

RESEARCH ARTICLE

Billiard Quantum Chaos: A Pioneering Image Encryption Scheme in the Post-Quantum Era

SEONG OUN HWANG¹, (Senior Member, IEEE), HAFIZ MUHAMMAD WASEEM¹,
AND NOOR MUNIR²

¹Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea

²Department of Smart Security, Gachon University, Seongnam 13120, South Korea

Corresponding author: Seong Oun Hwang (seongoun.hwang@gmail.com)

This work was supported in part by the National Research Foundation of Korea (NRF) through the Korean Government (Ministry of Science and Information and Communication Technology) under Grant RS-2024-00340882 and in part by The Circle Foundation (TCF), Republic of Korea, through the 2023 TCF Innovative Science Project-05.

ABSTRACT In an era marked by escalating data breaches and the emergence of quantum computing, ensuring robust data security is paramount. This study introduces an innovative image encryption scheme that employs billiard quantum chaos in conjunction with the Fibonacci sequence to reinforce data integrity against quantum threats. The proposed approach exploits the unpredictable behavior inherent in quantum particles, thereby augmenting the level of randomness in image data. For distributed keys, the Fibonacci sequence operates on the least significant bits, while the sequence generated through billiard quantum chaos affects the most significant bits of the image. This dual-layered approach adds complexity and resilience against advanced persistent threats. The uniform distribution of least and most significant bits is contingent on the key length, and the proposed model ensures adaptability to diverse security requirements. A comprehensive analysis on the ciphered image substantiates the effectiveness of the methodology in achieving security objectives. Comparative assessments validate its applicability in real-world scenarios, underscoring its robustness against quantum attacks. Through the integration of state-of-the-art cryptographic techniques, this scheme presents a formidable response to the challenges posed by quantum computing, positioning a solid foundation for secure image encryption in the post-quantum era.

INDEX TERMS Billiard chaos, fibonacci sequence, image encryption, quantum chaos, true randomness.

I. INTRODUCTION

Image encryption schemes hold significant importance in modern society due to their widespread use of digital images in various domains. With the proliferation of personal devices and social media platforms, their impact can be seen in several key areas such as privacy preservation, healthcare, national security, financial transactions, forensics, e-commerce, remote sensing, and entertainment. These schemes strive for several security goals, including authentication, resistance to cryptanalysis, robustness against different types of attacks, key sensitivity, avalanche effect,

and scalability, ensuring the confidentiality and integrity of digital images.

Chaos theory capitalizes on the inherent unpredictability and complexity of chaotic systems to effectively address these security objectives. By enhancing the security of encryption processes, it provides a robust and reliable method for protecting digital images from unauthorized access, tampering, and interception [1]. It utilizes deterministic systems that exhibit highly sensitive dependence on initial conditions, even a tiny change in the initial conditions can lead to extremely different outcomes. Furthermore, these encryption schemes offer several distinct advantages and have a significant impact compared to other conventional encryption methods, including sensitivity to initial conditions, minimal computational overhead [2], fast encryption and decryption

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed¹.

process [3], adaptability to dynamic environments [4], and potential applicability in emerging technologies such as quantum key distribution [5].

Traditional chaos-based encryption methods, though effective, face several potential threats posed by the advent of quantum computing. For instance, Shor's algorithm demonstrates remarkable efficiency in factorizing large numbers and solving discrete logarithm problems, directly threatening classical encryption algorithms, including those potentially employed in chaos-based cryptosystems [6]. Furthermore, quantum computers have the potential to significantly reduce the effective key length required for breaking classical encryption algorithms [7]. Therefore, even with a shorter key length, a quantum computer can still feasibly break the encryption, rendering chaos-based cryptosystems vulnerable. Conversely, quantum key distribution offers a secure mechanism for exchanging cryptographic keys utilizing quantum properties [8], however, its practical implementation is limited by the requirement for specialized quantum hardware, which is not yet widely available.

In light of these potential risks, researchers are actively engaged in the development and adoption of post-quantum cryptographic techniques with the aim of fortifying defenses against the formidable computational capabilities of quantum machines. These include the exploration of quantum chaos and hybrid strategies that combine classical chaos with quantum-resistant algorithms [9], [10], [11], [12]. Quantum chaos-based encryption schemes hold considerable assurance, owing the fundamental principles of superposition that exhibit inherent uncertainty, offering a significantly higher level of security and resilience against quantum threats compared to conventional chaos-based methodologies. Although these schemes signify a substantial advancement in secure communication, they are confronted by various challenges and limitations, primarily due to their early stage of development [13]. The implementation of quantum encryption schemes necessitates specialized hardware and communication systems, equipped with sufficient numbers of qubits with low error rates, which is quite challenging. Additionally, many quantum-based schemes deal with constraints related to adaptability and scalability [14], [15], [16]. They must be seamlessly integrated with classical information processing systems and exhibit compatibility with real-time applications operating within the confines of limited computational resources.

In addressing the challenges associated with quantum chaos-based encryption, this study introduces a novel model based on billiard quantum chaos. In the proposed framework, particles are characterized by evolving wave functions governed by the Schrödinger equation [17], rather than following predictable trajectories, as classical physics dictates for billiard systems using Newton's laws [18]. Quantum mechanics introduces inherent probabilistic behavior when applied to billiards, resulting in complex interactions of interference patterns and superposition states, yielding intricate quantum dynamics. Leveraging the inherent complexity and

unpredictability of quantum chaos, this approach designs highly secure encryption schemes. The proposed billiard quantum chaos-based scheme offers distinct advantages over general quantum chaos methods, including deterministic behavior, confined phase space, lower sensitivity to perturbations, predictability and control, efficient computational simulations, and potential for hardware implementation. The key features of billiard quantum chaos in image encryption scheme can be characterized as follows:

- Exhibit sensitive dependence on initial conditions, small changes in initial conditions can lead to vastly different outcomes over time, a hallmark of chaotic systems.
- Exhibit statistical properties in terms of energy levels, eigenstates, and other observables, rather than discrete and quantized values.
- Chaos behavior in billiard systems generates pseudorandom patterns that are inherently unpredictable.
- Eigenfunctions (wave functions) associated with chaotic billiard systems are highly complex, with intricate patterns and irregularities.

Overall, while both general quantum chaos and billiard quantum chaos offer opportunities for enhancing information security, the controlled and deterministic nature of billiard systems provides distinct advantages in terms of predictability, stability, and potential for tailored encryption schemes. These benefits make billiard quantum chaos a promising avenue for the development of secure communication protocols and encryption algorithms.

The remaining sections of the paper are organized as follows: Section II provides preliminaries with methodology, Section III presents the experimentation with extensive security analyses, Section IV analyzes the security measures in comparison with existing methodologies, and Section V comprises concluding remarks.

II. PRELIMINARIES AND METHODOLOGY

In this section, we provide a concise overview of quantum billiard chaos (including experimental analysis), Fibonacci sequence, and outline the methodology. Quantum billiard chaos is characterized by the time-independent Schrödinger equation, which governs the quantum dynamics of particles, and the Fibonacci sequence, on the other hand, has the capacity to generate a finite sequence of pseudorandom numbers.

A. QUANTUM BILLIARD CHAOS

Quantum billiard chaos in image encryption involves leveraging the complex and unpredictable behavior exhibited by quantum particles moving within a confined, boundary-rich region, much like a billiard ball bouncing around a table, to enhance the security of image encryption. This phenomenon arises due to the wave-like nature of quantum particles and their interactions with the boundaries [19], and can be described by the time-independent Schrödinger equation which governs the quantum dynamics of particles

within the billiard-like region as follows:

$$H\Psi(x, y) = E\Psi(x, y), \tag{1}$$

where H is the Hamiltonian operator, representing the total energy of the quantum system, $\Psi(x, y)$ is the wave function, a complex-valued function that encodes the probability amplitude of finding the bit at position (x, y) , and E is the energy eigenvalue, which quantizes the energy levels of the system.

In the context of image encryption, this system is used to generate a quantum key or a random sequence governed by the laws of physics, which is employed in the encryption and decryption processes. The boundary conditions are precarious in this scenario, as they precept how the wave functions interact with the boundaries. The wave function must satisfy appropriate boundary conditions that align with the image encryption process.

The dynamics of quantum billiard chaos become complex due to the interference of wave functions reflecting off the boundaries. This leads to the formation of quantum eigenstates, representing the allowed energy levels of the system. These eigenstates $\Psi_n(x, y)$ are solutions to the Schrödinger equation with the appropriate boundary conditions as follows:

$$H\Psi_n(x, y) = E_n\Psi_n(x, y), \tag{2}$$

where eigenvalues E_n represent the quantized energy levels of the system, and the corresponding eigenstates $\Psi_n(x, y)$ describe the probability distribution of finding the bit at different positions within the field.

1) BILLIARD TRAJECTORIES

First we define a parameterized curve that represents the trajectory of a billiard ball based on a Limacon of Pascal curve [20]. The simulated billiard trajectories, in Fig. 1, using numerical integration, taking into account reflections at the boundary, defined by curve equation based on parameters a and ϵ is:

$$(x^2 + y^2 - a\epsilon x)^2 - a^2(x^2 + y^2) = 0, \tag{3}$$

where a and ϵ are parameters that influence the shape and behavior of the curve, respectively. By varying these parameters, we can obtain different curves that satisfy this equation. These curves may have different geometrical properties, such as size, symmetry, and complexity, depending on the values chosen for a and ϵ .

2) INITIALIZATION DATA

The motion of a billiard ball within a specified region, taking into account reflections at the boundary, based on the Pascal curve equation. The generated data points for a Poincaré section by simulating multiple billiard trajectories in parallel by introducing initial conditions, defined by most significant bits (MSBs) of key, within the defined region. The simulation results of Poincaré sections are generated for different values, and presented here for $\epsilon = 0$ and $\epsilon = 0.5$ in Fig. 2.

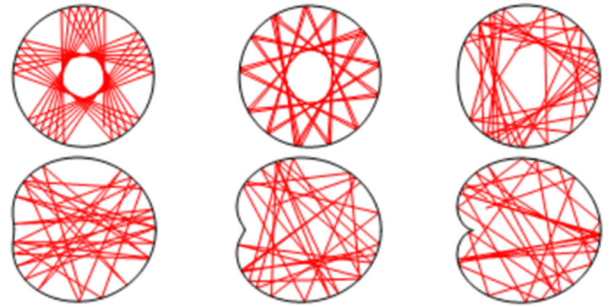


FIGURE 1. Simulation of billiard trajectories.

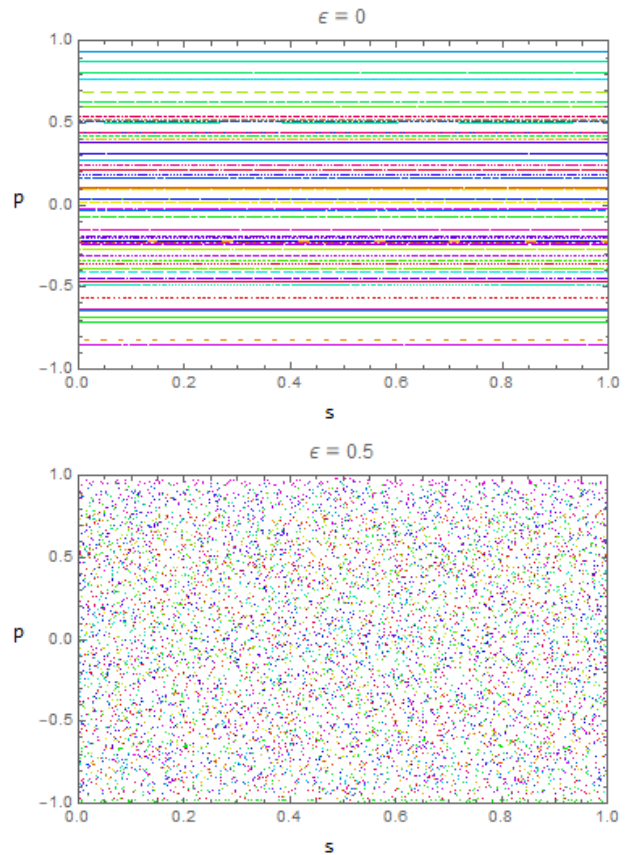


FIGURE 2. Parallel simulation of multiple billiard trajectories on data points within the defined region for a Poincaré.

3) QUANTUM BILLIARDS

We simulated the functions for Bunimovich stadium and Robnik billiard, including eigenvalues and eigenfunctions, and presented the results for Bunimovich stadium billiard in Fig. 3. The probability density plots associated with eigenvalues and eigenfunctions are evaluated at random data points within a specified region.

4) POTENTIAL AND HAMILTONIAN

To compute the Hamiltonian, which is the total energy of the system, we define energy function based on the variables x and y . It combines the kinetic and potential energies to

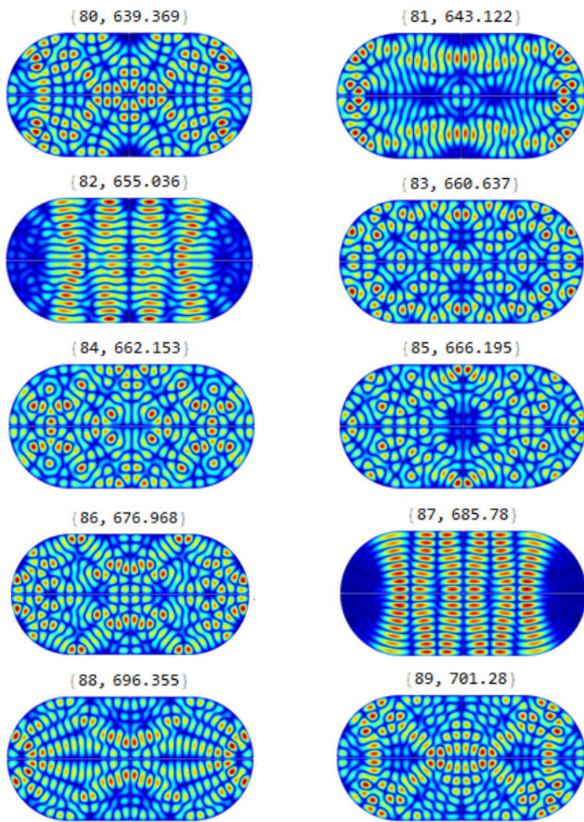


FIGURE 3. Probability density plots on random data points within a specified region of Bunimovich stadium billiard.

represent the total energy of the system as follows:

$$H(x, y, p_x, p_y) = \frac{1}{2} (p_x^2 + p_y^2 + V(x, y)), \quad (4)$$

where p_x and p_y are the momentum components in the x and y directions, p_x^2 and p_y^2 represents the kinetic energy, and $V(x, y)$ is the potential energy, such that $V(x, y) = \frac{1}{2} (x^2 + y^2 + 2x^2y - \frac{2}{3}y^3)$.

Jacobi matrix is employed to relate the partial derivatives of the Hamiltonian with respect to the position and momentum variables. It is used in conjunction with the Hamiltonian derivatives to formulate the equations of motion to quantify the system's behavior near a specific point in phase space. In the experiment, we created a 4×4 matrix with specific entries (1, 1, -1, -1) at positions (1, 3), (2, 4), (3, 1), and (4, 2) respectively. These specific entries are used in the sparse array to create the matrix. The equations of motion are derived from the Hamiltonian function, which governs the dynamics of the system. The trajectory in Fig. 4 showcases how the system's state evolves over time under the influence of the Hamiltonian dynamics.

5) POINCARÉ SECTION

– The Poincaré function efficiently identifies points that intersect with the specified surface in phase space, allowing for

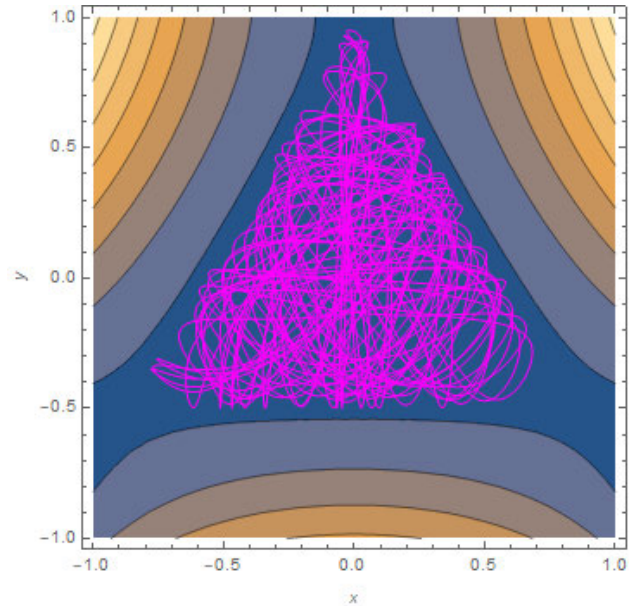


FIGURE 4. System's behavior under the influence of Hamiltonian dynamics.

detailed analysis of the system's behavior at those specific moments [21]. We implemented the Poincaré section with the specified energy level and input parameters, x_0 , y_0 , p_{x0} , and p_{y0} , as initial conditions in the phase space. We specify the event locator with condition $p_x[t] > 0$, which means it triggers when the momentum component (p_x) is greater than zero, to locate events during the integration process and record the values of y , p_y , and t at the events. Figure 5 presents the plots of Poincaré sections for a specified energy level and the number of trajectories.

6) LYAPUNOV SPECTRUM

Lyapunov exponent describes how a dynamic system behaves under small perturbations. The spectrum provides valuable information about the system's sensitivity to initial conditions, such as exponential divergence or convergence of nearby trajectories in a dynamic system, which is an essential feature of chaos theory [22]. We assessed the Lyapunov spectrums by defining the maximum time for the simulation with initial conditions, x_0 , y_0 , p_{x0} , and p_{y0} , in the phase space.

The plot in Fig. 6 (a) shows the Lyapunov exponents over time on a linear scale, indicating the rates of separation of infinitesimally close trajectories in the system. Positive exponents signify chaotic behavior, zero indicates neutral stability (such as in a periodic orbit), and negative values suggest convergence to a stable point or cycle. The exponents λ_1 , λ_2 , λ_3 , and λ_4 are plotted as functions of time or normalization steps, with each line representing the value of a Lyapunov exponent over time. Moreover, the plot in Fig. 6 (b) shows the first two Lyapunov exponents on a log-log scale, providing a clearer view of the exponents' behavior over many orders of magnitude. The log-log scaling on both axes highlights the exponential nature of the growth or decay of the exponents.

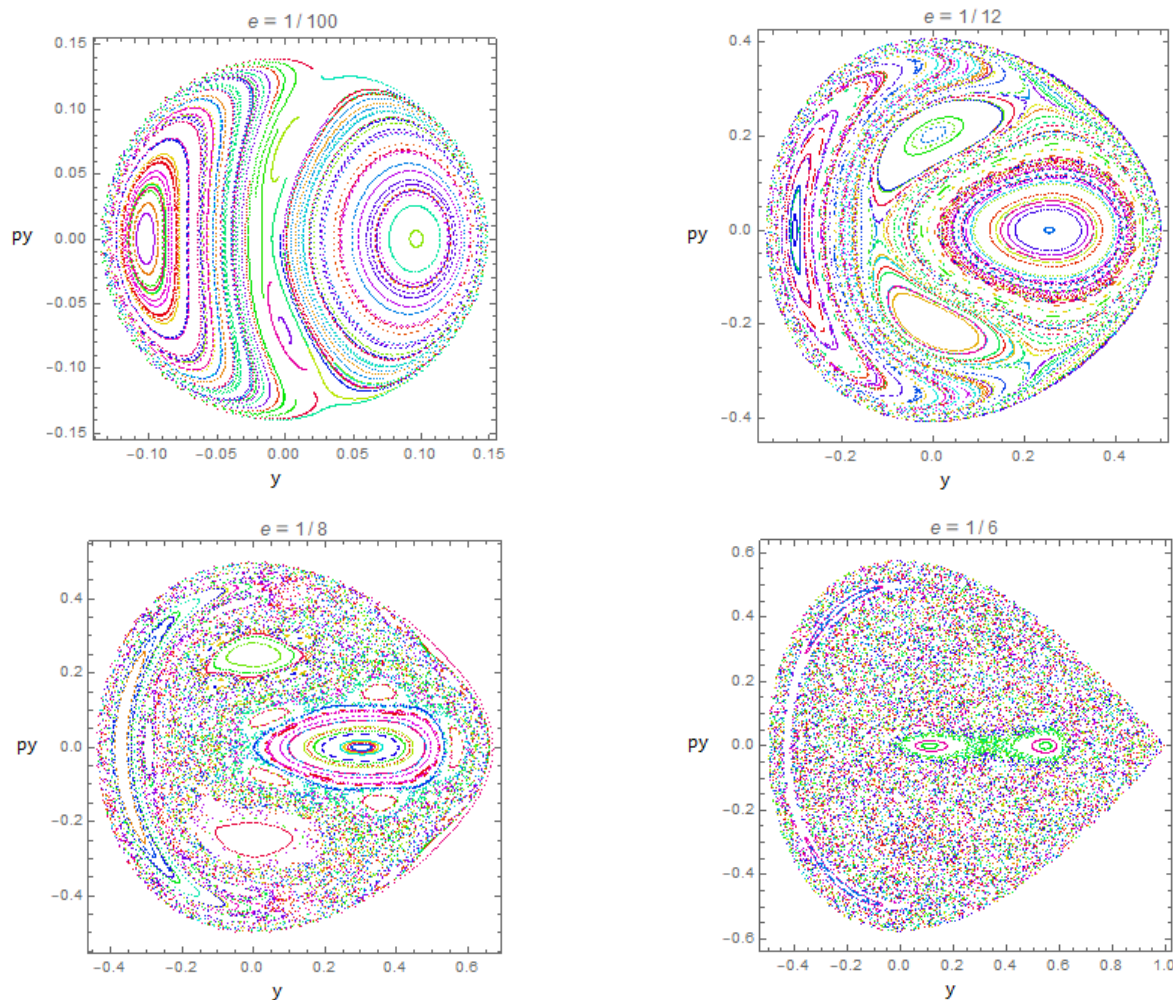


FIGURE 5. Poincaré section plots for a specified energy level and number of trajectories.

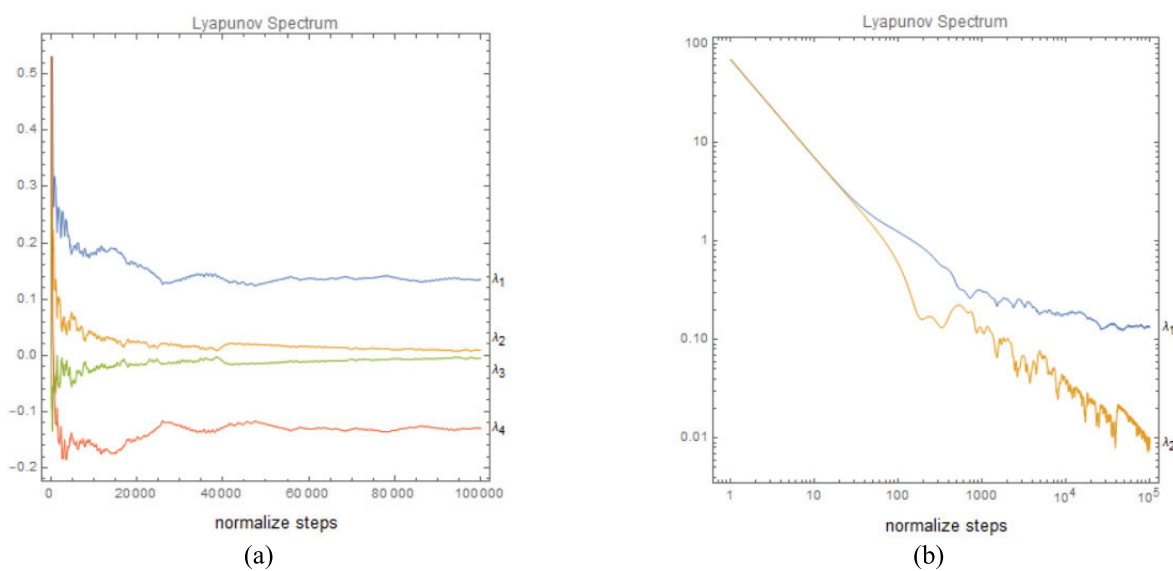


FIGURE 6. Lyapunov spectrum plots: (a) Lyapunov exponents on a linear scale, (b) Lyapunov exponents on a log-log scale.

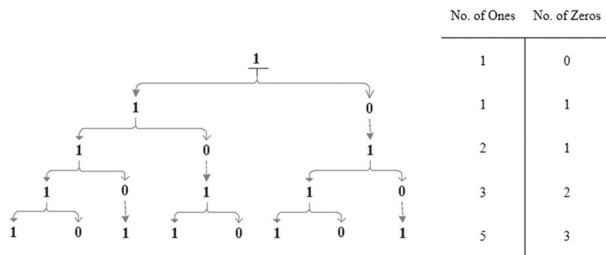


FIGURE 7. Fibonacci sequence of pseudorandom numbers.

B. FIBONACCI SEQUENCE

The Fibonacci sequence is a series of numbers in which each number (after the first two) is the sum of the two preceding ones to generate a pseudorandom sequence [23]. It begins with 0 and 1, and continues as follows: 0, 1, 1, 2, 3, 5, 8, 13, 21, and so forth. We can initiate the sequence by opting F_0 and F_1 , and the subsequent numbers can be determined using $F_{n-1} + F_{n-2}$ as follows:

$$F_n = \begin{cases} 0, & \text{if } n = 0 \\ 1, & \text{if } n = 1 \\ F_{n-1} + F_{n-2}, & \text{if } n > 1 \end{cases} \quad (5)$$

where n represents the position in the sequence. Depending on the specific encryption algorithm, the Fibonacci sequence, depicted in Fig. 7, may be truncated or transformed to generate a finite sequence of pseudorandom numbers. In the context of image encryption schemes, this phenomenon may be used to assign a pseudorandom number from the truncated Fibonacci sequence to each pixel in the image [24]. This number will determine the encryption operation applied to that pixel.

C. ALGORITHM

Billiard quantum chaos arises when the classical counterpart of the system exhibits chaotic behavior. Through the strategic integration of the billiard quantum chaos with the Fibonacci sequence, we have formulated an innovative image encryption scheme that harnesses the wave-like nature and the interference patterns of quantum particles to provide an unpredictable trajectory to produce complex system for image encryption scheme.

Encrypted images are typically recovered by manipulating the least significant bits (LSBs), as altering the LSBs has a minimal visual impact on the image. During encryption, in our algorithm, LSBs of the pixel values in the image are modified with the Fibonacci sequence at given instances. Using the same algorithm and key, the recipient applies the reverse operation to the encrypted image, which involves manipulating the LSBs back to their original state, to recover the original image. While LSB modification can provide a basic level of security for image encryption, we modify most significant bits (MSBs) of the image with the sequence generated by billiard quantum chaos. These modifications are made in such a way that they are statistically indistinguishable

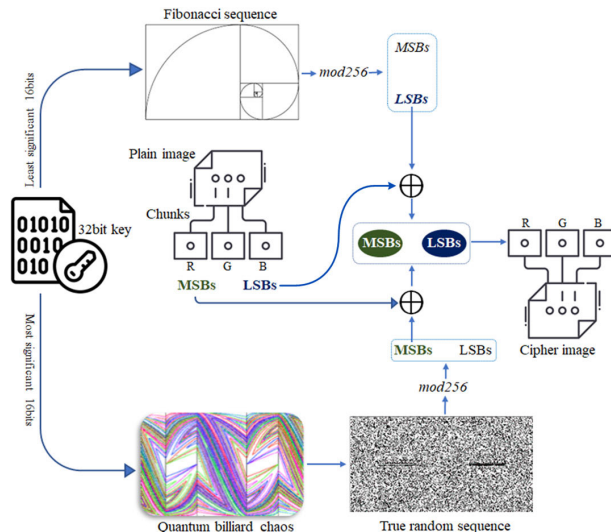


FIGURE 8. Proposed image encryption scheme.

from random noise, and the true recipient can recover the original data efficiently.

The proposed algorithm operates based on the assumption of symmetric keys and associated quantum chaos values. The operational principle of the proposed algorithm, as shown in Fig. 8, is as follows:

1. Equidistribution of LSBs and MSBs: Regarding key length, we deliberated equidistribution to organize the most and least significant bits. This entails using 8 bits for each in the case of a 16-bit key, and 16 bits for each in the case of a 32-bit key.
2. Initialization: For experimentation, a key with the binary representation 1000110000101100 is set to initiate both Fibonacci and billiard quantum chaos sequences.
 - In relation to the decimal value of the least significant bits (LSBs), i.e. 44, we start the Fibonacci sequence at n_{44} .
 - Concerning the decimal value of the most significant bits (MSBs), we set the initial condition at m_{140} to initiate the billiard quantum chaos sequence.
3. Image fragmentation: For an 8-bit input image M , which contains RGB content, we fragmented the LSBs and MSBs.
4. LSBs transformation: To transform the LSBs of the image values, we assign a pseudorandom number (obtained by taking mod256 from the truncated Fibonacci sequence) to each pixel in the image. This is accomplished by performing a bit-XOR operation between the pixel value and the LSBs of the corresponding pseudorandom number from the Fibonacci sequence, thereby modifying the pixel value. In order to decrypt the image, the recipient must possess the same initial values used to generate the Fibonacci sequence.

TABLE 1. Encryption and decryption analyses for the ASCII characters.

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

- MSBs transformation: To modify the MSBs of the image values, we assign a true random number (again obtained by taking mod256) and conduct a bit-XOR operation between the MSBs of the image and the MSBs of the sequence generated by the billiard quantum chaos.
- All processed chunks are then reassembled to construct the cipher image.

This algorithm introduces an innovative approach to secure image encryption, leveraging the interplay of billiard quantum chaos and the Fibonacci sequence with digital images to ensure robust data protection.

III. EXPERIMENT AND SECURITY ANALYSES

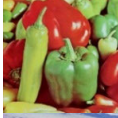




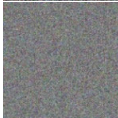

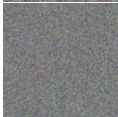


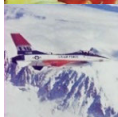
We conducted comprehensive experiments on text and a variety of 256×256 images sourced from the SIPI image database [25], employing the proposed algorithm. These experiments intensely showcase the algorithm’s adaptability to diverse types of content.

- For text analysis, we modify the algorithm pertaining the LSBs and MSBs of ASCII characters. The outcomes of these modifications are summarized in Table 1. By varying a single bit in the key, whether in the LSBs or MSBs, we examined the impact of randomness generated in the ASCII sequence during decryption.

- For image analysis, we showcased the encryption practices applied to multiple contents of the Pepper and Airplane images, presented in Fig. 9. By varying a single bit in the key, either in the LSBs or MSBs, we assessed the randomness generated in both images upon decryption, as presented in Table 2.

To ensure the effectiveness and security of the proposed algorithm, we conducted comprehensive assessments involving factual examination, inconsistencies detection, and sensitivity analysis on the encrypted images using our developed approach. These evaluations encompassed a wide range of analytical techniques such as histogram, entropy, correlation, evaluation of pixel attributes, and differential analyses.

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	
		1000110000101100	

These trials collectively provide a robust evaluation system to measure the algorithm’s performance and its ability to withstand real-world conditions.

A. HISTOGRAM ANALYSES

Histogram analysis provides valuable insights of statistical properties present in the image. It scrutinizes how pixel intensity values are dispersed within an encrypted image. This analysis allows us to detect irregularities, assess uniformity, and uncover potential weaknesses in the encryption procedure [26]. In Figs. 10–11, the histograms of the encrypted Pepper and Airplane images, generated using our proposed technique, do not reveal any noticeable patterns or disclose information about the original content. This serves as validation for the robustness of our encryption scheme against statistical attacks.

B. ENTROPY ANALYSES

Entropy analysis quantifies the level of randomness or uncertainty in the pixel distribution of an encrypted image. It can

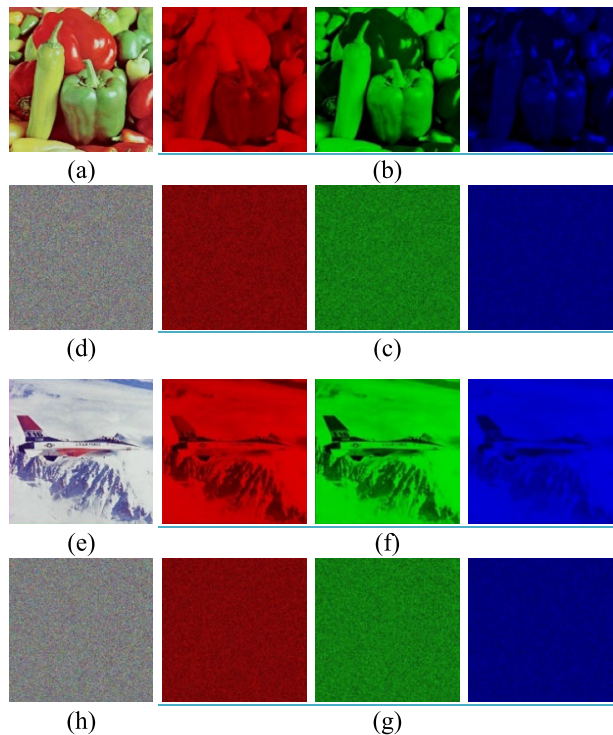


FIGURE 9. Layer-wise encryption of pepper and airplane images: (a) Plain Pepper image, (b) Extracted layers (c) Encrypted layers, (d) Encrypted Pepper image; (e) Plain Airplane image, (f) Extracted layers (g) Encrypted layers, (h) Encrypted Airplane image.

be estimated using the following expression:

$$H = - \sum p(x) \log_2(p(x)), \quad (6)$$

where $p(x)$ signifies the probability of a pixel in the image having the value x . A higher entropy value indicates a more random distribution of pixel values, implying greater security [27]. The assessment of entropy for various encrypted images utilizing our proposed methodology is presented in Table 3.

C. CORRELATION ANALYSES

In image encryption schemes, correlation analysis entails evaluating the statistical relationships between pixel values within an encrypted image. It provides a means to understand how alterations in one pixel correspond to changes in adjacent pixels [28]. The correlation coefficient (ρ) between two variables X and Y can be expressed as:

$$\rho = \frac{Cov(X, Y)}{\sigma_X \sigma_Y}, \quad (7)$$

where $Cov(X, Y)$ is the covariance between variables X and Y , and σ_X, σ_Y are the standard deviations of X and Y respectively. We performed this analysis to assess the degree of association between adjacent pixels, Fig. 12.

The lower correlation values in Table 4 indicate that neighboring pixels exhibit less interdependence. This is a favorable trait for encryption schemes as it indicates that patterns in the

TABLE 3. Layer-wise entropies and differential analyses for source and corresponding encrypted images.

Image	Content	Entropies		Differential analysis	
		Plain	Encrypted	NPCR	UACI
Pepper	Red	7.3516	7.9995	99.84	33.56
	Green	7.5812	7.9992	99.87	33.52
	Blue	7.1347	7.9996	99.81	33.78
Airplane	Red	6.7489	7.9995	99.81	33.27
	Green	6.8106	7.9995	99.78	33.26
	Blue	6.2682	7.9994	99.82	33.29
Lena	Red	7.2531	7.9993	99.86	33.19
	Green	7.5940	7.9992	99.79	33.18
	Blue	6.9684	7.9993	99.83	33.24
Baboon	Red	7.7444	7.9994	99.79	33.31
	Green	7.4493	7.9991	99.78	33.46
	Blue	7.7513	7.9995	99.87	33.33
House	Red	7.4493	7.9995	99.78	33.41
	Green	7.2632	7.9995	99.79	33.24
	Blue	7.4891	7.9994	99.81	33.28
Sailboat	Red	7.3166	7.9993	99.86	33.39
	Green	7.6443	7.9993	99.80	33.42
	Blue	7.3030	7.9992	99.82	33.51

original image are being disrupted. This analysis reinforces the effectiveness of the proposed encryption scheme in dispersing information across the image, thereby strengthening its resilience against attacks.

D. DIFFERENTIAL ATTACK ANALYSIS

Differential attack analysis estimates the encryption scheme's susceptibility to minor alterations in the plaintext. This involves assessing how changing one or more bits in the input affects the resulting ciphertext [29]. We employed this analysis on various cipher images, specifically focusing on 1-bit alterations. The evaluation outcomes, detailed in Table 3, were assessed using two standard metrics:

1) NUMBER OF PIXEL CHANGES RATE (NPCR)

This metric measures the percentage of pixel changes in the ciphertext when a single pixel in the plaintext is modified. It indicates the encryption algorithm's sensitivity to small input changes and can be evaluated as follows:

$$NPCR = \frac{N - M}{N} \times 100\%, \quad (8)$$

where N represents the total number of pixels in the image and M is the number of pixels that remain unaltered in the ciphertext when one pixel in the plaintext is changed.

2) UNIFIED AVERAGE CHANGING INTENSITY (UACI)

This estimates the average intensity of pixel changes when one bit is altered in the plaintext. It provides a measure of how

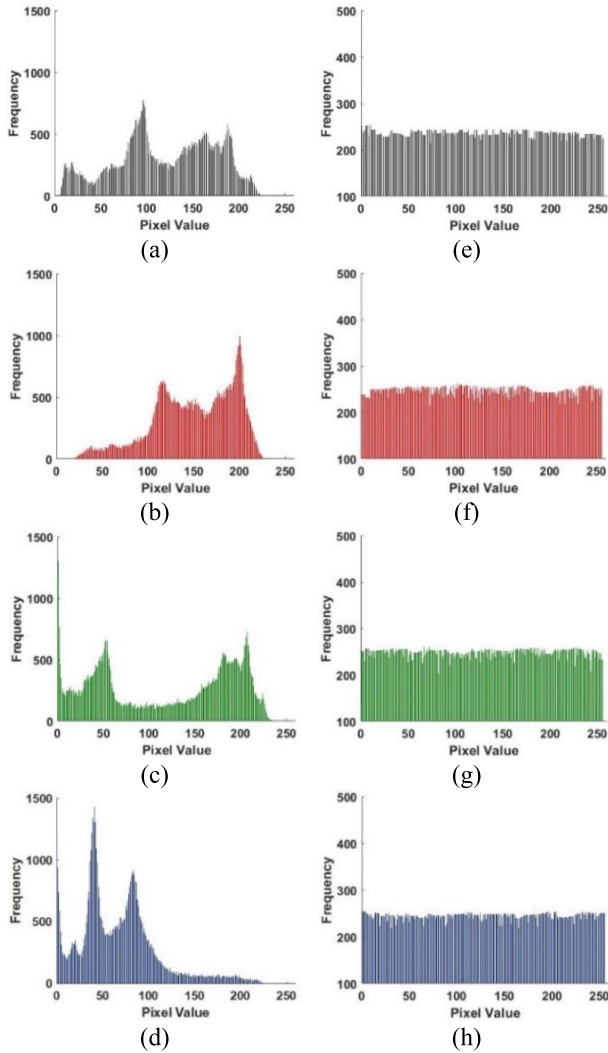


FIGURE 10. Layer-wise histograms of pepper image: (a-d) Plain image – histograms at grayscale and corresponding RGB content, (e-h) Encrypted image – histograms at grayscale and corresponding RGB content.

much the image changes in response to minor adjustments in the input and can be evaluated as follows:

$$UACI = \frac{1}{N} \sum_{i=1}^N \frac{|C_i - C'_i|}{L} \times 100\%, \quad (9)$$

where C_i and C'_i denote the intensity values of the i^{th} pixels in the original and modified ciphertexts, and L represents the maximum possible pixel intensity value (e.g., 255 for an 8-bit image). Higher NPCR values, as shown in Table 3, indicate greater resilience against differential attacks, signifying that even slight changes in the plaintext lead to substantial alterations in the ciphertext.

E. PIXELS' SIMILARITY ANALYSES

Pixel similarity analysis quantifies the resemblance of correlated pixel values across different image regions [30]. We assess this similarity using three widely recognized measures, outlined in Table 5, as follows:

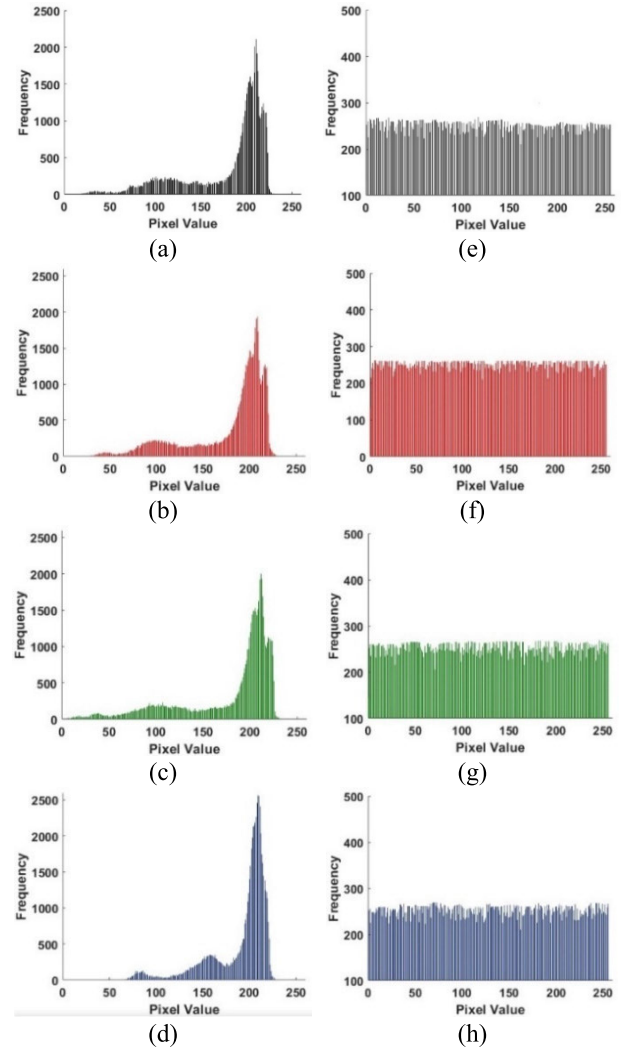


FIGURE 11. Layer-wise histograms of airplane image: (a-d) Plain image – histograms at grayscale and corresponding RGB content, (e-h) Encrypted image – histograms at grayscale and corresponding RGB content.

1) STRUCTURAL SIMILARITY INDEX MATRIX (SSIM)

This metric evaluates the similarity between two images, considering luminance, contrast, and structure. It can be evaluated as:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \quad (10)$$

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

2) NORMALIZED CROSS-CORRELATION (NCC)

This measure quantifies the similarity between two images by assessing the cross-correlation between their pixel values. It can be evaluated as:

$$NCC(x, y) = \frac{\sum (x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum (x_i - \mu_x)^2 \sum (y_i - \mu_y)^2}}, \quad (11)$$

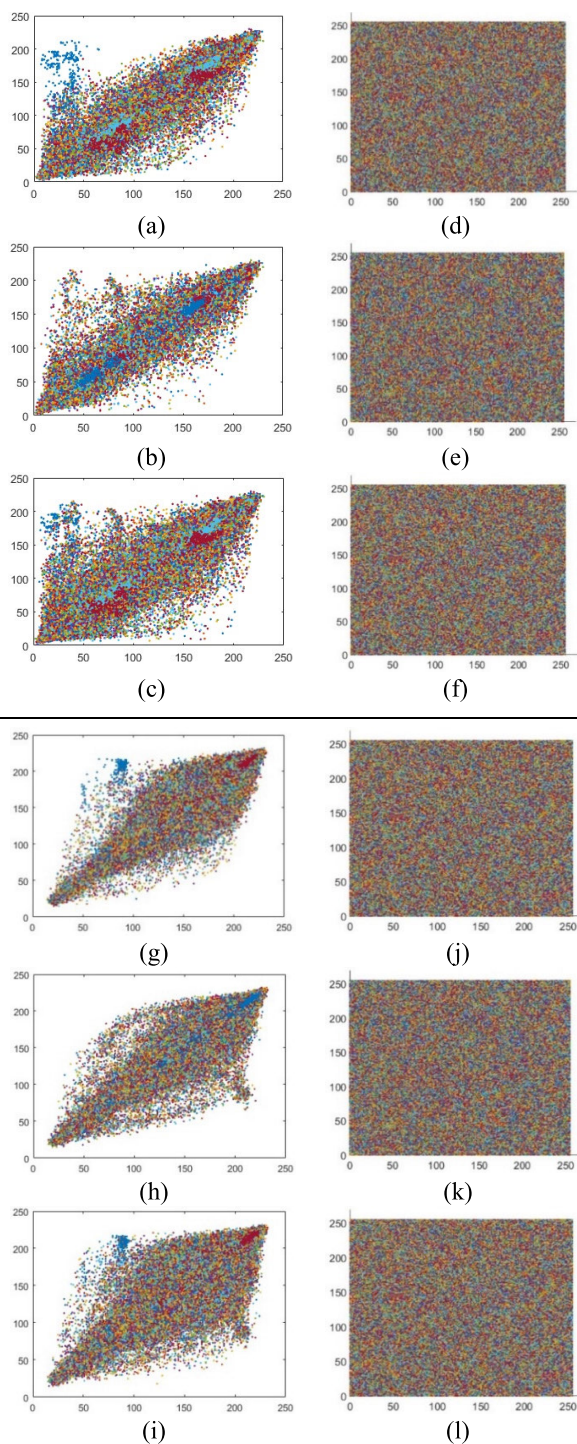


FIGURE 12. Correlation analyses of adjacent pixels for source and encrypted images in horizontal, vertical, and diagonal directions. (a-f) analysis of source and corresponding encrypted Pepper image; (g-l) analysis of source and corresponding encrypted airplane image.

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 .

3) STRUCTURAL CONTENT

This metric evaluates the structural content of an image by comparing gradients. It can be quantified using the Gradient

TABLE 4. Layer-wise correlation coefficients analyses for source and corresponding encrypted images.

Image	Content	Direction		
		Horizontal	Vertical	Diagonal
Pepper	Plain	0.9757	0.9779	0.9635
	Encrypted	-0.0012	0.0021	-0.0026
Airplane	Plain	0.9662	0.9639	0.9368
	Encrypted	0.0011	0.0014	-0.0010
Lena	Plain	0.9719	0.9850	0.9593
	Encrypted	-0.0013	0.0006	0.0018
Baboon	Plain	0.8534	0.7598	0.7300
	Encrypted	-0.0019	-0.0021	-0.0024
House	Plain	0.9479	0.9570	0.9132
	Encrypted	0.0016	-0.0009	0.0015
Sailboat	Plain	0.9737	0.9700	0.9569
	Encrypted	-0.0024	-0.0017	0.0007

Similarity Index (GSI) as:

$$GSI(x, y) = \frac{2\sigma_x\sigma_y + C_3}{\sigma_x^2\sigma_y^2 + C_3}, \tag{12}$$

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

Table 5 provides an overview of the results from the similarity analyses conducted on the source and encrypted images. These findings reveal notable distinctions in structural attributes between the original and encrypted content. Furthermore, Fig. 13 visually underscores the correlations and resemblances observed between the source and encrypted versions of the Pepper and Airplane images. Notably, the anticipated values for NCC and GSI intimately approach zero, indicating a significant degree of dissimilarity among the various content variations.

F. PIXELS' DIFFERENCE ANALYSES

Pixel disparity analysis investigates the difference between corresponding pixels in two images, providing insights into the performance of various image processing techniques, including encryption methods [31]. We computed the disparity among pixels in source and encrypted images using three common measures, outlined in Table 5, as follows:

1) MEAN ABSOLUTE ERROR (MAE)

This metric determines the average absolute difference between corresponding pixels in two images, representing the average magnitude of errors. It can be computed as:

$$MAE(x, y) = \frac{1}{N} \sum_{i=1}^N |x_i - y_i|, \tag{13}$$

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

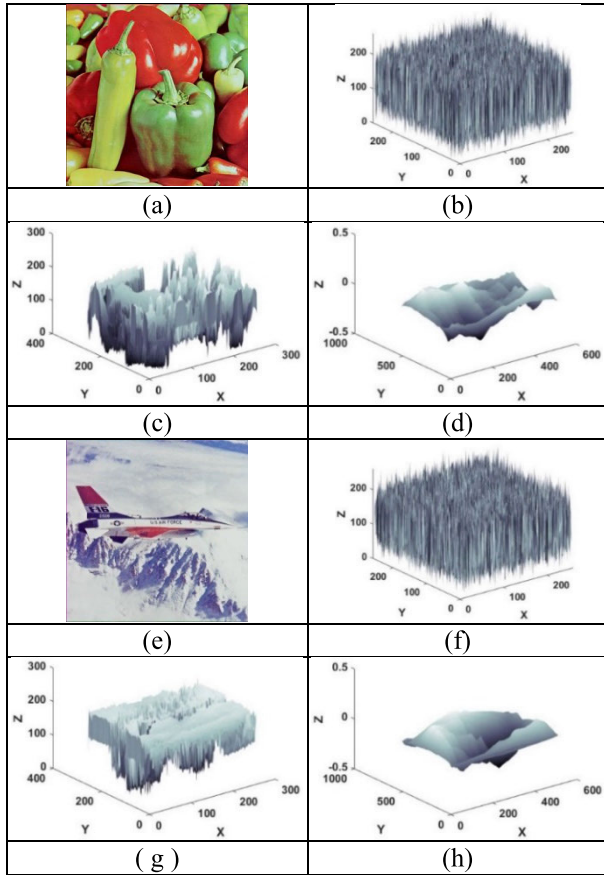


FIGURE 13. Surface plots for the normalized cross-correlation of image contents. Pepper image – (a-b) Plain and encrypted, (c-d) Corresponding surface plots; Airplane image – (e-f) Plain and encrypted, (g-h) Corresponding surface plots.

2) MEAN SQUARED ERROR (MSE)

This measure determines the average of the squared differences between corresponding pixels, giving more emphasis to larger discrepancies compared to MAE. It can be computed as:

$$MSE(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2. \quad (14)$$

3) PEAK SIGNAL-TO-NOISE RATIO (PSNR)

This metric assesses the ratio between the maximum possible signal value (pixel values) and the introduced noise (error from the encryption process). It can be evaluated as:

$$PSNR(x, y) = 10 \cdot \log_{10} \left(\frac{MAX^2}{MSE(x, y)} \right), \quad (15)$$

where *MAX* represents the maximum possible pixel value (e.g., 255 for 8-bit images) and *MSE*(*x*, *y*) is the mean squared error between the original image *x* and the encrypted image *y*.

The data in Table 5 conclusively affirms that MAE highlights a substantial variance in pixel values between the source and encrypted images. Moreover, MSE exhibits significant variations alongside PSNR. Notably, when MSE is

TABLE 5. Pixels’ similarity and difference analyses between source and corresponding encrypted images.

Image	Similarity analyses			Difference analyses		
	SSIM	NCC	GSI	MAE	MSE	PSNR
Pepper	0.00180	0.0025	0.0038	84.64	5496.40	10.76
Airplane	0.00154	0.0032	0.0022	75.88	7332.97	9.51
Lena	0.00165	0.0043	0.0028	79.89	4847.39	11.31
Baboon	0.00171	0.0029	0.0031	74.65	4417.28	11.71
House	0.00137	0.0046	0.0026	64.78	5950.19	10.42
Sailboat	0.00119	0.0032	0.0017	68.37	6844.17	9.81

TABLE 6. Pixels’ fidelity analyses between source and corresponding encrypted images.

Image	NAE	AD	MD
Pepper	0.0499	0.0508	221
Airplane	0.0399	0.0263	223
Lena	0.0455	0.0272	223
Baboon	0.0441	0.0312	199
House	0.0391	0.0374	231
Sailboat	0.0458	0.0428	233

higher and PSNR is lower, or vice versa, it indicates an enrichment in the encryption quality.

G. PIXELS’ FIDELITY ANALYSES

Pixels’ fidelity analyses determine the quality of encryption in terms of maintaining image fidelity. This ensures the encrypted images retain their integrity and are resistant to unauthorized access and tampering [32]. We computed the fidelity among pixels in source and encrypted images using three common measures, outlined in Table 6, as follows:

1) NORMALIZED ABSOLUTE ERROR (NAE)

It quantifies the average relative difference between corresponding pixels in the original and encrypted images. It provides a normalized view of the errors, making it useful for comparing images of different scales or resolutions. It can be evaluated as:

$$NAE = \frac{1}{N} \sum \frac{|x_i - y_i|}{(L - 1)}, \quad (16)$$

where *N* is the total number of pixels in the image, *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).

2) AVERAGE DIFFERENCE (AD)

This metric computes the average absolute difference between corresponding pixel values in the plaintext and ciphertext images. It provides a measure of the overall discrepancy between the images. It can be computed as:

$$AD = \frac{1}{N} \sum |x_i - y_i|. \quad (17)$$

3) MAXIMUM DIFFERENCE (MD)

This metric quantifies the maximum absolute difference between corresponding pixel values in the plaintext and ciphertext images. It highlights the most significant variation between the images, as can be computed as follows:

$$MD = \max |x_i - y_i|. \tag{18}$$

These measures assess the discrepancies introduced during encryption. A lower NAE and AD, in Table 6, indicates that the encryption process introduces minimal relative differences and maintains close alignment of pixel values between the original and encrypted images, resulting in a minimal average difference and preserving the image quality effectively.

H. NOISE AND OCCLUSION ATTACK ANALYSES

Noise and occlusion attack analyses assess the algorithm’s resilience to disruptions and partial image obstructions. These attacks replicate real-world situations where images can face different types of interference. In a noise attack, random disruptions or pixel value alterations are introduced to the image [33], while an occlusion attack involves concealing portions of the image, imitating situations where chunks of the image are concealed or degraded [34]. These analyses can be modeled as follows:

$$I_{ns} = I_{org} + G, \tag{19}$$

$$I_{oc} = I_{org} \odot B, \tag{20}$$

where I_{org} , I_{ns} , and I_{oc} are the original, noisy, and occluded images, G represents the added noise (specifically Gaussian noise), and B is a binary mask indicating the occluded regions.

The objective of the noise attack analysis is to assess the encryption scheme’s ability to withstand information degradation or distortion in the presence of noise. To validate the algorithm’s robustness, we computed MSE and PSNR metrics by introducing Gaussian noise with normalized power levels of 0.000001, 0.000003, 0.000005, and 0.000007. The corresponding results are presented in Table 7.

The occlusion attack analysis aims to evaluate the encryption scheme’s capability to recover the original image from an occluded version. We conducted this analysis on the encrypted image occluded by fractions of 1/4, 1/2, and 3/5, and the outcomes are portrayed in Fig. 14 and summarized in Table 8.

In both scenarios, an effective image encryption scheme should ideally possess the capacity to retrieve the original image even in the presence of noise or occlusion. The ability to withstand these attacks is a critical factor in appraising the efficacy of an encryption scheme for image data. The observed slight variations in the noise ratio and error estimation when varying the noise strength from 0.000001 to 0.000007 emphasize the robust efficiency of the proposed framework against noise attacks. Furthermore, the results regarding MSE and PSNR, as shown in Table 8 and Fig. 14, indicate that the proposed algorithm can withstand up to a 60% occlusion attack.

TABLE 7. Noise attack analysis.

Image	Trial	Noise intensity			
		0.000001	0.000003	0.000005	0.000007
Pepper	MSE	9970.2	9652.6	9302.3	9117.5
	PSNR	7.8401	7.9116	7.9903	8.0819
Airplane	MSE	9991.4	9702.1	9411.2	9198.6
	PSNR	7.5616	7.6911	7.7714	7.8517
Lena	MSE	9688.5	9443.4	9201.9	9003.7
	PSNR	7.6758	7.7589	7.8416	7.9601
Baboon	MSE	9718.7	9570.6	9374.2	9126.1
	PSNR	7.8610	7.9217	7.9698	8.0519
House	MSE	9706.5	9514.1	9318.8	9108.9
	PSNR	7.8718	7.9261	7.9611	8.0094
Sailboat	MSE	9745.1	9569.9	9327.7	9119.1
	PSNR	7.9553	7.9942	8.0316	8.1026

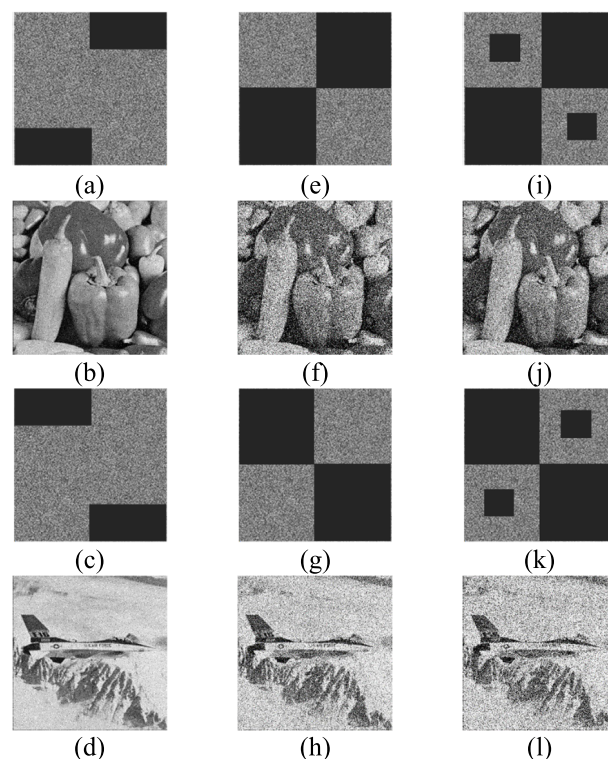


FIGURE 14. Occlusion analysis for the encrypted Pepper and Airplane images. (a-d) Occluded by fraction of 1/4 (in the corners) and corresponding recovered images; (e-h) Occluded by fraction of 1/2 (in the diagonals) and corresponding recovered images; (i-l) Occluded by fraction of 3/5 (in the diagonals, and mid of top-left/right and end-left/right corners) and corresponding recovered image.

IV. DISCUSSION

The proposed algorithm exhibits superior performance compared to state-of-the-art literature across various key metrics. Although practical quantum computing hardware is not publicly available yet, we simulated the quantum algorithm on IBM Quantum Composer with the QISKit library for generating quantum states and simulated the billiard trajectory on Jupyter Notebook with Wolfram Engine 12.1. Here, we provide a detailed discussion on comparative analyses of the

TABLE 8. Occlusion analysis.

Image	Trial	1/4	1/2	3/5
Pepper	MSE	6570.4	4856.1	3621.5
	PSNR	10.5366	12.1514	13.3155
Airplane	MSE	6721.35	4881.2	3741.13
	PSNR	10.4501	12.1164	13.1904
Lena	MSE	6478.29	5003.19	3754.88
	PSNR	11.0719	13.0017	13.6581
Baboon	MSE	6508.43	478.21	3636.12
	PSNR	10.4249	12.5582	13.1231
House	MSE	5981.21	4298.38	3510.55
	PSNR	11.1301	12.6317	13.2219
Sailboat	MSE	5994.32	4388.65	3702.54
	PSNR	11.3127	12.7759	13.2979

proposed algorithm with existing methodologies, including statistical, differential, luminance, structural, contrast, cross-correlation, and fidelity assessments as follows:

A. ENTROPY AND DIFFERENTIAL ATTACK ASSESSMENT

The proposed algorithm demonstrates higher entropy values, signifying increased unpredictability, and lower sensitivity to input alterations, indicating its effectiveness in protecting against differential attacks. Table 9 validates the high randomness and low sensitivity, pertaining the small changes in the plaintext, observed in encrypted images with the proposed method in comparison to existing methodologies [35], [36], [37], [38], as the computed entropy closely aligns with the ideal entropy for 8-bit digital content. This correspondence ensures that the encrypted images exhibit resilience against statistical and differential attacks, as well as potential information leakage.

B. CORRELATION COEFFICIENTS ASSESSMENT

The proposed algorithm exhibits lower correlation coefficients, implying reduced predictability, which makes it more resistant to attacks relying on linear dependencies. Table 10 validates the effectiveness of the proposed encryption scheme in dispersing information across the image, showcasing its improved resilience in comparison with existing methodologies [36], [39] to attacks targeting linear relationships.

C. PIXELS' SIMILARITY ASSESSMENT

The proposed algorithm demonstrates lower pixel similarity in different image regions, indicating reduced predictability and greater resistance to attacks exploiting correlated pixel values. Table 11 validates the notable distinctions between plain and encrypted images for the proposed method in comparison with existing methodologies [40], [41], considering luminance, contrast, cross-correlation, and structural content. The anticipated values for normalized cross-correlation and gradient similarity index with the proposed method intimately approach zero, indicating a significant degree of dissimilarity among the various content variations.

TABLE 9. Comparative analysis of proposed scheme with existing methodologies for average entropies and differential attack analysis.

Algorithm	Analysis	Reference image				
		Pepper	Airplane	Lena	Baboon	Sailboat
Proposed	Entropy	7.9994	7.9995	7.9993	7.9993	7.9993
	NPCR	99.85	99.81	99.83	99.81	99.83
	UACI	33.52	33.28	33.21	33.36	33.44
Ref. [35]	Entropy	7.9985	7.9985	7.9985	7.9985	-
Ref. [37]	Entropy	7.9993	7.9993	7.9993	7.9992	-
Ref. [36]	Entropy	7.9965	7.9967	7.9975	7.9870	7.9968
	NPCR	99.62	99.61	99.60	99.58	99.61
	UACI	33.47	33.47	33.47	33.45	33.45
Ref. [38]	NPCR	99.60	99.61	-	99.60	99.60
	UACI	33.48	33.50	-	33.42	33.45

TABLE 10. Comparative analysis of proposed scheme with existing methodologies for correlation coefficients.

Algorithm	Analysis	Reference image				
		Pepper	Airplane	Lena	Baboon	Sailboat
Proposed	Horizontal	-0.0012	0.0011	-0.0013	-0.0019	-0.0024
	Vertical	0.0021	0.0014	0.0006	-0.0021	-0.0017
	Diagonal	-0.0026	-0.0010	0.0018	-0.0024	0.0007
Ref. [39]	Horizontal	-0.0236	-0.0057	-0.0054	-0.0166	-0.0166
	Vertical	-0.0084	-0.0246	-0.0236	-0.0243	-0.0035
	Diagonal	-0.0351	-0.0034	-0.0535	-0.1016	-0.0189
Ref. [36]	Horizontal	0.0005	0.0038	-0.0021	0.0015	0.0023
	Vertical	0.0004	-0.0048	-0.0012	0.0048	0.0032
	Diagonal	0.0032	-0.0001	0.0017	0.0016	0.0016

TABLE 11. Comparative analysis of proposed scheme with existing methodologies for Pixels' similarity analysis.

Algorithm	Analysis	Reference image				
		Pepper	Airplane	Lena	Baboon	Sailboat
Proposed	SSIM	0.00180	0.00154	0.00165	0.00171	0.00119
	NCC	0.0025	0.0032	0.0043	0.0029	0.0032
	GSI	0.0038	0.0022	0.0028	0.0031	0.0017
Ref. [40]	SSIM	0.00113		0.00192	0.00161	0.00126
	NCC	0.0035		0.0027	0.0038	0.0035
	GSI	0.0029		0.0023	0.0016	0.0018
Ref. [41]	SSIM	0.3406	0.3429	0.3016	0.4008	0.3586
	NCC	0.3039	0.2858	0.3074	0.3495	0.3681
	GSI	0.2570	0.2708	0.3098	0.3496	0.3622

D. PIXELS' DIFFERENCE ASSESSMENT

The proposed algorithm exhibits lower mean absolute error and better tradeoffs of mean squared error and peak signal-to-noise ratio in comparison to existing methodologies [42], [43], signifying fewer relative differences between corresponding pixels. The average of the squared differences between corresponding pixels are sufficiently high to the ratio between the maximum possible signal values and the introduced noise in the encryption process, in Table 12, indicates effective preservation of image quality during encryption.

TABLE 12. Comparative analysis of proposed scheme with existing methodologies for Pixels' difference analysis.

Algorithm	Analysis	Reference image				
		Pepper	Airplane	Lena	Baboon	Sailboat
Proposed	MAE	84.64	75.88	79.89	74.65	68.37
	MSE	5496.40	7332.97	4847.39	4417.28	6844.17
	PSNR	10.76	9.51	11.31	11.71	9.81
Ref. [42]	MAE	75.25	85.41	78.89	76.48	-
	MSE	8334	10,933	9290	8643	-
	PSNR	8.9219	7.7434	8.4506	8.764	-
Ref. [43]	MAE	82.0156	-	77.409	75.3335	82.0101
	MSE	10,074.0	-	8890.05	8345.25	10,063.3
	PSNR	8.09877	-	8.64176	8.91641	8.10339

TABLE 13. Comparative analysis of proposed scheme with existing methodologies for Pixels' fidelity analysis.

Algorithm	Analysis	Reference image				
		Pepper	Airplane	Lena	Baboon	Sailboat
Proposed	NAE	0.0499	0.0399	0.0455	0.0441	0.0458
	AD	0.0508	0.0263	0.0272	0.0312	0.0428
	MD	221	223	223	199	233
Ref. [41]	NAE	0.0494	0.0375	0.0480	0.0231	0.0617
	AD	0.0195	0.0236	0.0198	0.0516	0.0239
	MD	143	127.5	110.3	138.9	112.2
Ref. [44]	NAE	0.6306	0.4639	0.5926	0.5870	-
	AD	7.9524	5.1054	4.1009	5.9597	-
	MD	226	231	235	210	-

E. PIXELS' FIDELITY ASSESSMENT

The proposed algorithm maintains close alignment of pixel values between the original and encrypted images, resulting in a minimal average difference and preserving the image quality effectively. In comparison to existing methodologies, [41], [44], lower normalized absolute errors and average differences between corresponding pixel values, in Table 13, with the proposed method ensures the encrypted images retain their integrity and resistivity to unauthorized access and tampering.

In summary, the proposed algorithm outperforms existing methods in a comprehensive range of analyses, demonstrating its superior resilience and effectiveness in preserving digital images against a diverse set of attacks and instabilities. This makes it a promising advancement in the collateral era.

V. CONCLUSION

In forthcoming frameworks, as adversaries increasingly employ advanced AI technologies, it is anticipated that many image encryption schemes may become vulnerable to a range of threats. The presented image encryption scheme utilizes billiard quantum chaos on the secure shared key, incorporating true randomness in the data. This arrangement ensures that an adversary cannot circumvent the protocol, even if one of the secrets from the key pairs is compromised. Notably, the experiment is conducted without relying on assumptions

of computational hardness. The results of the experiment confirm that quantum physics enables enhanced security tradeoffs for specific computing tasks within classical communications. Both performance and security assessments validate the proposed method's superior resilience compared to the state-of-the-art approaches when subjected to hostile attacks. It is worth noting that the outcomes generated by the proposed methodology align well with the existing technology. This suggests that our work indicates the promising domain of quantum practices to fortify the security of classical image encryption schemes.

REFERENCES

- [1] M. Li, M. Wang, H. Fan, K. An, and G. Liu, "A novel plaintext-related chaotic image encryption scheme with no additional plaintext information," *Chaos, Solitons Fractals*, vol. 158, May 2022, Art. no. 111989.
- [2] A. Daoui, H. Karmouni, O. E. Ogrı, M. Sayyouri, and H. Qjidaa, "Robust image encryption and zero-watermarking scheme using SCA and modified logistic map," *Expert Syst. Appl.*, vol. 190, Mar. 2022, Art. no. 116193.
- [3] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, "FPGA implementation of a chaos-based image encryption algorithm," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9926–9941, Nov. 2022.
- [4] K. L. Neela and V. Kavitha, "Blockchain based chaotic deep GAN encryption scheme for securing medical images in a cloud environment," *Int. J. Speech Technol.*, vol. 53, no. 4, pp. 4733–4747, Feb. 2023.
- [5] H. Muhammad Waseem and S. O. Hwang, "Design of highly nonlinear confusion component based on entangled points of quantum spin states," *Sci. Rep.*, vol. 13, no. 1, p. 1099, Jan. 2023.
- [6] C. DeCusatis and E. Mcgettrick, "Near term implementation of Shor's algorithm using qiskit," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 1564–1568.
- [7] B. Khanal, J. Orduz, P. Rivas, and E. Baker, "Supercomputing leverages quantum machine learning and Grover's algorithm," *J. Supercomput.*, vol. 79, no. 6, pp. 6918–6940, Apr. 2023.
- [8] M. W. Hafiz and S. O. Hwang, "A probabilistic model of quantum states for classical data security," *Frontiers Phys.*, vol. 18, no. 5, pp. 1–12, Oct. 2023.
- [9] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of image ciphers with permutation-substitution network and chaos," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 6, pp. 2494–2508, Jun. 2021.
- [10] J. Shi, S. Chen, T. Chen, T. Zhao, J. Tang, Q. Li, C. Yu, and H. Shi, "Image encryption with quantum cellular neural network," *Quantum Inf. Process.*, vol. 21, no. 6, p. 214, Jun. 2022.
- [11] M. Hu, J. Li, and X. Di, "Quantum image encryption scheme based on 2D Sine 2-Logistic chaotic map," *Nonlinear Dyn.*, vol. 111, no. 3, pp. 2815–2839, 2023.
- [12] S. Zhou, Y. Qiu, G. Qi, and Y. Zhang, "A new conservative chaotic system and its application in image encryption," *Chaos, Solitons Fractals*, vol. 175, Oct. 2023, Art. no. 113909.
- [13] Z. Wang, M. Xu, and Y. Zhang, "Review of quantum image processing," *Arch. Comput. Methods Eng.*, vol. 29, no. 2, pp. 737–761, 2022.
- [14] M. F. Alotaibi, N. Raza, M. H. Rafiq, and A. Soltani, "New solitary waves, bifurcation and chaotic patterns of fokas system arising in monomode fiber communication system," *Alexandria Eng. J.*, vol. 67, pp. 583–595, Mar. 2023.
- [15] Y. Li, A. H. Aghvami, and D. Dong, "Intelligent trajectory planning in UAV-mounted wireless networks: A quantum-inspired reinforcement learning perspective," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1994–1998, Sep. 2021.
- [16] Y. Li, A. H. Aghvami, and D. Dong, "Path planning for cellular-connected UAV: A DRL solution with quantum-inspired experience replay," *IEEE Trans. Wireless Commun.*, vol. 21, no. 10, pp. 7897–7912, Oct. 2022.
- [17] K. Hashimoto, K. Murata, N. Tanahashi, and R. Watanabe, "Krylov complexity and chaos in quantum mechanics," 2023, *arXiv:2305.16669*.
- [18] E. G. Holliday, J. F. Lindner, and W. L. Ditto, "Solving quantum billiard eigenvalue problems with physics-informed machine learning," *AIP Adv.*, vol. 13, no. 8, pp. 085013-1–085013-7, Aug. 2023, doi: 10.1063/5.0161067.
- [19] E. G. Carnio, H.-P. Breuer, and A. Buchleitner, "Wave-particle duality in complex quantum systems," *J. Phys. Chem. Lett.*, vol. 10, no. 9, pp. 2121–2129, 2019.

- [20] R. Garcia and D. Reznik, *Discovering Poncelet Invariants in the Plane*. Rio de Janeiro, Brazil: IMPA, 2021, pp. 147–143.
- [21] D. Clemente-López, E. Tlelo-Cuautle, L.-G. de la Fraga, J. de Jesús Rangel-Magdaleno, and J. M. Muñoz-Pacheco, “Poincaré maps for detecting chaos in fractional-order systems with hidden attractors for its Kaplan–Yorke dimension optimization,” *AIMS Math.*, vol. 7, no. 4, pp. 5871–5894, 2022.
- [22] S. Sahoo and B. K. Roy, “Design of multi-wing chaotic systems with higher largest Lyapunov exponent,” *Chaos, Solitons Fractals*, vol. 157, Apr. 2022, Art. no. 111926.
- [23] Z. Liang, Q. Qin, and C. Zhou, “An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm,” *Neural Comput. Appl.*, vol. 34, no. 21, pp. 19313–19341, Nov. 2022.
- [24] G. Ye, M. Liu, and M. Wu, “Double image encryption algorithm based on compressive sensing and elliptic curve,” *Alexandria Eng. J.*, vol. 61, no. 9, pp. 6785–6795, Sep. 2022.
- [25] A. G. Weber. (2006). *The USC-SIPI Image Database: Version 5*. [Online]. Available: <http://sipi.usc.edu/database/>
- [26] P. Liu, X. Wang, and Y. Su, “Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 5, pp. 2506–2519, May 2023.
- [27] Y. Xian, X. Wang, and L. Teng, “Double parameters fractal sorting matrix and its application in image encryption,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 6, pp. 4028–4037, Jun. 2022.
- [28] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, and X. Tang, “Asynchronous updating Boolean network encryption algorithm,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 8, pp. 4388–4400, Aug. 2023.
- [29] Y. Zhang and W. Luo, “Vector-based efficient data hiding in encrypted images via multi-MSB replacement,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 11, pp. 7359–7372, Nov. 2022.
- [30] Y. Su, L. Teng, P. Liu, S. Unar, X. Wang, and X. Fu, “Visualized multiple image selection encryption based on log chaos system and multilayer cellular automata saliency detection,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 9, pp. 4689–4702, Sep. 2023.
- [31] H. Xu, H. Hu, S. Chen, Z. Xu, Q. Li, T. Jiang, and Y. Chen, “Hyperspectral image reconstruction based on the fusion of diffracted rotation blurred and clear images,” *Opt. Lasers Eng.*, vol. 160, Jan. 2023, Art. no. 107274.
- [32] A. Alghafis, H. M. Waseem, M. Khan, S. S. Jamal, M. Amin, and S. I. Batool, “A novel digital contents privacy scheme based on quantum harmonic oscillator and Schrodinger paradox,” *Wireless Netw.*, vol. 2020, pp. 1–20, May 2020.
- [33] H. M. Waseem, A. Alghafis, and M. Khan, “An efficient public key cryptosystem based on dihedral group and quantum spin states,” *IEEE Access*, vol. 8, pp. 71821–71832, 2020.
- [34] U. Erkan, A. Toktas, and Q. Lai, “2D hyperchaotic system based on schaffer function for image encryption,” *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 119076.
- [35] N.-R. Zhou, L.-L. Hu, Z.-W. Huang, M.-M. Wang, and G.-S. Luo, “Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm,” *Expert Syst. Appl.*, vol. 238, Mar. 2024, Art. no. 122052.
- [36] Q. Lai, G. Hu, U. Erkan, and A. Toktas, “A novel pixel-split image encryption scheme based on 2D Salomon map,” *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118845.
- [37] A. Paul, S. Kandar, and B. C. Dhara, “Image encryption using permutation generated by modified regula-falsi method,” *Appl. Intell.*, vol. 52, no. 10, pp. 10979–10998, Aug. 2022.
- [38] X. Liu, X. Tong, Z. Wang, and M. Zhang, “Uniform non-degeneracy discrete chaotic system and its application in image encryption,” *Nonlinear Dyn.*, vol. 108, no. 1, pp. 653–682, Mar. 2022.
- [39] N. Rani, S. R. Sharma, and V. Mishra, “Grayscale and colored image encryption model using a novel fused magic cube,” *Nonlinear Dyn.*, vol. 108, no. 2, pp. 1773–1796, Apr. 2022.
- [40] N. Abughazalah, A. Latif, M. W. Hafiz, M. Khan, A. S. Alanazi, and I. Hussain, “Construction of multivalued cryptographic Boolean function using recurrent neural network and its application in image encryption scheme,” *Artif. Intell. Rev.*, vol. 56, no. 6, pp. 5403–5443, Jun. 2023.
- [41] S. Sundarakrishnan, B. J. B. Jaison, and S. P. R. S. P. Raja, “Secured color image compression based on compressive sampling and lü system,” *Inf. Technol. Control*, vol. 49, no. 3, pp. 346–369, Sep. 2020.
- [42] M. Ahmad, S. Agarwal, A. Alkhayyat, A. Alhudaif, F. Alenezi, A. H. Zahid, and N. O. Aljehane, “An image encryption algorithm based on new generalized fusion fractal structure,” *Inf. Sci.*, vol. 592, pp. 1–20, May 2022.
- [43] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, “Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption,” *Symmetry*, vol. 15, no. 5, p. 1081, May 2023.
- [44] M. W. Hafiz, W.-K. Lee, S. O. Hwang, M. Khan, and A. Latif, “Discrete logarithmic factorial problem and Einstein crystal model based public-key cryptosystem for digital content confidentiality,” *IEEE Access*, vol. 10, pp. 102119–102134, 2022.



SEONG OUN HWANG (Senior Member, IEEE) received the B.S. degree in mathematics from Seoul National University, in 1993, the M.S. degree in information and communications engineering from Pohang University of Science and Technology, in 1998, and the Ph.D. degree in computer science from Korea Advanced Institute of Science and Technology, in 2004, South Korea. He worked as a Software Engineer at LGCNS Systems, Inc., from 1994 to 1996. He also worked as a Senior Researcher at the Electronics and Telecommunications Research Institute (ETRI), from 1998 to 2007. He worked as a Professor at the Department of Software and Communications Engineering, Hongik University, from 2008 to 2019. He is currently a Professor with the Department of Computer Engineering, Gachon University. His research interests include cryptography, cybersecurity, and artificial intelligence. He is also an Editor of *ETRI Journal*.



HAFIZ MUHAMMAD WASEEM received the B.S. degree in electronics engineering from the COMSATS Institute of Information Technology, Pakistan, in 2014, the M.S. degree in electrical engineering from the Institute of Space Technology (IST), Pakistan, in 2018, and the Ph.D. degree in computer engineering from Gachon University, South Korea, in 2023. He worked as an Assistant Manager at the Telecommunications Industry, from 2014 to 2018. He is currently an Assistant

Professor with the Department of Computer Engineering, Gachon University. His research interests include quantum computing, cryptography, and quantum AI.



NOOR MUNIR received the B.S. degree in mathematics from the University of Wah, Wah Cantt, Pakistan, in 2017, and the M.S. and Ph.D. degrees in mathematics from the Institute of Space Technology, Islamabad, Pakistan, in 2019 and 2022, respectively. She worked as a Research Associate at the Cyber and Information Security Laboratory (CISL) Islamabad, from 2017 to 2012. She is currently working as an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea. Her research interests include data encryption, cryptography, cryptanalysis, vulnerability assessment, and machine learning.

• • •