Received 22 August 2022, accepted 10 September 2022, date of publication 19 September 2022,
date of current version 30 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3207781

RESEARCH ARTICLE

Discrete Logarithmic Factorial Problem and Einstein Crystal Model Based Public-Key Cryptosystem for Digital Content Confidentiality

MUHAMMAD WASEEM HAFIZ[1], (Graduate Student Member, IEEE), WAI-KONG LEE[2], (Member, IEEE), SEONG OUN HWANG[2], (Senior Member, IEEE), MAJID KHAN[3], AND ASIM LATIF[4]

[1]Department of IT Convergence Engineering, Gachon University, Seongnam 13120, South Korea
[2]Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea
[3]Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad 44000, Pakistan
[4]Department of Software Engineering, Foundation University, Rawalpindi 46000, Pakistan

Corresponding author: Seong Oun Hwang (sohwang@gachon.ac.kr)

This work was supported in part by the National Research Foundation of Korea Grant funded by the Korea Government [Ministry of Science and ICT (MSIT)] under Grant 2020R1A2B5B01002145, and in part by the Gachon University Research Fund under Grant GCU-202106360001.

ABSTRACT Public-key encryption is extensively used to provide digital data confidentiality and deliver the security features, such as nonrepudiation (digital signature) and secure key exchange. Conventional public-key schemes are based on mathematical problems with inflexible constraints, and the security of digital contents relies on computational complexity. In the era of emerging technologies, most public-key image encryption schemes are susceptible to various threats. We propose a novel public-key encryption in this article with near-ring criteria and provide confidentiality to private data with the microstates of the Einstein crystal model. The virtual oscillator generated by microstates of initial oscillators for the common secrets with the public-key scheme produces unique states to encrypt digital data. The privacy-preserved structure, that mimics the data stream of digital content with the behavior of the improved Einstein crystal model, describes a system in terms of microstates to generate diffusion in the plain data with unique states of a virtual oscillator. The performance and digital forensic evaluations, such as randomness, histogram uniformity, pixels' correlation, pixels' similarity, visual strength, pixels' incongruity, key sensitivity, linear and differential attacks, noise, and occlusion attacks analyses, certify the resistivity of the proposed algorithm against potential threats and provide superior capacity in comparison to existing methodologies to hostile certain attacks.

INDEX TERMS Discrete logarithmic factors problem, Einstein crystal model, information security, image encryption, key exchange, Monte Carlo random walk, public-key cryptography.

I. INTRODUCTION

Rapid developments in communication technology have resulted in tremendous growth in multimedia and digital communication. The exchange of digital data across the internet is becoming more prevalent, and the data might be subject to security issues such as illegal access and modification. Secure information transmission over a public channel has an incredible impact and is dynamically imperative due to the risk of theft and manipulation. The ability to process digital content securely is imperative for the public and officialdom [1], and improvements within the systems bring us near to such a variation that allows us to explore the intersection of next-generation networks and cybersecurity.

Cybersecurity is an important aspect of communication because it helps to protect digital content, software, and

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

hardware from malicious attacks enabling access to significant information and causing interruptions in private data. Eventually, the victims of cyber-attacks suffer from economic and social loss [2].

Digital content exists in many forms, including text and images. Normally, images contain rich visual data. Consistency in color depth enables object recognition, and texture provides high-frequency detail and information about shape and size. This makes digital content more challenging to process securely, compared to ordinary content. The significant applications for image encryption schemes in public and private sectors are in satellite imagery [3], military surveillance [4], healthcare industries for telemedicine [5], internet banking transactions [6], etc.

As the proliferation of digital content grows exponentially, most of the algorithms specifically designed to encrypt images are unable to cope with all aspects of security. In the last few decades, several image encryption schemes were proposed based on domain transformation [7], DNA computing [8], vector quantization [9], chaotic and hyper-chaotic systems [10], etc. These schemes have weak security parameters that are unable to attain real-time encryption. The image encryption scheme in [7] using fractional Fourier transform and Jigsaw transform has sufficient algorithm complexity but weak security and performance results. The grayscale image encryption scheme in [11] is based on bit-plane operations and the chaotic maps has low encryption efficiency due to the complex computations of bit-plane operations. To improve its efficiency, the authors recommended a chaos-based mixed image-element grayscale image encryption scheme in [12]. Although it increased encryption efficiency, security analyses indicated it is weaker than the previous scheme. The estimated reckonings of histograms of encrypted images are not uniformly distributed, hence this scheme may also be vulnerable to statistical attacks.

Nowadays, most image encryption schemes are developed on the notion of confusion [13], [14] and diffusion components [15], and the construction of traditional block and stream ciphers were used in many ways to create confusion in the image data. Most of the modern privacy-preserving structures are established in light of substitution-permutation networks (SPN) in which confusion criteria are fulfilled by substitution, and permutation is utilized to perform diffusion in the image data [16]. By aiming at all the above problems, we developed a new encryption scheme that provides the ultimate performance and security.

At present, digital content protection surveys all the points of view influencing communication and computation security with the advancement of artificial intelligence (AI). Asymmetric encryption methods must be secure from chosen plain text attacks (CPA) and chosen ciphertext attacks (CCA). RSA is not secure against CPA even with padding, and encryption of the same plaintext always generates the same ciphertext due to its deterministic aspect. If the message itself is amenable to brute force, it can be recovered by trying potential message values until a match is found [17]. Also, RSA is insecure against CCA if the message is a small integer. For instance, if the message is 200-bit integer and the public exponent is 3, then the available public message will be a 600-bit integer. This means the message can be recovered using a non-modular cube root, which is simple and easy to compute [18]. Furthermore, for chosen-ciphertext (CCA) security, a variation of the Cramer-Shoup (CS) method [19] makes use of the computational Diffie-Hellman (CDH) assumption. The high-security cost of this cipher is that the size of ciphertexts is much larger than with the CS scheme (which is based on the decisional Diffie-Hellman assumption) [20].

The proposed discrete logarithmic factorial problem (DLFP) based public-key establishment scheme in this article provides a secure way to generate common keys. The adversary can't bypass the protocol even with one of the secrets from pairs, and the developed scheme resists the CPA and CCA attacks. To share the digital content securely on the shared key, we developed a privacy-preserved structure that mimics the data stream with the behavior of the improved Einstein crystal model, which reflects wave–particle duality [21], [22]. This model describes a system in terms of microstates, whereas each microstate acts as a harmonic oscillator in a three-dimensional potential. We generated diffusion in the plain data with unique states of a virtual oscillator followed by a random walk on inimitable points without including the full dynamics (Monte Carlo). In the first approximation, we introduced a simplified interaction between the oscillators by allowing data transfer randomly from one oscillator to another with no overhead. The stochastic model of uncorrelated states has similar behavior to generate sequence as in quantum chaos and provides the chaos transition from a Poisson to a Gaussian distribution. The security and performance measures for the proposed model validate the effectiveness in comparison with existing techniques.

This article is organized into six sections. The preliminaries of the Einstein crystal model, Monte Carlo modification, and DLFP key establishment are explained in Section II. The anticipated algorithm and its execution on standard images are deliberated in Section III, with performance and security evaluations assessed in Section IV. Digital forensic analysis of the outcomes from the proposed strategy is presented in Section V, and concluding notes with upcoming prospects are given in Section VI.

II. FUNDAMENTAL TERMINOLOGIES

The basic terminologies to design the encryption/ decryption algorithm are explained in this section. We developed the DLFP key exchange algorithm and set the Einstein crystal model—Monte Carlo design using the established key with the exchange algorithm.

A. PROPOSED DLFP KEY ESTABLISHMENT ALGORITHM

Public-key algorithms establish common secrets between users for secure communication over public channels [23]. Most of the effective public-key schemes are based on finite commutative rings. The addition and multiplication

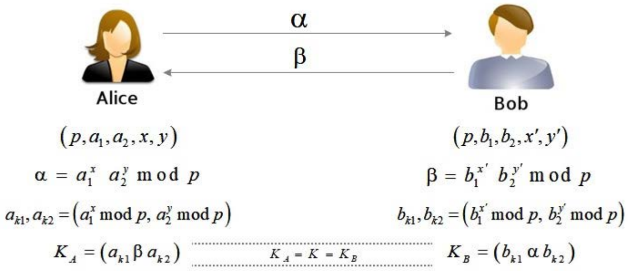

α
β
Alice
Bob
(p, a_1, a_2, x, y)
(p, b_1, b_2, x', y')
$\alpha = a_1^x\ a_2^y \bmod p$
$\beta = b_1^{x'}\ b_2^{y'} \bmod p$
$a_{k1}, a_{k2} = (a_1^x \bmod p,\ a_2^y \bmod p)$
$b_{k1}, b_{k2} = (b_1^{x'} \bmod p,\ b_2^{y'} \bmod p)$
$K_A = (a_{k1}\, \beta\, a_{k2})$
$K_A = K = K_B$
$K_B = (b_{k1}\, \alpha\, b_{k2})$

FIGURE 1. Demonstration of the DLFP key generation algorithm.

operations for the binary satisfy the axioms of the entire ring, except sometimes for the distributive and commutative laws, and these systems are noted as near-rings.

$(N, +, \bullet)$ triplet refer as near-ring if

- an ordered pair $(N, +)$ is a group, and
- an ordered pair $(N, \bullet)$ is a semigroup, and for each element $n_1,\ n_2,\ n_3 \in N$, $(n_1 + n_2) \cdot n_3 = n_1 \cdot n_3 + n_2 \cdot n_3$

Assumptions: For a factorial problem, the component ω of non-abelian group, near-ring N and sub near-rings $N_1,\ N_2 \in N$, determine the elements $a_1 \in N_1$ and $a_2 \in N_2$ that satisfy $\omega = a_1\, a_2$.

Given the prime p for DLFP, when the generator of the cyclic group $\mathbb{Z}_p$ is α and element $\beta \in \mathbb{Z}_p$, find an integer $0 \leq x \leq p - 1$ that satisfies $\alpha^x = \beta$.

For a DLFP, N is a near-ring non-abelian identity constituent e and $a_1,\ a_2,\ \alpha$ are the arbitrary components of N, and $x,\ y$ are the random elements of $\mathbb{Z}_p$. For $\alpha = a_1^x\, a_2^y$, calculate $a_1,\ a_2 \in N$ and $x,\ y \in \mathbb{Z}_p$.

DLFP-based key establishment: Let N be a near-ring with identity e, and let $a_1, a_2 \in N$ be the two random numbers that satisfy $\langle a_1 \rangle \cap \langle a_2 \rangle = e$. The given product is split into pair $(a_1^x, a_2^y) \in N \times N$, where x and y are randomly picked arbitrary integers.

- Alice chooses $a_1, a_2 \in N$, generates private key (a_1^x, a_2^y), and shares public key $\alpha = a_1^x, a_2^y$ with Bob.
- Bob chooses $b_1, b_2 \in N$, generates private key $(b_1^{x'}, b_2^{y'})$, and shares public key $\beta = b_1^{x'}, b_2^{y'}$ with Alice.
- Alice uses her secrets and computes $K_A = a_1^x \beta a_2^y = a_1^{x+x'} + a_2^{y+y'}$.
- Bob uses his secrets and computes $K_B = b_1^{x'} \alpha b_2^{y'} = b_1^{x+x'} + b_2^{y+y'}$.
- The generated common secret between Alice and Bob is $K = K_A = K_B$.

Let the communicating parties, Alice and Bob, agree on some prime numbers, p , in order to generate the common secret. Fig. 1 demonstrates the establishment of the common key using the secret credentials.

Example: Validation of the proposed design using a simple evaluation is demonstrated in this example. Let Alice and Bob agree on a prime number, $n = 37$, to generate the common secret with their private credentials. These credentials include two secret primitives and two randomly selected values for each of them. After generating and sharing the public keys, they are able to develop a common secret between them using their private key pairs with each other's shared public key. The evaluation of the common secret between Alice and Bob from their private keys is demonstrated in Table 1.

Security analysis of the proposed key establishment algorithm: An adversary can bypass the protocol by obtaining Alice's or Bob's private key in the following attacks.

The possible attack on Alice's private key is to find the elements a_1^x and a_2^y that commute with each element of the sub–near-rings of N_1 and N_2, such that $K_A = a_1^x\, \beta\, a_2^y$. Similarly, the attack on Bob's private key is to find the elements $b_1^{x'}$ and $b_2^{y'}$ that commute with each element of the sub–near-rings of N_1 and N_2 such that $K_B = b_1^{x'}\, \alpha\, b_2^{y'}$.

Suppose $N_1 = \langle n_1, \ldots, n_k \rangle$, and let us say an adversary is trying to find x but has no knowledge of where to choose y in the beginning. The adversary just knows that it commutes with all the elements in N_1. Even if he computes $N_1 = N\,(n_1, \ldots, n_k)$ and $N_2 = N\left(n_1', \ldots, n_k'\right)$, it is hard to determine a_1^x and a_2^y.

B. EINSTEIN CRYSTAL MODEL AND MONTE CARLO MODIFICATION

The Einstein crystal model describes a system in terms of microstates wherein the atoms in the crystal do not interact directly. Each atom acts as a three-dimensional harmonic oscillator with a central potential, and the total system consists of N atoms [24], [25]. The atoms in the system share the total energy in the system. Each atom in a three-dimensional structure consists of three independent oscillators in the x, y, and z directions. In other words, a system with N oscillators consists of ${}^{N}\!/_{3}$ atoms. Each oscillator has potential $v\,(x) = \frac{1}{2} k\, x^2$, where k is the spring constant and x is the derivation of the equilibrium position. The energies of such oscillators are quantized with several possible values ($\in = h\, v\, n$) where $n = 0,\ 1,\ 2,\ \ldots$ can only be integers. The measurement of energy is $h\, v = \in$, and for the dimensionless energy states, we choose the symbol q. Let us consider a simplified four-oscillator system with $N = 4$ and quantized level $q = 2$. In Fig. 2, we describe the states by using a simple illustration with possible energy levels for $N = 4$ oscillators. There are generally two possibilities.

1) In Case A, one oscillator may be at energy level 2 with the others at energy level 0.
2) In Case B, two oscillators may be at energy level 1 with the others at energy level 0.

The possible configurations by sequence are n_1, n_2, n_3, n_4, where $n_i = 0,\ 1,\ 2,\ \ldots$ describes the state of oscillator i.

Case A: The oscillator at energy level 2 can be placed in N = 4 possible places: (2,0,0,0), (0,2,0,0), (0,0,2,0), and (0,0,0,2). There are four possible states of the system with one oscillator at energy level 2, and the rest at energy level 0.

Case B: The two oscillators at level 1 can be placed in six possible configurations. If we place the first energy unit in oscillator 1 and the second in oscillator 2, we get the

TABLE 1. Common secret generation using DLFP.

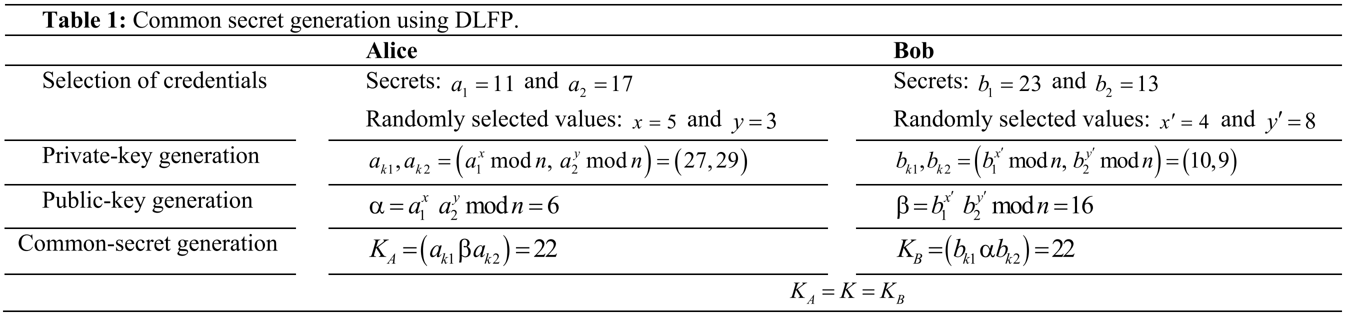


Table 1: Common secret generation using DLFP.

	Alice	Bob
Selection of credentials	Secrets: $a_1 = 11$ and $a_2 = 17$ Randomly selected values: $x = 5$ and $y = 3$	Secrets: $b_1 = 23$ and $b_2 = 13$ Randomly selected values: $x' = 4$ and $y' = 8$
Private-key generation	$a_{k1}, a_{k2} = \left(a_1^x \bmod n,\ a_2^y \bmod n\right) = (27, 29)$	$b_{k1}, b_{k2} = \left(b_1^{x'} \bmod n,\ b_2^{y'} \bmod n\right) = (10, 9)$
Public-key generation	$\alpha = a_1^x\ a_2^y \bmod n = 6$	$\beta = b_1^{x'}\ b_2^{y'} \bmod n = 16$
Common-secret generation	$K_A = \left(a_{k1} \beta a_{k2}\right) = 22$	$K_B = \left(b_{k1} \alpha b_{k2}\right) = 22$
	$K_A = K = K_B$	

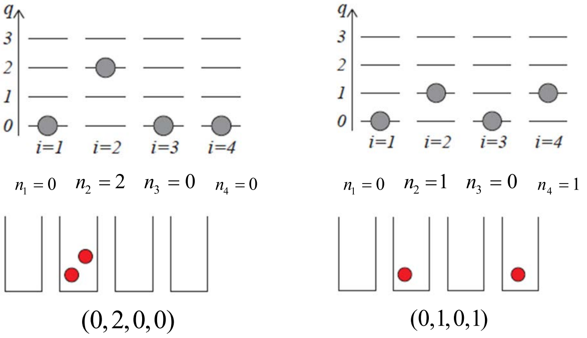


FIGURE 2. Demonstration of the Einstein crystal model.

state (1,1,0,0), but this is the same state we would get if we place the first energy unit in oscillator 2 and the second in oscillator 1. The possible states are therefore (1,1,0,0), (1,0,0,1), (0,0,1,1), (1,0,1,0), (0,1,0,1), and (0,1,1,0).

Time development of the Einstein crystal (Monte Carlo) model: The Einstein crystal model only describes the system in terms of the microstate, (n_1, n_2, ..., Nn). If the system is in one particular microstate, we have no physical laws that tell us how the system can develop into another microstate. To include dynamics, we need to add further assumptions to the model. When we defined the Einstein crystal, we assumed there were no interaction between the individual oscillators, whereas for the molecular dynamics simulations, the particles had both specific positions in the crystal and they interacted with their neighbors [26]. We extend the Einstein crystal model to include both simplified interactions and the relative positions of the particles, so that we can model energy flow without including the full dynamics [27]. The number of microstates for the Einstein model with q energy units and N oscillators is specified as follows:

$$\Omega(N, q) = \binom{N - 1 + q}{q} = \frac{(N - 1 + q)!}{q!\,(N - 1)!} \tag{1}$$

We assumed a small modification to the Einstein crystal model to include some of the facts below. The system consists of two parts, A and B, so that each oscillator belongs to either A or B. In the first approximation, we introduced a simplified interaction between the oscillators by allowing energy to move randomly from one oscillator to another by conserving the total energy. This means the system will move from one microstate, S_1, to another microstate, S_2, with the same energy. Hence, both microstates are equally probable, since all microstates are equally probable.

To simulate the random transmission of energy in the system, the process is as follows.

- Select an oscillator (particle) at random, i_1, and transport the energy from this oscillator.
- Select another oscillator (particle) at random, i_2, and receive the energy from n_1.

We generate a virtual state oscillator from oscillators A and B with the same energy. The resulting dynamics of the oscillators are expressed in Fig. 3.

Monte Carlo simulation

In the stochastic model, we generate a sequence of uncorrelated microstates. For each sample, we randomly generate a new microstate, ensuring no correlation with the previous state [28]. We sample many such states in a long sequence before making statistical predictions about the probability of a microstate. This motion is observed to be in a zigzag path and is referred to as a Monte Carlo model for a microcanonical system. There is also a strong connection between the random walk and the Schrödinger equation by replacing time with imaginary time. Quantum chaos is also linked to a Monte Carlo diffusion process for the quantum energy–level spacing sequences. These levels acts as a function to execute a random walk, which infers uncorrelated random increments in the level spacing, and transforms the chaos transition from a Poisson to a Gaussian distribution. The random walk of Monte Carlo microstates is shown in Fig. 4.

III. PROPOSED ALGORITHM

Digital content that navigates through the flowchart described in Fig. 5 produces encrypted streams with high randomness. To demonstrate our idea clearly, we consider here a simplified 22-oscillator system with N = 22 atoms (DLFP, Section II-A) and quantized level q = 256 (for eight-bit images).

Referring to Fig. 5, Alice and Bob assess the shared secret and have enough knowledge to produce microstates at random (Monte Carlo). They can use their common secrets to share data through an insecure communication channel

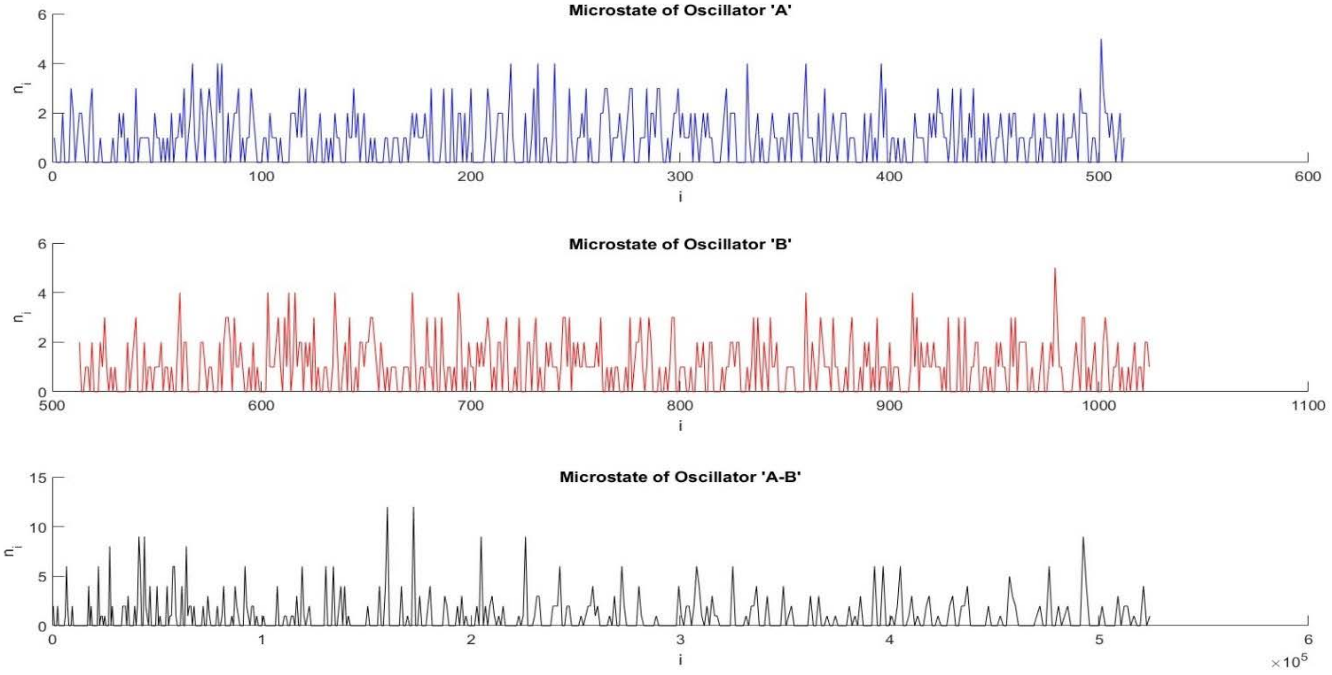


FIGURE 3. **Illustration of development in Einstein crystals over time.**

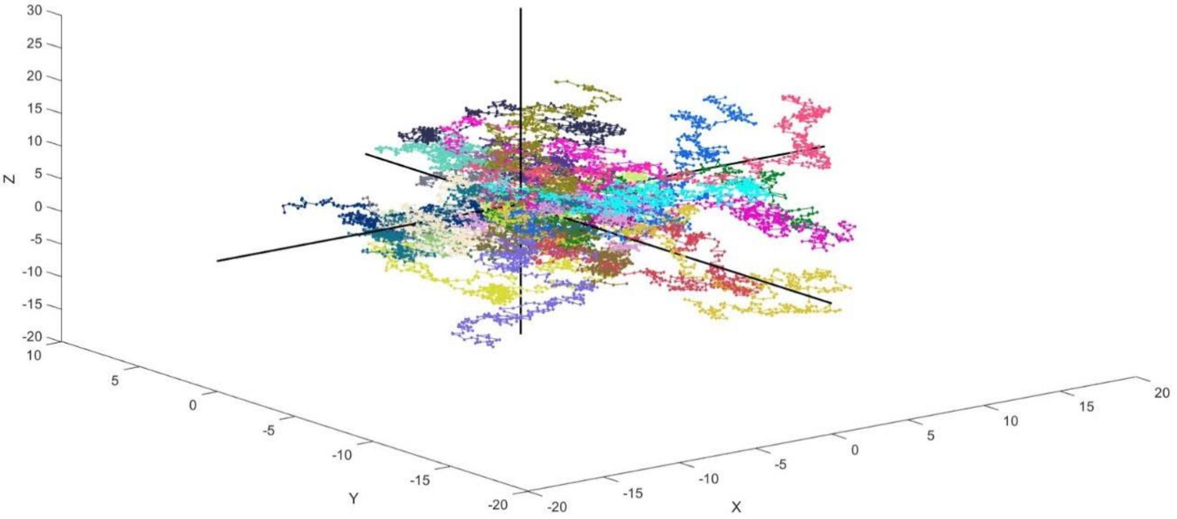


FIGURE 4. **Demonstration of the random walk for 24 particles at 512 steps each.**

by analyzing the microcanonical system and the temporal evolution of the crystal model.

A. PROCEDURE

- First, we established the common secret between Alice and Bob using the DLFP technique, explained in Section II-A.
- After establishing the common secret, we generate the microstates of two oscillators and launch a Monte Carlo random walk sequence with the common secret, as explained in Section II-B.
- By performing a bitwise XOR operation between the microstates of the two generated oscillators, we develop a virtual oscillator.
- For Alice, we operate layer-wise plain image pixels with the microstates of the virtual oscillator to generate diffusion in their values.
- To diffuse the pixel values completely, we pass each layer of the generated cipher image from the virtual

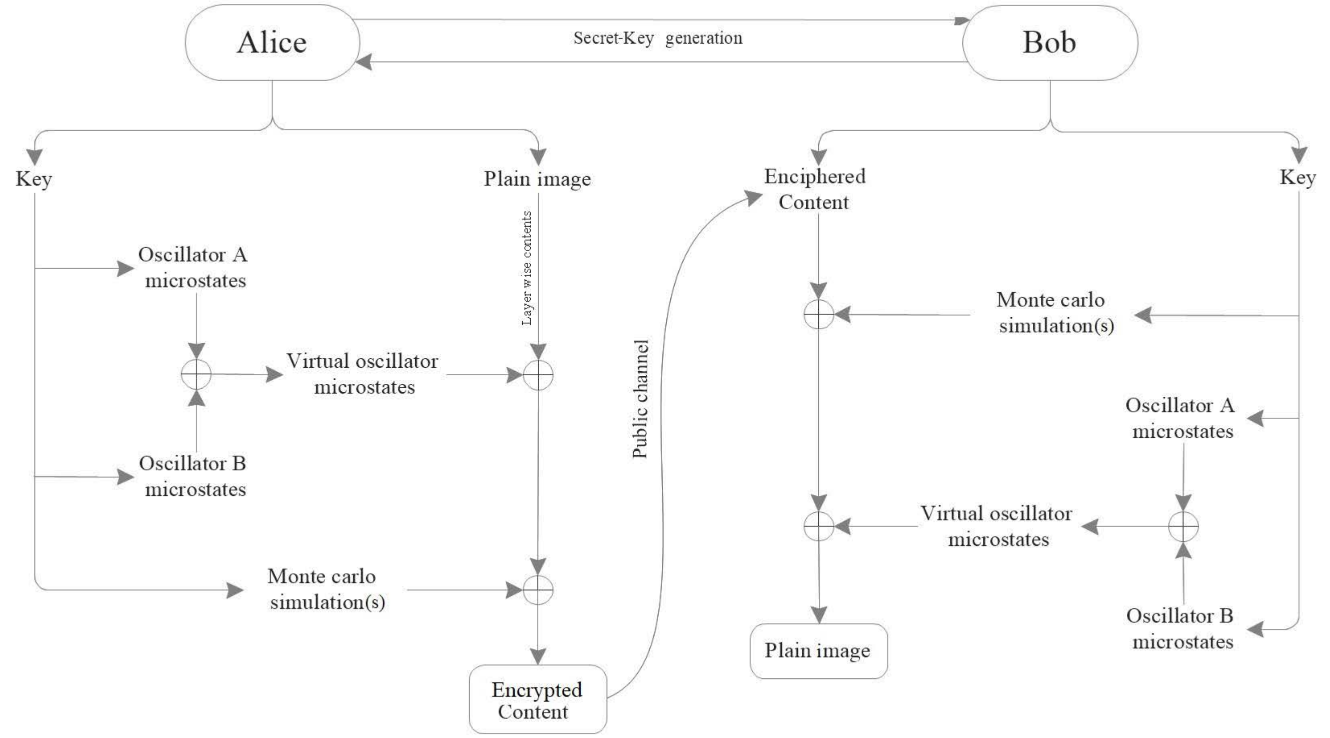


FIGURE 5. Proposed encryption and decryption structure.

oscillator through the random walk sequence of the Monte Carlo simulation.

- The layer-wise encrypted results of the plain images are depicted in Fig. 6.
- Bob will obtain the plain image by following the same procedure on the cipher image but in reverse order.

B. EXPERIMENTATION WITH THE PROPOSED ALGORITHM

We performed an experiment using the standard Airplane and Baboon digital content with dimensions 512 × 512. We process the pixels of each piece of content with the microstates of oscillators A–B and via the Monte Carlo random walk to provide confidentiality for the digital content. The outcomes of the proposed methodology are in Fig. 6.

IV. PERFORMANCE AND SECURITY ANALYSES

We conducted various standard investigations (an uncertainty test, factual assessment, and a sensitivity evaluation) on standard images to measure the strength of the anticipated design of Fig. 5. These images are taken from the database of the Signal and Image Processing Institute (SIPI) [29].

A. RANDOMNESS ANALYSIS

Identification of randomness from the probable esteem is characterized by entropy. It is the source's mean significance value expressing certainty from a set of distinct occurrences $\{x_1, x_2, x_3, \ldots, x_n\}$ with similar probabilities [30], [31]. For digital content, the Shannon entropy is calculated as follows:

$$H = -\sum_{n=0}^{2^N-1} p\left(x_n\right) \log_2 p\left(x_n\right), \tag{2}$$

where $p\left(x_n\right)$ is the probability of source x_n and is expressed in bits. For dissimilarity in eight-bit digital content, the optimum Shannon entropy is 8. Table 2 depicts entropy analysis for plain and encrypted content, as well as assessment with existing techniques.

The outcomes of the proposed method in Table 2 are reasonably close to the perfect estimation of Shannon entropy and outperform the previous methods. These results demonstrate that there is a negligible data loss and the structure in Fig. 5 is resistant to entropy attacks.

B. HISTOGRAM UNIFORMITY ANALYSIS

We processed original and encrypted image content having 256 dark-dimension intensities in order to estimate the consistency of histograms for the proposed methodology [34], [35]. An evaluation of the original and encrypted content for the Airplane and Baboon images from the proposed methodology are demonstrated in Fig. 7 and Fig. 8.

We evaluated the plain and encrypted content in Figs. 7 and 8 to ensure consistency in encrypted content to make the factual assaults hard.

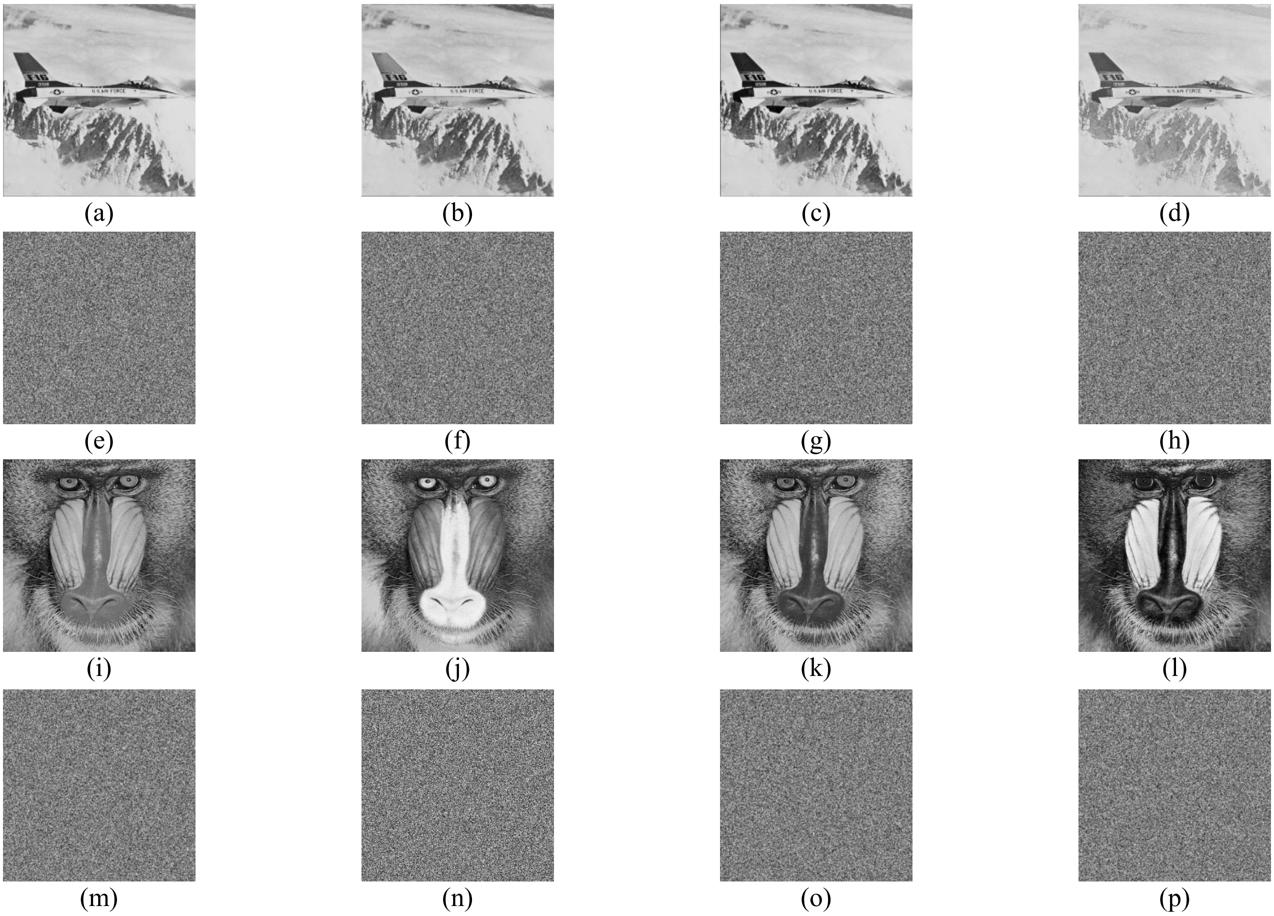


FIGURE 6. Plain and encrypted content of the Airplane and Baboon images: (a-d) Plain Airplane images at gray and RGB scale, (e-h) Encrypted contents of Airplane images at gray and RGB scale; (i-l) Plain Baboon images at gray and RGB scale, (m-p) Encrypted contents of Baboon images at gray and RGB scale.

TABLE 2. Randomness analysis for plain and encrypted content, and comparisons with the most recent approach.

Image	Plain				Encrypted				Ref. [32]	Ref. [33]		
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Airplane	6.70560	6.74894	6.81058	6.26817	7.99936	7.99931	7.99925	7.99927	7.9974	7.9983	7.9982	7.9988
Baboon	7.34846	7.74439	7.44932	7.75129	7.99922	7.99931	7.99921	7.99935	7.9972	7.9985	7.9983	7.9982
Pepper	7.58888	7.35162	7.58118	7.13466	7.99936	7.99933	7.99936	7.99932	-	7.9981	7.9985	7.9986
Lena	7.44506	7.25310	7.59403	6.96842	7.99921	7.99931	7.99933	7.99935	7.9974	7.9986	7.9981	7.9979

C. PIXELS' CORRELATION ANALYSIS

Correlation analysis is the statistical approach used to assess the strength of the association between two quantitative variables. This approach is associated with linear regression analysis, which signifies the statistical method for modeling the relationship between dependent variables. To observe the relationship between the original and encrypted digital content, we performed an analysis between the pixel pairs in horizontal, diagonal, and vertical directions [36], [37].

Let us choose 10,000 combinations of close pixels from the plain and encrypted content, primarily to observe the correspondence in adjacent pixels. The observation of pixel pairs in Airplane and Pepper images at grayscale in Fig. 9-10 is evaluated with the following expression:

$$r_{x,y} = \frac{\sigma_{x,y}}{\sqrt{\sigma_x^2 \sigma_y^2}}, \tag{3}$$

where x and y are the adjacent grayscale pixel values, σ_x^2 and σ_y^2 are the variances, and $\sigma_{x,y}$ is the covariance of random variables x and y.

The encoded information in Figs. 9-10 serves as a barrier (in the sense of quantifiable investigation) to information release. Furthermore, we evaluated the various plain and

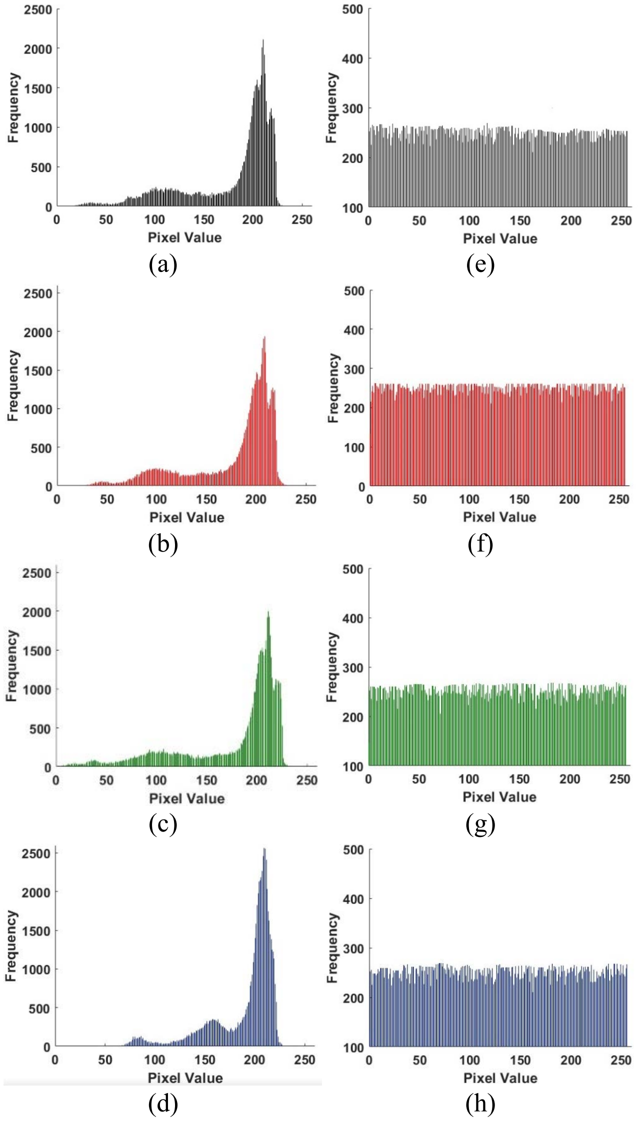


FIGURE 7. Histograms of plain and encrypted Airplane images: (a-d) Histograms of plain image at gray and RGB scales (e-h) Histograms of encrypted image at gray and RGB scales.

encrypted image pairs by computing their two-dimensional correlation coefficients using the following equations [38]:

$$r = \frac{\sum_{i,j=1}^{M,N} (P_{ij} - \overline{P})(C_{ij} - \overline{C})}{\sqrt{\left(\sum_{i,j=1}^{M,N} (P_{ij} - \overline{P})^2\right)\left(\sum_{i,j=1}^{M,N} (C_{ij} - \overline{C})^2\right)}}, \qquad (4)$$

where P and C signify the plain and encrypted content, respectively, with mean approximations of $\overline{P}$ and $\overline{C}$, and M, N denote the height and width of the content.

Table 3 depicts the evaluation of correlation coefficients for plain and encrypted content for the methodology depicted in Fig. 5, as well as their comparisons with the most recent approach.

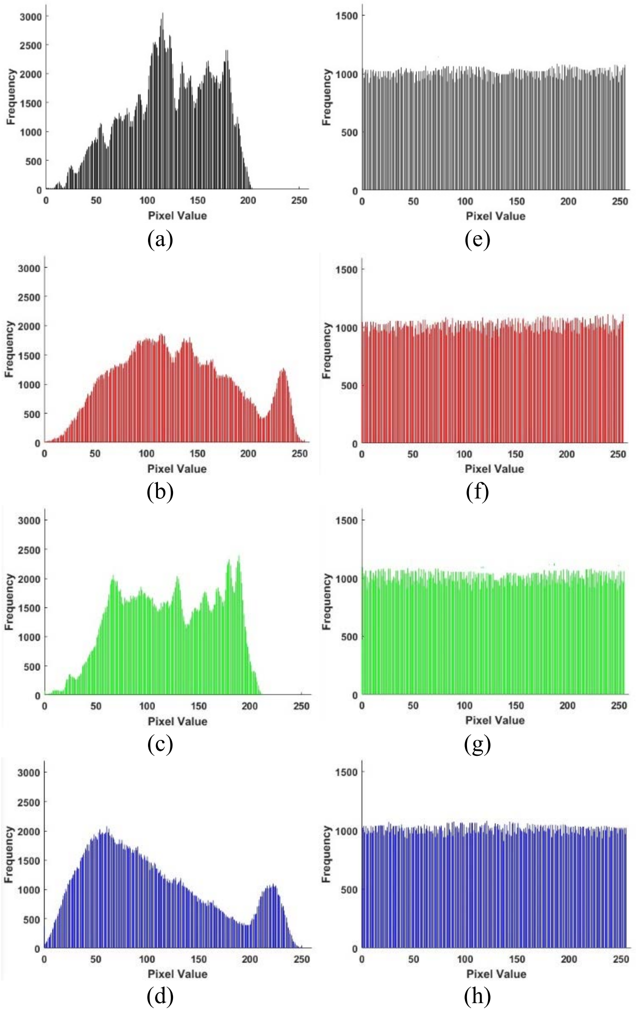


FIGURE 8. Histograms of plain and encrypted Baboon images: (a-d) Histograms of plain image at gray and RGB scales (e-h) Histograms of encrypted image at gray and RGB scales.

TABLE 3. Correlation coefficients for plain and encrypted content in grayscale and RGB color, and assessments with the most recent technique.

Image		Plain content			Encrypted content			Ref. [39]		
	Content	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Airplane	Gray	0.9672	0.9647	0.9647	-0.0019	0.0023	-0.0096	-0.0046	0.0012	-0.0019
	Red	0.9662	0.9331	0.9617	-0.0070	0.0027	-0.0071	-0.0011	-0.0062	0.0003
	Green	0.9695	0.9435	0.9690	-0.0052	0.0029	-0.0091	0.0006	-0.0014	0.0005
	Blue	0.9526	0.9058	0.9410	-0.0030	-0.0002	-0.0105	0.0004	0.0015	-0.0026
Baboon	Gray	0.8654	0.7719	0.7719	-0.0066	0.0032	-0.0065	0.0015	-0.0018	-0.0021
	Red	0.9224	0.8477	0.8680	0.9225	0.0007	-0.0046	0.0010	-0.0014	-0.0013
	Green	0.8825	0.7704	0.8068	-0.0066	0.0013	-0.0046	-0.0012	0.0016	0.0002
	Blue	0.9239	0.8566	0.8827	-0.0060	0.0051	-0.0071	0.0008	-0.0035	-0.0013
Pepper	Gray	0.9812	0.9832	0.9832	-0.0040	0.0019	-0.0077	-0.0055	0.0011	0.0025
	Red	0.9772	0.9592	0.9787	-0.0036	0.0020	-0.0063	-0.0046	0.0012	-0.0019
	Green	0.8825	0.7704	0.8068	-0.0066	0.0013	-0.0046	-0.0021	-0.0034	0.0017
	Blue	0.9769	0.9586	0.9779	-0.0065	0.0000	-0.0047	0.0007	-0.0023	-0.0022
Lena	Gray	0.9737	0.9868	0.9868	-0.0077	-0.0002	-0.0095	-0.0045	0.0013	-0.0070
	Red	0.9813	0.9709	0.9908	-0.0036	-0.0001	-0.0078	-0.0035	-0.0021	0.0002
	Green	0.9713	0.9714	0.9849	0.9713	0.0013	-0.0063	0.0004	-0.0016	0.0002
	Blue	0.9425	0.9244	0.9675	-0.005	-0.0032	-0.0057	0.0001	-0.0008	-0.0041

The correlation coefficients in Table 3 are quite close to zero, which implies the variables are either hardly related or dissimilar, and show results superior to the existing approach.

D. PIXEL SIMILARITY ANALYSES

Similarity analyses measure the resemblance of pixels from among different digital content. To observe the

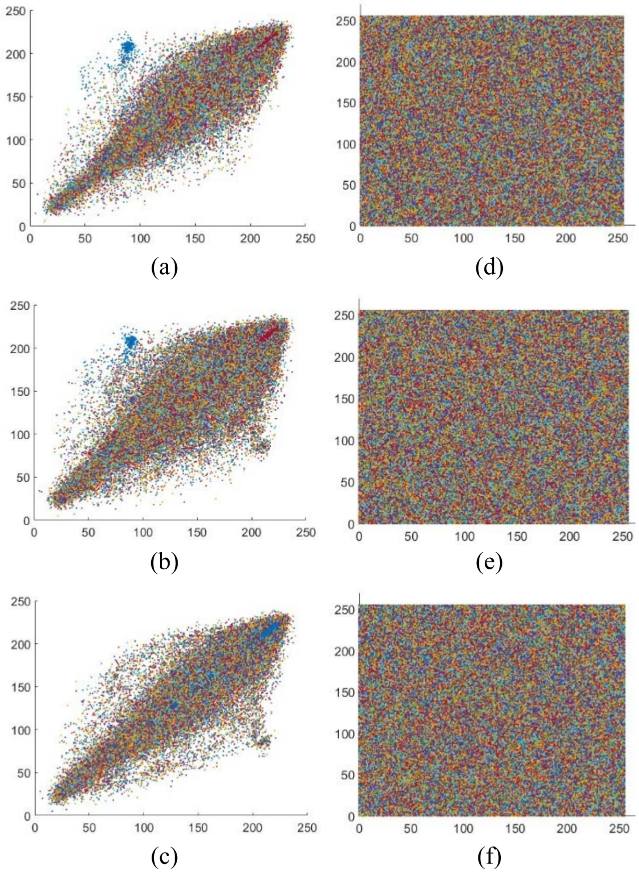


FIGURE 9. Pixel correlation investigations for the Airplane image in the horizontal, diagonal, and vertical directions: (a-c) plain image analysis, (d-f) encrypted image analysis.

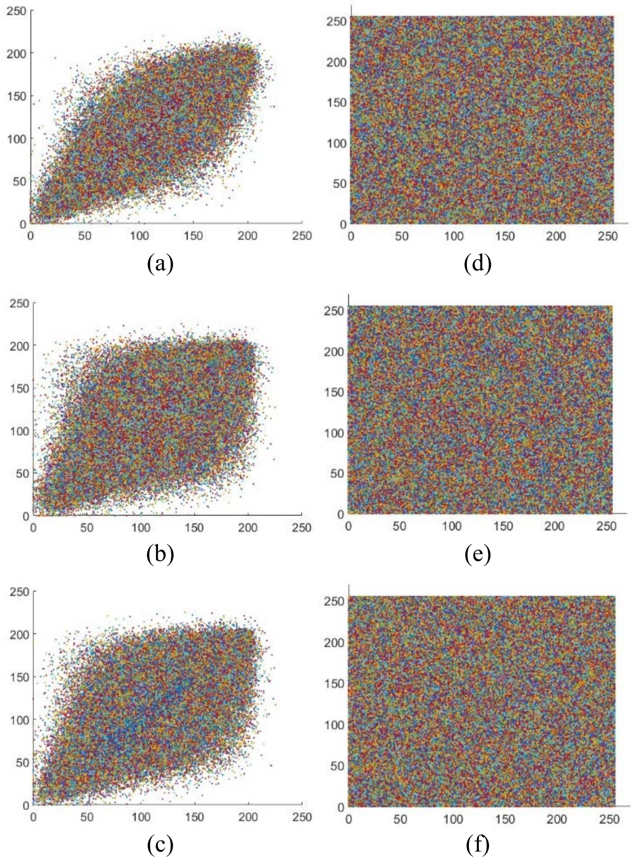


FIGURE 10. Pixel correlation investigations for the Baboon image in the horizontal, diagonal, and vertical directions: (a-c) plain image analysis, (d-f) encrypted image analysis.

pixels' similarity between plain and corresponding encrypted images, we compared the divergence and luminance using structural similarity index measures (SSIM), applied normalized cross-correlation (NCC) to measure the traces of correspondence, and used structural content (SC) to observe the quality of an image with regard to noise and sharpness. NCC also measured the structural similarity between original and encrypted images in Fig. 11. A higher estimation of SSIM, i.e. 1, infers strong resemblance between the original and encrypted images [40]. We also evaluated the maximum difference (MD) to analyze the maximum variation, and evaluated the average difference (AD) to determine the average value between plain and encrypted content having the same dimensions [41], as follows:

$$SSIM = \frac{(2\mu_p\,\mu_c + C_1)(2\sigma_{pc} + C_2)}{(\mu_p^2 + \mu_c^2 + C_1)(\sigma_p^2 + \sigma_c^2 + C_2)}, \tag{5}$$

$$NCC = \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} \frac{P_{k,\,l} \times C_{k,\,l}}{\sum_{k=0}^{M-1}\sum_{l=0}^{N-1} P_{k,\,l}^2}, \tag{6}$$

$$S\,C = \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} \frac{P_{k,\,l}^2}{\sum_{k=0}^{M-1}\sum_{l=0}^{N-1} C_{k,\,l}^2}, \tag{7}$$

$$MD = Max\left|P_{k,l} - C_{k,l}\right|, \tag{8}$$

$$AD = \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} \frac{(P_{k,l} - C_{k,l})}{M \times N}. \tag{9}$$

$P_{k,\,l}$ and $C_{k,\,l}$ represent the plain and encrypted content, μ_p and μ_c represent the mean values, and σ_{pc} is the standard deviation. The evaluation of similarity analyses for the plain-encoded content with the proposed algorithm and assessments with the most recent approach are conveyed in Table 4.

Table 4 shows that there is no pixel resemblance between plain and encrypted image content. Moreover, the approximations of SSIM, SC, and NCC have better consequences than the existing approach.

E. VISUAL STRENGTH ANALYSIS

Visual strength analysis is a statistical approach for measuring the chromatic quality and texture of an image by reflecting the spatial association of pixels in the gray level co-occurrence matrix (GLCM) [42], [43]. The classification

TABLE 4. Pixel-based similitude analyses for plain-encoded content and assessments with the most recent existing approach.

Image	Pixel similitude analyses					Ref. [40]	Ref. [25]	
	SSIM	NCC	SC	MD	AD	SSIM	NCC	SC
Airplane	0.0019	0.0022	0.0018	231	51.0541	0.1075	0.0014	0.0008
Baboon	0.0013	0.0018	0.0011	210	5.9597	0.0957	0.0038	0.0009
Pepper	0.0017	0.0025	0.0017	226	7.9524	0.0815	0.0021	0.0006
Lena	0.0012	0.0027	0.0009	235	4.1099	0.1056	0.0017	0.0012

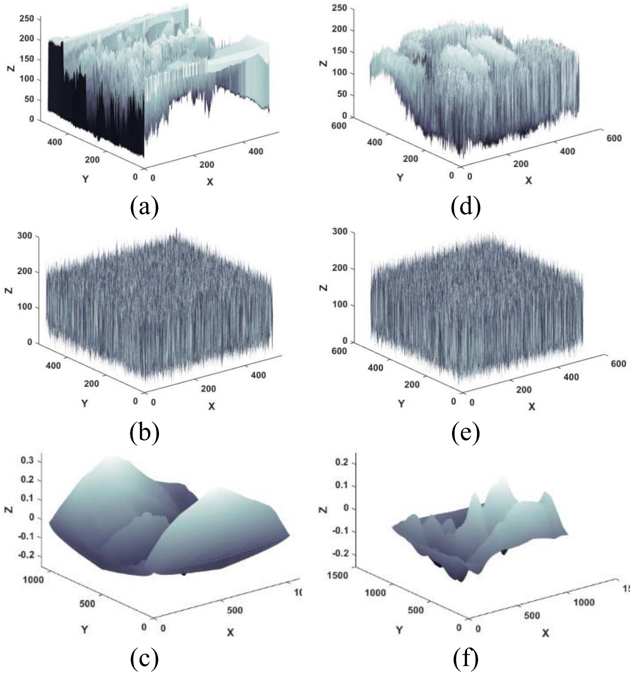


FIGURE 11. Surface plots of NCC for the plain, encrypted, and plain-encrypted Airplane and Baboon images: (a-c) Airplane image and (d-f) Baboon image.

of texture is concerned with region identification from a given set of texture classes. Each of these constituencies has unique characteristics, including contrast, dissimilarity, homogeneity, angular second moment, maximum probability, energy, mean, variance, and correlation.

The amount of local variation present in an image is measured by contrast analysis. It recognizes the objects in the texture of the encrypted content. Dissimilarity analysis measures the heterogeneous effect of an image, and homogeneity analysis investigates the nearness of the distribution of elements in GLCM to GLCM diagonally [44]. The angular second moment is a measure of an image's homogeneity. It uses second-order statistics to estimate the association between groups of two pixels separated by a certain distance. Maximum probability corresponds to the largest entry in the matrix, and resembles the strongest response. The number of variations within a fixed window is measured by energy analysis, and coarse texture has a grain size magnitude of the displacement vector estimated by mean analysis. The variance measures the dispersion of the gray level difference at a certain distance, and the correlation measures the linearity of an image. The correlation will be high if the image follows a linear structure. These GLCM analyses are evaluated with the following expressions:

$$Contrast = \sum_{i,j} |k-l|^2 \rho(k,l), \tag{10}$$

$$Dissimilarity = \sum_{k,l} \rho(k,l)\ |k-l|, \tag{11}$$

$$Homogeneity = \sum_{k,l} \frac{\rho(k,l)}{1+|k-l|}, \tag{12}$$

$$Angular\ \sec ond\ moment\ (ASM) = \sum_{k,l} \rho(k,l)^2, \tag{13}$$

$$Maximum\ probability = Max(\rho(k,l)), \tag{14}$$

$$Energy = \sqrt{ASM}, \tag{15}$$

$$Mean\ (\mu_{k,l}) = \sum_{k,l} k\,l\ (\rho(k,l)), \tag{16}$$

$$Variance = \sum_{k,l} \rho_{k,\,l}\ (\rho(k\,l - \mu_{k,\,l}), \tag{17}$$

$$Correlation = \sum_{k,l} \rho_{k,\,l} \left[\frac{(k-\mu_k)(l-\mu_l)}{\mu_{k,\,l}}\right]. \tag{18}$$

where k and l are the row and column positions of the pixels. The homogeneity and energy of the image are between 0 and 1, and the contrast range is between 0 and $(size(image)-1)^2$. Table 5 shows the visual strength evaluations for the proposed structure in Fig. 5.

F. PIXEL ERROR ANALYSES

Pixel error assessment analyses evaluate the divergence of encrypted content from plain content. To measure the error in digital content, we calculate the normalized absolute error (NAE), mean absolute error (MAE), mean square error (MSE), root mean square error (RMSE), signal-to-noise ratio (SNR), and peak signal-to-noise ratio (PSNR) [45]. The correctness of interminable variables and the divergence in encrypted content concerning plain text are evaluated using NAE and MAE. The eminence of the encrypted content is computed here by using MSE and SNR, and RMSE and PSNR. The lower the MSE and RMSE esteem in relation to SNR and PSNR, the more the similarity between the data.

TABLE 5. Visual strength analyses of grayscale images and assessments with the most recent methodology.

Image			Plain	Encrypted	Ref. [39]
Airplane	Contrast Group	Contrast	0.2765077	11.1262	10.6103
		Dissimilarity	7.686961	86.081001	
		Homogeneity	0.70237	0.9876	0.9856
	Orderliness Group	Angular Second Moment	0.001609	0.000024	-
		Maximum Probability	0.010267	0.000483	-
		Energy	0.040117	0.004867	0.0156
	Statistics Group	Mean	175.371255	129.137701	-
		Variance	2145.953829	5571.918693	-
		Correlation	0.935632	0.001580	-
Baboon	Contrast Group	Contrast	1.016526342	11.12501	10.5001
		Dissimilarity	21.625649	86.139410	-
		Homogeneity	0.076238	0.9875	0.9890
	Orderliness Group	Angular Second Moment	0.000104	0.000024	-
		Maximum Probability	0.000586	0.000502	
		Energy	0.010191	0.004872	0.0155
	Statistics Group	Mean	123.107083	129.036805	-
		Variance	1829.899177	5560.091059	-
		Correlation	0.722246	0.000434	-
Pepper	Contrast Group	Contrast	0.181210090	11.1370	10.6103
		Dissimilarity	6.441313	86.140372	-
		Homogeneity	0.76079	0.9873	0.9856
	Orderliness Group	Angular Second Moment	0.000344	0.000024	-
		Maximum Probability	0.001769	0.000609	-
		Energy	0.018540	0.004903	0.0156
	Statistics Group	Mean	121.411177	129.233543	-
		Variance	2877.471037	5578.651137	-
		Correlation	0.968514	0.001813	-

The following parameters are used to analyze the evaluations of these investigations.

$$NAE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{\left|P_{i,j} - C_{i,j}\right|}{\sum\limits_{i=0}^{M-1}\sum\limits_{j=0}^{N-1}\left|P_{i,j}\right|}, \tag{19}$$

$$MAE = \frac{1}{M \times N}\sum_{k=0}^{M-1}\sum_{l=0}^{N-1}\left|P_{k,l} - C_{k,l}\right|, \tag{20}$$

$$MSE = \frac{\sum\limits_{k=1}^{M}\sum\limits_{l=1}^{N}(P_{k\,l} - C_{k\,l})^2}{M \times N}, \tag{21}$$

$$RMSE = \sqrt{\frac{\sum\limits_{k=1}^{M}\sum\limits_{l=1}^{N}(P_{k\,l} - C_{k\,l})^2}{M \times N}}, \tag{22}$$

$$\text{SNR} = 20\log_{10}\left[\frac{I_{MAX}}{MSE}\right], \tag{23}$$

$$\text{PSNR} = 20\log_{10}\left[\frac{I_{MAX}}{RMSE}\right], \tag{24}$$

where $P_{k,l}$ and $C_{k,l}$ are the pixel positions for the plain and encrypted information in the k^{th} row and l^{th} column, respectively, and I_{MAX} is an estimate of the digital content's maximum possible pixel. A higher MSE esteem and a more consistent PSNR can increase the quality of digital content encryption, or vice versa [46]. Table 6 depicts the analysis of standard digital content for the attainability of the anticipated structure.

V. DIGITAL FORENSIC ANALYSES

To determine what happened to the digital content, we performed a systematic data evaluation while keeping an archived sequence of evidence. To sustain the resistivity of

TABLE 6. Pixel divergence investigations for the originally encrypted digital content and a comparison with the most recent methodology.

Image	Pixel divergence analyses						Ref. [47]		Ref. [48]
	NAE	MAE	MSE	RMSE	SNR (dB)	PSNR (dB)	MAE	MSE	PSNR
Airplane	0.463957	83.15	10352.4	101.74705	-16.085	7.9804	79.95	8553.77	8.9998
Baboon	0.58707	71.68	7406.30	86.05985	-14.638	9.4688	83.56	8219.66	8.5412
Pepper	0.63064	75.87	8507.19	92.23445	-15.287	8.8669	81.45	8392.82	8.7723
Lena	0.59260	73.51	7875.38	88.74332	-14.897	9.2021	79.84	7715.76	9.4314

TABLE 7. Error assessment analysis by introducing Gaussian noise in the transmitted content.

Image	Error and noise analysis		Noise intensity							
			0.000001		0.000003		0.000005		0.000007	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Airplane	10352.4	7.9804	10124.7	7.9836	9956.1	7.9921	9795.8	8.0251	9612.6	8.0612
Baboon	7406.30	9.4688	7269.18	9.4814	7136.77	9.5011	6992.71	9.5372	6843.42	9.5701
Pepper	8507.19	8.8669	8341.54	8.8803	8191.35	8.8998	8016.84	8.9285	7898.13	8.9516
Lena	7875.38	9.2021	7713.75	9.2256	7609.48	9.2558	7468.32	9.2798	7304.53	9.3104

the foreseen structures, we performed linear, key sensitivity, noise, and differential assault analyses as follows.

A. LINEAR ATTACK ANALYSIS

The key employed by the cryptanalyst conducts a linear assault to identify the logic used in encryption and decryption to perceive immediate information for the association between particular bits of plain and encrypted data [49]. The analyst will attempt to decode the information using all available keys to find the similarities in the ciphers. The anticipated methodology has no information about the arbitrary sequence created by the virtual oscillator or the random walk to induce diffusion in the plain data. Moreover, the analyst will concentrate on factual assessments by varying the parameters, but the received outcomes have no association with any previous consequences.

B. KEY SENSITIVITY ANALYSIS

The sensitivity of the key is determined by how much of key-space is available to withstand a brute force attack [50]. The total number of keys needed to encrypt or decrypt the algorithm is specified. We analyzed brute force, computational, and ciphertext attacks on the proposed algorithm.

Brute force analysis: We evaluated the simplest example in Section II-A by choosing Alice's first secret of four bits and the second secret of five bits with three-bit random values. Let us assume Alice has 32 bits for each secret, with 16-bit random values. The effective key-space to resist a brute force attack will be $32^{16} \times 32^{16} = 2^{80} \times 2^{80} = 2^{160}$. Similarly, if we just improve the selection of the random value from 16 bits to 32 bits, the key-space will be 2^{320}.

Computational analysis: The fastest existing machine can perform 2^{80} computations in just one second [51]. The total number of computations in a year will be $2^{80} \times 365(\text{days}) \times 24(\text{hours}) \times 60(\text{minutes}) \times 60(\text{seconds}) \approx 2^{105}$. A computational attack requires 2^{55} years $\left(\frac{2^{160}}{2^{105}} = 2^{55}\right)$ to compute 32-bit secrets with 16-bit random values.

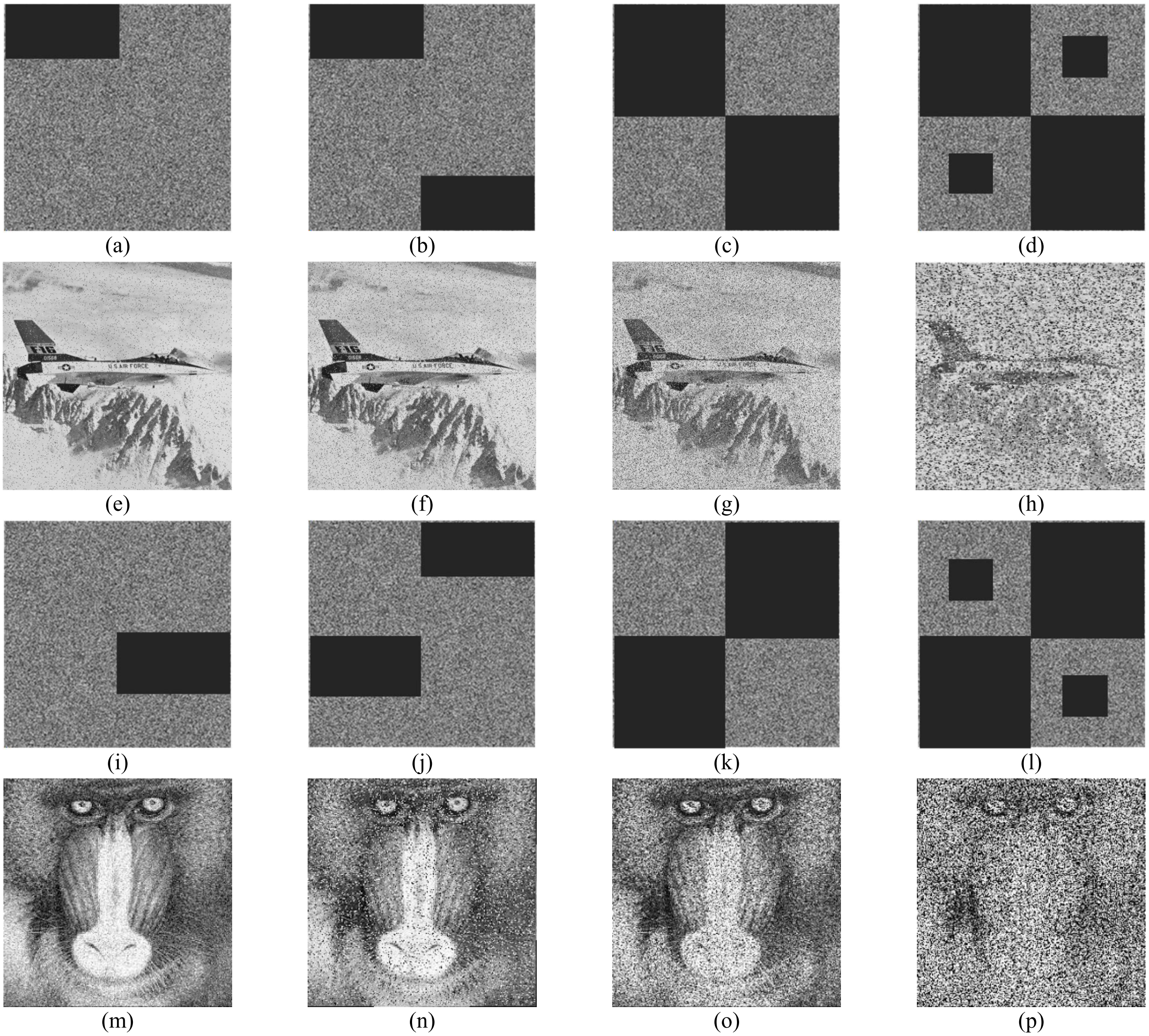
Ciphertext analysis: To analyze ciphertext attacks, an analyst requires the key matrix to bitwise XOR the cipher image [52]. For an eight-bit image having dimensions of 64 × 64, the analyst requires $(64 \times 64)!$ combinations of eight-bit values to decode the image. To crack the cipher images in Section III-B of this article, analysts need to compute $(512 \times 512)!$ combinations of eight-bit values, which is much harder than cracking the key with a brute force attack.

C. NOISE AND OCCLUSION ATTACK ANALYSIS

During transmission or reception, it is possible that the information may be affected by noises and can be tempered over the insecure channel. A cryptosystem should be capable to resist the attacks and recover the data up to a certain level even after tempering in data [53], [54]. To validate the robustness of the algorithm, we estimated the MSE and PSNR by introducing Gaussian noise and occlusion to transmitted content. The Gaussian noise analysis, having normalized power 0.000001, 0.000003, 0.000005, and 0.000007, for the gray level transmitted image is depicted in Table 7, and the occlusion analysis for the encrypted images occluded by 1/8, 1/4, and 1/2, 3/5 are given in Fig. 12 and Table 8.

By varying the noise strength from 0.000001 to 0.000007, there seems to be a minute variation in the noise ratio and the error estimation, which proves the robust efficiency of the proposed structure against noise assaults.

The effects of MSE and PSNR after introducing occlusion attack to encrypted images in Table 8 and the decrypted images in Fig. 12 are indicating that the proposed algorithm can withstand up to 50% occlusion attack. Hence, the proposed method provides better security against noise and resists the occlusion attack.


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

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

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

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

FIGURE 12. Occlusion analysis for the encrypted content of Airplane and Baboon images: (a-d) Encrypted Airplane image at grayscale with 1/8 occlusion in the top-left corner, 1/4 occlusion in the top-left and end-right corners, 1/2 occlusion in the diagonal, and 3/5 occlusion in the diagonal, mid of top-right and end-left corners, (e-h) Corresponding recovered Airplane images; (i-l) Encrypted Baboon image at grayscale with 1/8 occlusion in the third quarter of right position, 1/4 occlusion in the top-right corner and third quarter of right position, 1/2 occlusion in the top-right and end-left corners, and 3/5 occlusion in the top-right, end-left, mid of top-left and end-right corners, (m-p) Corresponding recovered Baboon images.

TABLE 8. Occlusion attack analysis on the encrypted content.

Image	Encrypted image		Occlusion to encrypted image							
			1/8		1/4		1/2		3/5	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Airplane	10352.4	7.9804	6544.11	11.4483	4129.73	13.962	2856.50	15.1224	1808.58	17.9157
Baboon	7406.30	9.4688	5783.09	11.1241	3866.27	13.391	2588.43	15.543	1479.26	17.3846
Pepper	8507.19	8.8669	6208.81	11.6152	4017.90	13.5941	2645.01	15.4126	1410.98	17.2207
Lena	7875.38	9.2021	5799.14	11.2275	3906.77	13.2035	2422.16	15.725	1278.05	18.0109

D. DIFFERENTIAL ATTACK ANALYSIS

Differential attack analyses validated the developed algorithm's quality based on the deviation of a single pixel within the relevant content by altering the encoded content with a likelihood of half-pixel modification [55], [56]. The variation within the k^{th} chunk of the transmuted content affects the corresponding encoded content's k^{th} chunk. The number of pixels change rate (NPCR) is bonded together to determine

TABLE 9. NPCR analysis of encrypted content, and a comparison with the most recent strategy.

Image	NPCR outcome				Ref. [25]			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Airplane	99.784	99.612	99.871	99.881	99.88	99.79	99.81	99.87
Baboon	99. 912	99.821	99.734	99.854	99.89	99.87	99.77	99.74
Pepper	99.861	99.833	99.855	99.689	99.86	99.78	99.84	99.76
Lena	99.863	99.862	99.806	99.827	99.85	99.84	99.81	99.79

TABLE 10. UACI analysis for encrypted content, and a comparison with the most recent strategy.

Image	UACI outcome				Ref. [60]			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Airplane	33.443	32.921	33.181	33.511	33.25	30.25	31.38	31.37
Baboon	33.460	33.531	33.229	33.119	-	29.93	28.63	31.38
Pepper	33.362	33.114	32.894	33.264	-	29.03	34.00	33.90
Lena	33.422	33.412	32.922	33.315	-	28.02	29.44	29.27

the unified average change intensity (UACI) to approximate the negligible effect within the modified content compared to encrypted information [57], [58]. To evaluate NPCR and UACI estimations, let us consider two pieces of encrypted content in which one is altered by a solo pixel.

$$\mathrm{NPCR} = \sum\nolimits_{k,l} \frac{E(k,l)}{X \times Y} \times 100\% \, , \tag{25}$$

where $E(k,l) = \begin{cases} 0, & T_1(k,l) = T_2(k,l) \\ 1, & T_1(k,l) \neq T_2(k,l) \end{cases}.$

$$UACI = \sum_{k=0}^{X-1} \sum_{l=0}^{Y-1} \frac{\left| T_1(k,l) - T_2(k,l) \big/ 255 \right|}{X \times Y} \times 100\% \, , \tag{26}$$

where $T_1(k,l)$ and $T_2(k,l)$ are the encrypted images, X and Y are the height and width, and E is a two-dimensional set similar to the encrypted image dimensions [59]. Evaluation of NPCR and UACI for the encoded content and a comparison with the most recent strategy are illustrated in Tables 9 and 10.

The outcome in Table 9 is legitimately near a seamless estimation of 1, which indicates that the foreseen structure has better results over the existing approach to opposing attacks, whereas the UACI results in Table 10 show that the proposed strategy's outcome prevails over the existing approach and is, to an incredible degree, sensitive to miniature modifications within normal content, even if the two pieces of encrypted content have a one-bit modification.

VI. CONCLUSION AND PROJECTIONS

In the next-generation frameworks, when adversaries will be fully equipped with AI technologies, it is predicted that most public-key image encryption schemes will be susceptible to various threats. The proposed discrete logarithmic factorial problem based public-key establishment scheme provides a secure way to generate common keys on which an adversary cannot bypass the protocol even with one of the secrets from key pairs is known. The virtual oscillator generated by microstates of initial oscillators for the common secrets, on the proposed public-key scheme, produces unique states to generate diffusion in the plain data followed by a random walk, comparable to quantum chaos, on inimitable points. The performance and digital forensic assessments certified the superior resistivity of the proposed method in comparison to existing schemes to hostile attacks. The developed structure in this article can be extended to applications of already developed models, such as secure transfer of satellite and drone imageries, low-profile mobile applications, audio-video encryptions, etc., and we strongly believe that there is room for further improvements to envisioned structures with even better cryptographic properties.

ACKNOWLEDGMENT

The authors are grateful to members of the Cyber and Information Security Laboratory, Institute of Space Technology, for their contribution to this work, and to the anonymous reviewers for their valuable feedback.

REFERENCES

[1] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Trans. Cybern.*, vol. 46, no. 5, pp. 1132–1143, May 2015.

[2] Y. Lindell, "How to simulate it—A tutorial on the simulation proof technique," in *Tutorials on the Foundations of Cryptography* (Information Security and Cryptography). Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-57048-8_6.

[3] B. Vaseghi, S. S. Hashemi, S. Mobayen, and A. Fekih, "Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems," *IEEE Access*, vol. 9, pp. 21332–21344, 2021.

[4] M. Devipriya and M. Brindha, "Image encryption using modified perfect shuffle-based bit level permutation and learning with errors based diffusion for IoT devices," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107954.

[5] W. El-Shafai, F. Khallaf, E.-S.-M. El-Rabaie, and F. E. A. El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 10, pp. 9007–9035, Oct. 2021.

[6] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," *Entropy*, vol. 22, no. 2, p. 175, Feb. 2020.

[7] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2556–2569, 2020.

[8] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019.

[9] X. Zhang, Y. Ren, L. Shen, Z. Qian, and G. Feng, "Compressing encrypted images with auxiliary information," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1327–1336, Aug. 2014.

[10] Y. He, Y.-Q. Zhang, X. He, and X.-Y. Wang, "A new image encryption algorithm based on the OF-LSTMS and chaotic sequences," *Sci. Rep.*, vol. 11, no. 1, pp. 1–22, Dec. 2021.

[11] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Opt. Lasers Eng.*, vol. 80, pp. 1–11, May 2016.

[12] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19853–19873, Jul. 2020.

[13] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.

[14] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," *Inf. Sci.*, vol. 593, pp. 121–154, May 2022.

[15] L. Y. Zhang, Y. Liu, F. Pareschi, Y. Zhang, K.-W. Wong, R. Rovatti, and G. Setti, "On the security of a class of diffusion mechanisms for image encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1163–1175, Apr. 2018.

[16] M. F. Khan, A. Ahmed, K. Saleem, and T. Shah, "A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system," *IEEE Access*, vol. 7, pp. 84980–84991, 2019.

[17] M. Mumtaz and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 1, pp. 9–29, Jan. 2019.

[18] S. K. Tripathi, B. Gupta, and K. K. S. Pandian, "An alternative practical public-key cryptosystems based on the dependent RSA discrete logarithm problems," *Expert Syst. Appl.*, vol. 164, Feb. 2021, Art. no. 114047.

[19] J. Liu, Y. Yu, B. Yang, J. Jia, and Q. Lai, "Cryptanalysis of cramer-shoup like cryptosystems based on index exchangeable family," *Int. J. Found. Comput. Sci.*, vol. 32, no. 1, pp. 73–91, Jan. 2021.

[20] P. Lafourcade, L. Robert, and D. Sow, "Fast cramer-shoup cryptosystem," in *Proc. 18th Int. Conf. Secur. Cryptography*, 2021.

[21] A. A. Tsirlin and H. Rosner, "Ab initio modeling of Bose-Einstein condensation in $Pb_2V_3O_9$," *Phys. Rev. B, Condens. Matter*, vol. 83, no. 6, Feb. 2011, Art. no. 064415.

[22] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*. Cambridge, U.K.: Cambridge Univ. Press, 2018.

[23] S. I. Batool, M. Amin, and H. M. Waseem, "Public key digital contents confidentiality scheme based on quantum spin and finite state automation," *Phys. A, Stat. Mech. Appl.*, vol. 537, Jan. 2020, Art. no. 122677.

[24] C.-S. Wong, J. Goree, and Z. Haralson, "Einstein frequency measurement for a strongly coupled dusty plasma," *IEEE Trans. Plasma Sci.*, vol. 46, no. 4, pp. 763–767, Apr. 2018.

[25] 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. 11, pp. 1–20, May 2020.

[26] H. Emmerich, H. Löwen, R. Wittkowski, T. Gruhn, G. I. Tóth, G. Tegze, and L. Gránásy, "Phase-field-crystal models for condensed matter dynamics on atomic length and diffusive time scales: An overview," *Adv. Phys.*, vol. 61, no. 6, pp. 665–743, Dec. 2012.

[27] N. Y. Yao, A. C. Potter, I.-D. Potirniche, and A. Vishwanath, "Discrete time crystals: Rigidity, criticality, and realizations," *Phys. Rev. Lett.*, vol. 118, no. 3, Jan. 2017, Art. no. 030401.

[28] I. M. Sobol, *A Primer for the Monte Carlo Method*. Boca Raton, FL, USA: CRC Press, 2018.

[29] A. G. Weber. (2006). *The USC-SIPI Image Database: Version 5*. [Online]. Available: http://sipi.usc.edu/database/

[30] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS ONE*, vol. 13, no. 11, Nov. 2018, Art. no. e0206460.

[31] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps," *IEEE Access*, vol. 9, pp. 52277–52291, 2021.

[32] N. Iqbal, M. Hanif, S. Abbas, M. A. Khan, S. H. Almotiri, and M. A. Al Ghamdi, "DNA strands level scrambling based color image encryption scheme," *IEEE Access*, vol. 8, pp. 178167–178182, 2020.

[33] A. Alghafis, H. M. Waseem, M. Khan, and S. S. Jamal, "A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states," *Phys. A, Stat. Mech. Appl.*, vol. 554, Sep. 2020, Art. no. 123908.

[34] Y. Sha, Y. Cao, H. Yan, X. Gao, and J. Mou, "An image encryption scheme based on IAVL permutation scheme and DNA operations," *IEEE Access*, vol. 9, pp. 96321–96336, 2021.

[35] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Sci. Rep.*, vol. 10, no. 1, pp. 1–15, Dec. 2020.

[36] M. F. Khan, K. Saleem, M. A. Alshara, and S. Bashir, "Multilevel information fusion for cryptographic substitution box construction based on inevitable random noise in medical imaging," *Sci. Rep.*, vol. 11, no. 1, pp. 1–23, Dec. 2021.

[37] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, pp. 1–16, Dec. 2020.

[38] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

[39] H. M. Waseem and M. Khan, "A new approach to digital content privacy using quantum spin and finite-state machine," *Appl. Phys. B, Lasers Opt.*, vol. 125, no. 2, p. 27, Feb. 2019.

[40] A. Toktas, U. Erkan, F. Toktas, and Z. Yetgin, "Chaotic map optimization for image encryption using triple objective differential evolution algorithm," *IEEE Access*, vol. 9, pp. 127814–127832, 2021.

[41] T. Shah, T. U. Haq, and G. Farooq, "Improved SERPENT algorithm: Design to RGB image encryption implementation," *IEEE Access*, vol. 8, pp. 52609–52621, 2020.

[42] X. Wang and P. Liu, "A new image encryption scheme based on a novel one-dimensional chaotic system," *IEEE Access*, vol. 8, pp. 174463–174479, 2020.

[43] S. Sun and Y. Guo, "A new hyperchaotic image encryption algorithm based on stochastic signals," *IEEE Access*, vol. 9, pp. 144035–144045, 2021.

[44] 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.

[45] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.

[46] A. H. Ismail, H. M. Waseem, M. Ishtiaq, S. S. Jamal, and M. Khan, "Quantum spin half algebra and generalized megrelishvili protocol for confidentiality of digital images," *Int. J. Theor. Phys.*, vol. 60, no. 5, pp. 1720–1741, May 2021.

[47] S. I. Batool and H. M. Waseem, "A novel image encryption scheme based on Arnold scrambling and Lucas series," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27611–27637, Oct. 2019.

[48] A. G. Mohamed, N. O. Korany, and S. E. El-Khamy, "New DNA coded fuzzy based (DNAFZ) S-boxes: Application to robust image encryption using hyper chaotic maps," *IEEE Access*, vol. 9, pp. 14284–14305, 2021.

[49] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *J. Supercomput.*, vol. 75, no. 10, pp. 6663–6682, Oct. 2019.

[50] W. K. Lee, C. W. Phan, W. S. Yap, and B. M. Goi, "Spring: A novel parallel chaos-based image encryption scheme," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 575–593, Apr. 2018.

[51] M. Brindha and N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem," *Appl. Soft Comput.*, vol. 40, pp. 379–390, Mar. 2016.

[52] J. Chen, L. Chen, and Y. Zhou, "Universal chosen-ciphertext attack for a family of image encryption schemes," *IEEE Trans. Multimedia*, vol. 23, pp. 2372–2385, 2021.

[53] S. Wang, Q. Peng, and B. Du, "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," *Opt. Laser Technol.*, vol. 148, Apr. 2022, Art. no. 107753.

[54] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," *IEEE Access*, vol. 9, pp. 76191–76204, 2021.

[55] H. M. Waseem, S. S. Jamal, I. Hussain, and M. Khan, "A novel hybrid secure confidentiality mechanism for medical environment based on Kramer's spin principle," *Int. J. Theor. Phys.*, vol. 60, no. 1, pp. 314–330, Jan. 2021.

[56] J. Hao, H. Li, H. Yan, and J. Mou, "A new fractional chaotic system and its application in image encryption with DNA mutation," *IEEE Access*, vol. 9, pp. 52364–52377, 2021.

[57] M. Khan and H. M. Waseem, "A novel digital contents privacy scheme based on Kramer's arbitrary spin," *Int. J. Theor. Phys.*, vol. 58, no. 8, pp. 2720–2743, 2019.

[58] J. He, S. Huang, S. Tang, and J. Huang, "JPEG image encryption with improved format compatibility and file size preservation," *IEEE Trans. Multimedia*, vol. 20, no. 10, pp. 2645–2658, Oct. 2018.

[59] H. M. Waseem, M. Khan, and T. Shah, "Image privacy scheme using quantum spinning and rotation," *J. Electron. Imag.*, vol. 27, no. 6, Dec. 2018, Art. no. 063022.

[60] U. Arshad, S. I. Batool, and M. Amin, "A novel image encryption scheme based on Walsh compressed quantum spinning chaotic Lorenz system," *Int. J. Theor. Phys.*, vol. 58, no. 10, pp. 3565–3588, Oct. 2019.

MUHAMMAD WASEEM HAFIZ (Graduate Student Member, IEEE) received the B.S. degree in electronics engineering from the COMSATS Institute of Information Technology, in 2014, and the M.S. degree in electrical engineering from the Institute of Space Technology (IST), Pakistan, in 2018. He is currently pursuing the Ph.D. degree with Gachon University, South Korea. He worked as an Assistant Manager in the telecommunications industry, from 2014 to 2018. He also worked as a Research Associate with the IST, from 2018 to 2020. He is also affiliated with the Department of IT Convergence Engineering, Gachon University. His research interests include cryptography, quantum information theory, artificial intelligence, and cybersecurity.

WAI-KONG LEE (Member, IEEE) received the B.Eng. and M.Eng.Sc. degrees in electronics from Multimedia University, in 2006 and 2009, respectively, and the Ph.D. degree in engineering from the University Tunku Abdul Rahman (UTAR), Malaysia, in 2018. From 2009 to 2012, he worked as a Research and Development Engineer for several multinational companies, including Agilent Technologies (now known as Keysight), Malaysia. He worked as an Assistant Professor and the Deputy Dean (research and development) of the Faculty of Information and Communication Technology, UTAR. He was a Visiting Scholar at Carleton University, Canada, in 2017; Feng Chia University, Taiwan, in 2016 and 2018; and OTH Regensburg, Germany, in 2015, 2018, and 2019. He is currently a Postdoctoral Researcher at Gachon University, South Korea. His research interests include cryptography, GPU computing, numerical algorithms, the Internet of Things (IoT), and energy harvesting. He served as a Reviewer for several international journals, such as the IEEE Transactions on Dependable and Secure Computing, in 2016 and 2017, IEEE Sensors Journal, IEEE Internet of Things Journal, from 2018 to 2021, and IEEE Transactions on Industrial Informatics, from 2018 to 2021.

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 the Pohang University of Science and Technology, in 1998, and the Ph.D. degree in computer science from the Korea Advanced Institute of Science and Technology, South Korea. He worked as a Software Engineer with LGCNS Systems Inc., from 1994 to 1996. He also worked as a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI), from 1998 to 2007. He worked as a Professor with 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*.

MAJID KHAN received the M.S. and Ph.D. degrees in mathematics from Quaid-e-Azam University, Islamabad, in 2008 and 2015, respectively. He is currently an Associate Professor with the Department of Applied Mathematics and Statistics, Institute of Space and Technology, Islamabad, Pakistan. His area of specialization is cryptography. He is also working in chaotic cryptography, quantum cryptography, and artificial intelligence-based encryption mechanisms.

ASIM LATIF received the bachelor's degree in mathematics from the University of Azad Jammu & Kashmir, in 2018, and the master's degree in mathematics from the Institute of Space Technology, Pakistan, in 2020. He is currently affiliated as a Lecturer with the Department of Software Engineering, Foundation University Rawalpindi (FURC), Pakistan. His research interests include cryptography, artificial intelligence, and mathematics behind hollow-chain and block-chain technologies.