponding positions, and μ_x and μ_y represent means of images *x* and *y*.

5.5.3. Gradient Similarity Index (GSI)

GSI evaluates the structural content by comparing image gradients [42]. It is particularly useful for assessing edge preservation in the encryption process and can be evaluated as:

$$\mathrm{GSI}(x,y)=\frac{2\sigma_x\sigma_y+C_3}{\sigma_x^2\sigma_y^2+C_3}, \tag{9}$$

where σ_x and σ_y are standard deviations of gradients of images *x* and *y*, and C_3 is a constant for stability.

Table 6 provides an overview of the similarity analysis results, revealing notable distinctions in structural attributes between original and encrypted content. The anticipated values for NCC and GSI approach zero, indicating significant dissimilarity among content variations.

Table 6. Pixels' similarity analysis for the plain-encrypted contents with the proposed methodology and comparison with SOTA.

Content	Proposed			Ref. [40]			Ref. [41]		
	SSIM	NCC	GSI	SSIM	NCC	GSI	SSIM	NCC	GSI
Pepper	0.00224	0.0028	0.0025	0.00113	0.0035	0.0029	0.3406	0.3039	0.2570
Airplane	0.00121	00.32	0.0029	–	–	–	0.3429	0.2858	0.2708
Lena	0.00132	0.0029	0.0028	0.00192	0.0027	0.0023	0.3016	0.3074	0.3098
Baboon	0.00142	0.0034	0.0021	0.00161	0.0038	0.0016	0.4008	0.3495	0.3496
House	0.00128	0.0022	0.0019	0.00124	0.0018	0.0019	0.2795	0.3200	0.2487
Sailboat	0.00124	0.0031	0.0023	0.00126	0.0035	0.0018	0.3586	0.3681	0.3622

5.6. Pixels' difference analyses

Pixel disparity analysis investigates differences between corresponding pixels in two images, providing insights into the performance of various image processing techniques, including encryption methods using three common measures, outlined in Table 7, as follows:

Table 7. Pixels' difference analysis for the plain-encrypted contents with the proposed methodology and comparison with SOTA.

Content	Proposed			Ref. [43]			Ref. [44]		
	MAE	MSE	PSNR	MAE	MSE	PSNR	MAE	MSE	PSNR
Pepper	85.24	10189.31	7.62	75.25	8334	8.92	82.01	10074.0	8.098
Airplane	79.81	10207.17	7.58	85.41	10,933	7.74	–	–	–
Lena	81.75	9985.43	7.56	78.89	9290	8.45	77.40	8890.05	8.641
Baboon	84.55	10048.52	7.68	76.48	8643	8.76	75.33	8345.25	8.916
House	78.89	9991.82	7.72	–	–	–	75.31	8361.44	8.907
Sailboat	82.73	10119.24	7.79	–	–	–	82.01	10063.3	8.103

5.6.1. Mean absolute error (MAE)

MAE determines the average absolute difference between corresponding pixels in two images. It provides a straightforward measure of the average magnitude of errors [43]. It can be computed as:

$$\mathrm{MAE}(x, y) = \frac{1}{N}\sum_{i=1}^{N}|x_i - y_i|, \tag{10}$$

where N signifies the total number of pixels, and x_i and y_i are pixel values at corresponding positions.

5.6.2. Mean squared error (MSE)

MSE estimates the average squared differences between corresponding pixels, emphasizing larger discrepancies compared to MAE [44]. It can be computed as:

$$\mathrm{MSE}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2. \tag{11}$$

5.6.3. Peak Signal-to-Noise Ratio (PSNR)

PSNR assesses the ratio between the maximum possible signal value and the introduced noise, providing a measure of the quality of the encrypted image [45]. It can be evaluated as:

$$\mathrm{PSNR}(x, y) = 10 \cdot log_{10}\left(\frac{MAX^2}{MSE(x,y)}\right), \tag{12}$$

where *MAX* represents the maximum possible pixel value (e.g., 255 for 8-bit images). Table 7, affirms substantial variance in pixel values between the source and encrypted images. MSE and PSNR variations indicate improved encryption quality with higher MSE and lower PSNR or vice versa.

5.7. Pixels' fidelity analyses

Pixels' fidelity analyses determine the quality of encryption by maintaining image fidelity, ensuring encrypted images retain their integrity and are resistant to unauthorized access and tampering. We computed the fidelity among pixels in source and encrypted images using three common measures [46], outlined in Table 6, as follows:

5.7.1. Normalized absolute error (NAE)

NAE quantifies the average relative difference between corresponding pixels in the original and encrypted images, providing a normalized view of errors. It can be evaluated as:

$$\mathrm{NAE} = \frac{1}{N}\frac{\sum|x_i - y_i|}{(L-1)}, \tag{13}$$

where N is the total number of pixels, x and y are pixel values at corresponding positions in the original and encrypted images, and L is the range of possible pixel values (e.g., 256 for an 8-bit image).

5.7.2. Average difference (AD)

AD calculates the average absolute difference between plaintext and ciphertext pixel values, providing a measure of overall discrepancy. It can be computed as:

$$\mathrm{AD} = \frac{1}{N}\sum|x_i - y_i|. \tag{14}$$

5.7.3. Maximum difference (MD)

MD quantifies the maximum absolute difference between corresponding pixel values, highlighting the most significant variation. It can be computed as follows:

$$\mathrm{MD} = max|x_i - y_i|. \tag{15}$$

Lower NAE and AD, in Table 8, indicate minimal relative differences, maintaining close alignment of pixel values between the original and encrypted images.

Table 8. Pixels' fidelity analysis for the plain-encrypted contents with the proposed methodology and comparison with SOTA.

Content	Proposed			Ref. [39]			Ref. [41]		
	NAE	AD	MD	NAE	AD	MD	NAE	AD	MD
Pepper	0.0349	0.0186	221	0.6306	7.9524	226	0.0494	0.0195	143
Airplane	0.0334	0.0136	234	0.4639	5.1054	231	0.0375	0.0236	127.5
Lena	0.0354	0.0154	223	0.5926	4.1009	235	0.0480	0.0198	110.3
Baboon	0.0312	0.0164	219	0.5870	5.9597	210	0.0231	0.0516	138.9
House	0.0310	0.0149	231	–	–	–	0.0296	0.0170	124.3
Sailboat	0.0325	0.0162	233	–	–	–	0.0617	0.0239	112.2

5.8. Noise and occlusion attack analyses

The noise and occlusion attack analyses are crucial for evaluating the resilience of the proposed encryption scheme against real-world disruptions, such as random noise interference and partial image obstructions. These analyses help determine the effectiveness of the scheme in maintaining image integrity and ensuring secure data transmission.

5.8.1. Noise attack analysis

Noise attacks simulate random disturbances in images, often introduced by environmental factors or data corruption during transmission. The analysis assesses the algorithm's ability to withstand these disturbances without significant degradation of the encrypted image. Gaussian noise, which is commonly used to simulate real-world noise, is added to the original image [47]. The noise model is defined as:

$$I_{ns} = I_{org} + G, \tag{16}$$

where I_{ns} is the noisy image, I_{org} is the original image, and G is the Gaussian noise with a specified mean and variance. The objective is to evaluate the encryption scheme's robustness by measuring the impact of noise on the encrypted image. This involves assessing how well the algorithm preserves the image's integrity despite noise interference.

Gaussian noise with normalized power levels of 0.000001, 0.000003, 0.000005, and 0.000007 was introduced to the images. The analysis, presented in Table 9, demonstrates that the proposed encryption framework exhibits strong resilience against noise attacks. The PSNR values remain relatively high, indicating that the encryption scheme effectively mitigates the impact of noise, maintaining the integrity and quality of the encrypted image.

Table 9. Noise and Occlusion Analysis.

		Noise intensity			Occlusion analysis		
Content	Trial	0.000001	0.000003	0.000005	1/4	1/2	3/5
Pepper	MSE	9987.16	9678.8	9104.6	6421.17	4784.18	3445.27
	PSNR	7.78	7.86	7.99	10.61	12.22	13.41
Airplane	MSE	9884.7	9452.7	9122.8	6552.54	4881.02	3398.13
	PSNR	7.71	7.82	7.94	10.56	12.64	13.94
Lena	MSE	9675.4	9428.8	9212.5	6514.19	5101.25	3568.74
	PSNR	7.68	7.79	7.92	11.05	13.12	13.48
Baboon	MSE	9882.7	9613.4	9302.5	6445.56	4478.32	3524.15
	PSNR	7.77	7.89	7.98	10.54	12.46	13.24
House	MSE	9718.7	9505.7	9298.4	5998.54	4495.48	3488.34
	PSNR	7.79	7.88	7.98	11.45	12.85	13.79
Sailboat	MSE	9798.7	9598.2	9346.2	6325.45	4615.45	3152.41
	PSNR	7.86	7.97	8.01	11.33	12.81	13.37

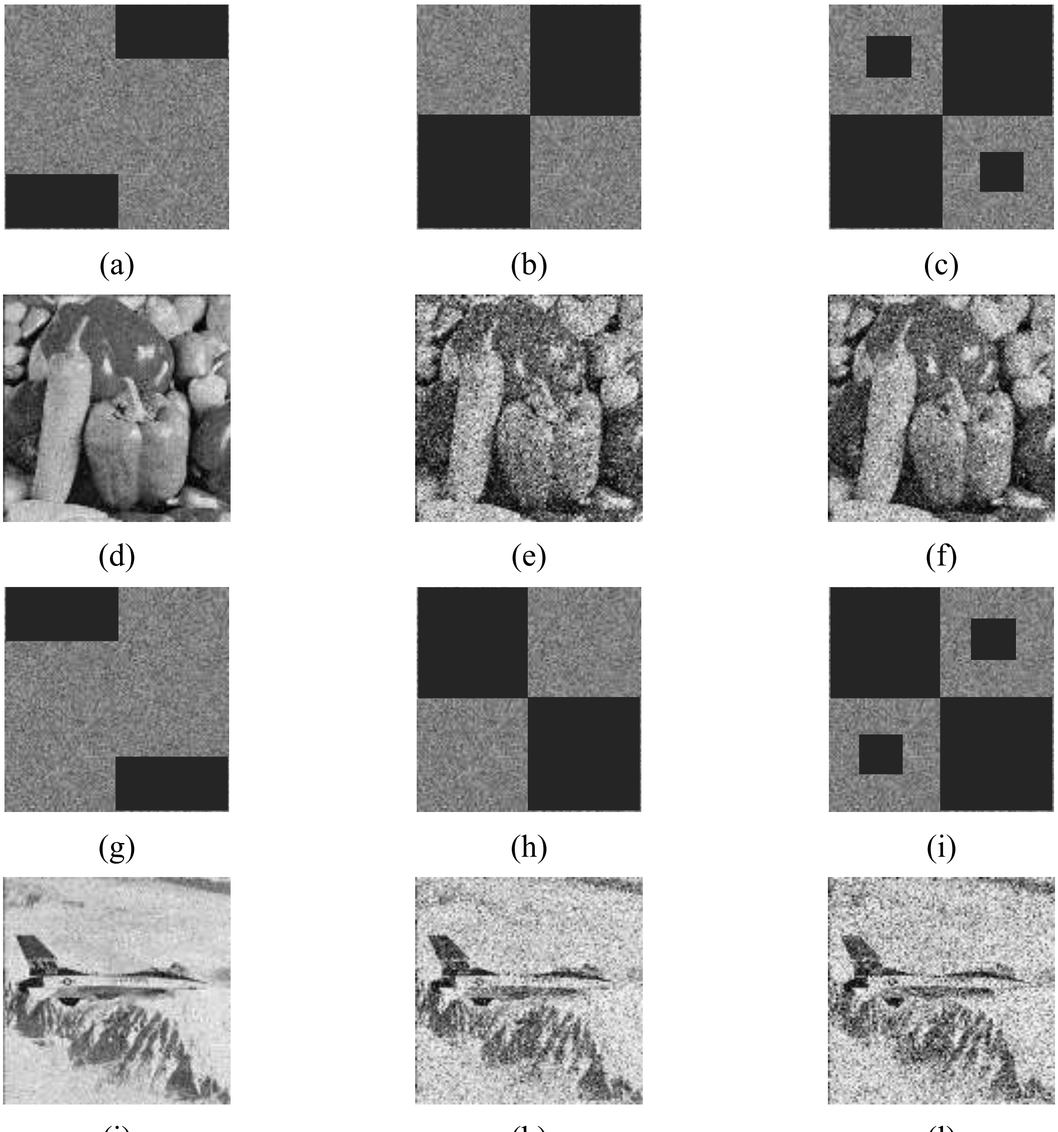
5.8.2. Occlusion attack analysis

Occlusion attacks involve concealing parts of an image, simulating scenarios where portions of the data are obstructed or missing. This analysis tests the algorithm's ability to recover and decrypt the original image despite partial data loss [48]. Occlusion is modeled by applying a binary mask to the original image, creating regions of complete or partial data loss:

$$I_{oc} = I_{org} \odot B, \tag{17}$$

where I_{oc} is the occluded image and B is a binary mask indicating the occluded regions.

The goal is to assess the encryption scheme's robustness in retrieving the original image when faced with occlusion. The analysis evaluates how effectively the algorithm can reconstruct the image and restore lost information. Occlusion attack analysis was performed on images with occluded areas representing fractions of 1/4, 1/2, and 3/5 of the total image area. These varying levels of occlusion simulate different degrees of data loss. The outcomes, summarized in Table 9 and illustrated in Figure 7, indicate that the proposed algorithm demonstrates a strong capacity to recover the original image even when up to 60% of the image is occluded. Despite significant data loss, the algorithm maintains the ability to reconstruct the essential features of the original image, highlighting its effectiveness in overcoming occlusion attacks.


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Figure 7. Occlusion analysis for the encrypted Pepper and Airplane images. (a, d; g, j) Occluded by fraction of 1/4 and corresponding recovered images; (b, e; h, k) Occluded by fraction of 1/2 and corresponding recovered images; and (c, f; i, l) Occluded by fraction of 3/5 and corresponding recovered image.

6. Conclusions

We present an innovative encryption scheme that integrates the quadratic chaotic map (QCM) with the Fibonacci sequence, addressing critical challenges in contemporary cryptographic systems. The proposed method effectively leverages chaotic dynamics to enhance security and unpredictability in encryption processes for both text and image data. By utilizing the inherent sensitivity and nonlinearity of chaotic maps, the scheme provides robust protection against brute-force and quantum-based decryption attempts while mitigating the risks of periodicity found in traditional methods like the Arnold Cat map. Comprehensive experimentation confirms the encryption scheme's sensitivity to key variations, ensuring that even minimal changes in the key produce significantly different encryption outputs. This characteristic, combined with the robustness demonstrated in noise and occlusion attack analyses, highlights the method's resilience against real-world disruptions and unauthorized access attempts. Furthermore, the methodology's adaptability across various data types underscores its practical application potential in diverse domains requiring secure data transmission and storage. Overall, the proposed QCM-based encryption framework offers a promising solution for modern cryptographic challenges, providing a secure, efficient, and versatile approach to digital data protection. Future research may focus on optimizing computational efficiency and exploring additional applications to further strengthen the scheme's utility in emerging technological landscapes.

Author contributions

Majid Khan conceptualized and designed the encryption framework, developed the theoretical foundation for the chaotic map, and contributed to the analysis of the algorithm’s performance and security. Hafiz Muhammad Waseem implemented the algorithm, conducted experiments, and validated results through simulations and comparative studies. He also contributed to writing the manuscript and interpreting the results. Both authors reviewed and approved the final version of the manuscript.

Acknowledgments

This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2024/R/1445).

Conflict of interest

The authors declare no conflicts of interest.

References

1. B. S. Kumar, R. Revathi, An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network, *J. Eng. Appl. Sci.,* **71** (2024), 41. https://doi.org/10.1186/s44147-023-00349-8
2. C. Wang, Y. Zhang, A novel image encryption algorithm with deep neural network, Signal Process., **196** (2022), 108536. https://doi.org/10.1016/j.sigpro.2022.108536

3. A. Ampavathi, G. Pradeepini, T. V. Saradhi, Optimized deep learning-enabled hybrid logistic piece-wise chaotic map for secured medical data storage system, *Int. J. Inf. Technol. Decis. Mak.*, **22** (2023), 1743–1775. https://doi.org/10.1142/S0219622022500869
4. H. Lee, Y. Lee, Optimizations of privacy-preserving DNN for low-latency inference on encrypted data, *IEEE Access*, **11** (2023), 104775–104788. https://doi.org/10.1109/ACCESS.2023.3318433
5. U. Sirisha, B. S. Chandana, Privacy preserving image encryption with optimal deep transfer learning-based accident severity classification model, *Sensors*, **23** (2023), 519. https://doi.org/10.3390/s23010519
6. W. S. Admass, Y. Y. Munaye, A. Diro, Cyber security: State of the art, challenges and future directions, *Cyber Security Appl.,* **2** (2023), 100031. https://doi.org/10.1016/j.csa.2023.100031
7. P. Singh, S. Dutta, P. Pranav, Optimizing GANs for cryptography: The role and impact of activation functions in neural layers assessing the cryptographic strength, *Appl. Sci.,* **14** (2024), 2379. https://doi.org/10.3390/app14062379
8. Y. Chen, S. Xie, J. Zhang, A hybrid domain image encryption algorithm based on improved henon map, *Entropy,* **24** (2022), 287. https://doi.org/10.3390/e24020287
9. M. Devipriya, M. Sreenivasan, M. Brindha, Reconfigurable architecture for image encryption using a three-layer artificial neural network, *IETE J. Res.,* **70** (2024), 473–86. https://doi.org/10.1080/03772063.2022.2127940
10. R. B. Naik, U. Singh, A review on applications of chaotic maps in pseudo-random number generators and encryption, *Ann. Data Sci.,* **11** (2024), 25–50. https://doi.org/10.1007/s40745-021-00364-7
11. A. Chattopadhyay, P. Hassanzadeh, D. Subramanian, Data-driven predictions of a multiscale Lorenz 96 chaotic system using machine-learning methods: reservoir computing, artificial neural network, and long short-term memory network, *Nonlinear Process. Geophys.,* **27** (2020), 373–389. https://doi.org/10.5194/npg-27-373-2020
12. K. Yang, Q. Duan, Y. Wang, T. Zhang, Y. Yang, R. Huang, Transiently chaotic simulated annealing based on intrinsic nonlinearity of memristors for efficient solution of optimization problems, *Sci. Adv.,* **6** (2020), eaba9901. https://doi.org/10.1126/sciadv.aba9901
13. F. Masood, W. Boulila, A. Alsaeedi, J. S. Khan, J. Ahmad, M. A. Khan, et al., A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map, *Multimedia Tools Appl.,* **81** (2022), 30931–30959. https://doi.org/10.1007/s11042-022-12844-w
14. S. I. Batool, H. M. Waseem, A novel image encryption scheme based on Arnold scrambling and Lucas series, *Multimedia Tools Appl.,* **78** (2019), 27611–27637. https://doi.org/10.1007/s11042-019-07881-x
15. J. Ye, X. Deng, A. Zhang, H. Yu, A novel image encryption algorithm based on improved Arnold transform and chaotic pulse-coupled neural network, *Entropy.,* **24** (2022), 1103. https://doi.org/10.3390/e24081103
16. B. Zhang, L. Liu, Chaos-based image encryption: Review, application, and challenges, *Mathematics.,* **11** (2023), 2585. https://doi.org/10.3390/math11112585
17. C. Qin, J. Hu, F. Li, Z. Qian, X. Zhang, JPEG image encryption with adaptive DC coefficient prediction and RS pair permutation, *IEEE Trans. Multimedia,* **25** (2022), 2528–2542. https://doi.org/10.1109/TMM.2022.3148591
18. Y. Peng, C. Fu, G. Cao, W. Song, J. Chen, C. W. Sham, JPEG-compatible joint image compression and encryption algorithm with file size preservation, *ACM T. Multim. Comput.,* **20** (2024), 1–20. https://doi.org/10.1145/363345

19. M. A. Cardona-López, R. O. Flores-Carapia, V. M. Silva-García, E. D. Vega-Alvarado, M. D. González-Ramírez, A comparison between EtC and SPN systems: The security cost of compatibility in JPEG images, *IEEE Access.,* **36** (2024), 1–14. https://doi.org/10.1109/ACCESS.2024.3458808
20. Q. Wang, X. Zhang, X. Zhao, Image encryption algorithm based on improved Zigzag transformation and quaternary DNA coding, *J. Inf. Secur. Appl.,* **70** (2022), 103340. https://doi.org/10.1016/j.jisa.2022.103340
21. Z. Guo, P. Sun, Improved reverse zigzag transform and DNA diffusion chaotic image encryption method, *Multimedia Tools Appl.,* **81** (2022), 11301–11323. https://doi.org/10.1007/s11042-022-12269-5
22. H. Wen, Z. Xie, Z. Wu, Y. Lin, W. Feng, Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography, *J. King Saud Univ. Comput. Inf. Sci.,* **36** (2024), 101871. https://doi.org/10.1016/j.jksuci.2023.101871
23. Y. Yang, L. Huang, N. V. Kuznetsov, B. Chai, Q. Guo, Generating multiwing hidden chaotic attractors with only stable node-foci: Analysis, implementation, and application, *IEEE Trans. Ind. Electron.,* **71** (2023), 3986–3995. https://doi.org/10.1109/TIE.2023.3273242
24. L. Xu, J. Zhang, A novel four-wing chaotic system with multiple attractors based on hyperbolic sine: Application to image encryption, *Integration.,* **87** (2022), 313–331. https://doi.org/10.1016/j.vlsi.2022.07.012
25. J. Zhang, J. Yang, L. Xu, X. Zhu, The circuit realization of a fifth-order multi-wing chaotic system and its application in image encryption, *Int. J. Circ. Theory Appl.,* **51** (2023), 1168–1186. https://doi.org/10.1002/cta.3490
26. M. W. Hafiz, S. O. Hwang, A probabilistic model of quantum states for classical data security, *Front. Phys.,* **18** (2023), 51304. https://doi.org/10.1007/s11467-023-1293-3
27. A. G. Weber, The USC-SIPI image database: *Version* 5, 2006. http://sipi.usc.edu/database/
28. S. I. Batool, M. Amin, H. M. Waseem, Public key digital contents confidentiality scheme based on quantum spin and finite state automation, *Phys. A Stat. Mech. Appl.,* **537** (2020), 122677. https://doi.org/10.1016/j.physa.2019.122677
29. S. Patel, A. Vaish, Block based visually secure image encryption algorithm using 2D-compressive sensing and nonlinearity, *Optik.,* **272** (2023), 170341. https://doi.org/10.1016/j.ijleo.2022.170341
30. Y. Peng, Z. Lan, K. Sun, W. Xu, A simple color image encryption algorithm based on a discrete memristive hyperchaotic map and time-controllable operation, *Opt. Laser Technol.,* **165** (2023), 109543. https://doi.org/10.1016/j.optlastec.2023.109543
31. H. M. Waseem, A. Alghafis, M. Khan, An efficient public key cryptosystem based on dihedral group and quantum spin states, *IEEE Access,* **8** (2020), 71821–71832. https://doi.org/10.1109/ACCESS.2020.2987097
32. A. Nabilah, L. Said, M. Khan, Construction of optimum multivalued cryptographic Boolean function using artificial bee colony optimization and multi-criterion decision-making, *Soft Comput.,* **28** (2024), 5213–5223. https://doi.org/10.1007/s00500-023-09267-6
33. N. Rani, S. R. Sharma, V. Mishra, Grayscale and colored image encryption model using a novel fused magic cube, *Nonlinear Dyn.,* **108** (2022), 1773–1796. https://doi.org/10.1007/s11071-022-07276-y
34. Q. Lai, G. Hu, U. Erkan, A. Toktas, A novel pixel-split image encryption scheme based on 2D Salomon map, *Expert Syst. Appl.,* **213** (2023), 118845. https://doi.org/10.1016/j.eswa.2022.118845
35. H. M. Waseem, S. S. Jamal, I. Hussain, M. Khan, A novel hybrid secure confidentiality mechanism for medical environment based on Kramer's spin principle, *Int. J. Theor. Phys.,* **60** (2021), 314–330. https://doi.org/10.1007/s10773-020-04694-9

36. X. Liu, X. Tong, Z. Wang, M. Zhang, Uniform non-degeneracy discrete chaotic system and its application in image encryption, *Nonlinear Dyn.,* **108** (2022), 653–682. https://doi.org/10.1007/s11071-021-07198-1
37. N. R. Zhou, L. J. Tong, W. P. Zou, Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation, *Signal Process.,* **211** (2023), 109107. https://doi.org/10.1016/j.sigpro.2023.109107
38. A. Alghafis, H. M. Waseem, M. Khan, S. S. Jamal, A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states, *Phys. A Stat. Mech. Appl.,* **554** (2020), 123908. https://doi.org/10.1016/j.physa.2019.123908
39. M. W. Hafiz, W. K. Lee, S. O. Hwang, M. Khan, A. Latif, Discrete logarithmic factorial problem and Einstein crystal model based public-key cryptosystem for digital content confidentiality, *IEEE Access.,* **10** (2022), 102119–102134. https://doi.org/10.1109/ACCESS.2022.3207781
40. N. Abughazalah, A. Latif, M. W. Hafiz, M. Khan, A. S. Alanazi, I. Hussain, Construction of multivalued cryptographic Boolean function using recurrent neural network and its application in image encryption scheme, *Artif. Intell. Rev.,* **56** (2023), 5403–5443. https://doi.org/10.1007/s10462-022-10295-1
41. K. S. Krishnan, B. Jaison, S. P. Raja, Secured color image compression based on compressive sampling and Lü system, *Inf. Technol. Control.,* **49** (2020), 346–369. https://doi.org/10.5755/j01.itc.49.3.25901
42. S. O. Hwang, H. M. Waseem, N. Munir, Billiard quantum chaos: A pioneering image encryption scheme in the post-quantum era, *IEEE Access.*, **12** (2024), 39840–39853. https://doi.org/10.1109/ACCESS.2024.3415083
43. M. Ahmad, S. Agarwal, A. Alkhayyat, A. Alhudhaif, F. Alenezi, A. H. Zahid, et al., An image encryption algorithm based on new generalized fusion fractal structure, *Inf. Sci.,* **592** (2022), 1–20. https://doi.org/10.1016/j.ins.2022.01.042
44. W. Alexan, Y. L. Chen, L. Y. Por, M. Gabr, Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption, *Symmetry.,* **15** (2023), 1081. https://doi.org/10.3390/sym15051081
45. M. Khan, H. M. Waseem, A novel digital contents privacy scheme based on Kramer's arbitrary spin, *Int. J. Theor. Phys.,* **58** (2019), 2720–2743 https://doi.org/10.1007/s10773-019-04162-z
46. A. H. Ismail, H. M. Waseem, M. Ishtiaq, S. S. Jamal, M. Khan, Quantum spin half algebra and generalized Megrelishvili protocol for confidentiality of digital images, *Int. J. Theor. Phys.,* **60** (2021), 1720–1741. https://doi.org/10.1007/s10773-021-04794-0
47. Y. Wang, Y. Shang, Z. Shao, Y. Zhang, G. Coatrieux, H. Ding, et al., Multiple color image encryption based on cascaded quaternion gyrator transforms, *Signal Process. Image Commun.,* **107** (2022), 116793. https://doi.org/10.1016/j.image.2022.116793
48. H. M. Waseem, S. O. Hwang, Design of highly nonlinear confusion component based on entangled points of quantum spin states, *Sci. Rep.,* **13** (2023), 1099. https://doi.org/10.1038/s41598-023-28002-7