IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Innovative Cybersecurity for Enhanced Data Protection: An Extended Bit-Plane Extraction and Chaotic Permutation-Diffusion Approach in Information Security

MUJEEB UR REHMAN[1], ARSLAN SHAFIQUE [2], KASHIF HESHAM KHAN[3], MALAK OLAMAIE [4]SAAD NASSER ALTAMIMI [5],SULTAN NOUMAN QASEM[5], MOHAMMED AL-SAREM[6]

[1]Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, UK (email: mujeeb.rehman@dmu.ac.uk)
[2]School of Biomedical Engineering, University of Glasgow, UK (e-mail: arslan.shafique@glasgow.ac.uk)
[3]School of Computing Technologies, STEM College, RMIT University (e-mail: KashifHesham.khan@rmit.edu.au)
[4]School of Science, Technology and Health, York St. John University, York, UK(e-mail: m.olamai@yorksj.ac.uk)
[5]College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia (e-mail: snaltamimi@imamu.edu.sa, SNMohammed@imamu.edu.sa)
[6]College of Computer and Engineering, Taibah University, Medina 41477, Saudi Arabia (e-mail:msarem@taibahu.edu.sa)

Corresponding author: Mujeeb Ur Rehman (e-mail: mujeeb.rehman@dmu.ac.uk)

ABSTRACT

In the era of big data, protecting digital images from cyberattacks during network transmission is of utmost importance. While various image encryption algorithms have been developed, some remain vulnerable to specific cyber threats. This paper presents an enhanced version of the image encryption algorithm based on bit-plane extraction (BPCPD) to address its vulnerability to chosen-plaintext attacks. The proposed cryptographic system encompasses three primary phases. The initial phase involves bit-plane extraction from the plaintext image and the generation of random sequences and a random image using multiple chaotic maps, such as the chaotic Arnold map and the chaotic CAT map. The second phase is dedicated to permutation operations, which comprise three sub-phases: multi-layer permutation, multi-round permutation, and recursive permutation. In the third phase, diffusion is introduced to the permuted image through pixel substitution, coupled with XOR operations performed on the respective bit-planes of the random image. To gauge the efficiency of the proposed encryption scheme, a range of experimental analyses are conducted, including histogram analysis, contrast assessment, entropy measurement, correlation analysis, encryption quality assessment, and investigations into noise attacks and occlusion attacks. The results of these experimental analyses, in comparison to an existing encryption scheme, demonstrate that the proposed framework surpasses both BPCPD and other existing encryption schemes in various aspects of performance.

INDEX TERMS Chaos, noise resistance, chaotic logistic map, DWT, security

I. INTRODUCTION

In the current landscape of big data and information technology, securing digital images from cyberattacks during network transmission has emerged as an important concern [1]. While numerous image encryption algorithms have been devised in recent decades, some persistently exhibit vulnerabilities to specific cyberattacks [2]–[4]. This research paper addresses this critical issue by presenting an advanced version of an image encryption algorithm, extending the Bit-Plane Extraction and Chaotic Permutation-Diffusion (BPCPD) [5] approach to fortify its resistance to chosen-plaintext attacks. The proposed cryptographic system is a multifaceted construct, characterized by three pivotal phases. The initial phase entails the extraction of bit-planes from the plaintext image, accompanied by the generation of random sequences and a random image via the utilization of multiple chaotic maps, such as the hyperchaotic map and the chaotic CAT map. The second phase is dedicated to a sequence

of permutation operations, encompassing three sub-phases: multi-layer permutation, multi-round permutation, and recursive permutation. In the third and final phase, diffusion is introduced to the permuted image through pixel substitution, coupled with XOR operations performed on the respective bit-planes of the random image. To evaluate the efficiency and robustness of the proposed encryption scheme, a comprehensive array of experimental analyses is undertaken, including histogram analysis, contrast assessment, entropy measurement, correlation analysis, and encryption quality assessment, as well as examinations of noise attacks and occlusion attacks. The outcomes of these experimental investigations, in comparison to an existing encryption scheme, affirm that the proposed framework excels in numerous facets of performance, surpassing both the BPCPD scheme and other established encryption methodologies. This research not only enhances image security but also contributes significantly to the broader domain of information security in the era of big data and networked communication.

The age of big data has brought about a significant transformation in the way we generate, share, and manage digital content. As multimedia technology rapidly evolves, the production and dissemination of digital content, including videos, audio files, and images, have experienced an unprecedented surge [6]. This surge is a testament to technological advancement and the evolving digital lifestyles of individuals and organizations alike. Notably, cloud-based storage solutions have gained widespread acceptance as a means of convenient and remote access to valuable image repositories. However, this convenience comes with a double-edged sword. In this digital realm, security challenges loom large, and without robust safeguards in place, confidential and private data embedded within images become susceptible to unauthorized access, data breaches, and privacy violations [7], [8]. The need for effective image protection mechanisms is more pronounced than ever. These mechanisms are entrusted with the crucial responsibility of preserving the confidentiality and integrity of images, ensuring that they remain shielded from prying eyes and malicious actors. As we navigate this digital landscape brimming with opportunities and vulnerabilities, the importance of technological innovation in securing our digital assets is underscored. Innovative solutions in information security have become indispensable in paving the way for a secure and resilient digital future.

Cryptographic systems have emerged as a valuable technology in the protection of digital images [9], [10]. These systems serve the fundamental purpose of transforming a meaningful image into a state of chaos, rendering it impervious to malicious extraction of plaintext information. In recent years, chaotic-based methods have garnered increasing interest in the field of image encryption [11]. A multitude of researchers has presented diverse schemes that harness the power of chaos to develop robust cryptosystems. One commonly employed method in this context is the chaotic Arnold map, which, when combined with XOR operations, has been demonstrated to produce chaotic images. Additionally, researchers have fused the hyperchaotic map with stochastic techniques to create a secure encryption approach that overcomes image size restrictions [12], [13]. Beyond the Arnold transform, various alternative techniques have been introduced, ranging from dividing pixel groups into subgroups to employing wavelet encryption methods, and even simultaneously encrypting multiple images using chaotic systems. While these methods have exhibited substantial promise, they often entail significant computational complexity, rendering them unsuitable for real-time applications, a critical requirement in the context of big data and networked communication.

A. MOTIVATION

The motivations behind this research are rooted in the recognized limitations and security vulnerabilities of existing image encryption schemes such as BPCPD. These limitations have spurred the development of an improved approach to image protection. The study's contributions and motivations can be summarized as follows: Firstly, a key distinctiveness algorithm is introduced to prevent the occurrence of equivalent keys, enhancing the overall security of the system. The need for unique and non-duplicable keys is a primary driving force. Secondly, the research introduces a nonlinear transformation within the diffusion operation, increasing the complexity of the encryption scheme. This enhancement involves substituting image pixels and integrating the bit-level diffusion technique with the XOR operation, fortifying the security framework. Thirdly, the proposed encryption technique incorporates innovative permutation methods, including multi-layer, multi-round, and recursive permutation techniques. These aim to address the limitations of conventional permutation approaches, providing heightened security and diversity. Lastly, the proposed study successfully reinforces the traditional confusion-diffusion framework by incorporating complex permutation and diffusion processes, resulting in a substantial boost to both security and efficiency. These motivations collectively guide the development of an advanced image protection mechanism, offering enhanced security and efficiency in response to the identified limitations and security challenges in existing encryption methods.

II. RELATED WORK

Cryptographic systems stand as a valuable technology for protecting digital images [14]. This process transforms a meaningful image into a state of chaos. Due to malicious individuals being unable to extract plaintext information from an enciphered image, the goal of image protection is achieved. In recent years, chaotic-based methods have shown an increasing interest in image encryption [15]–[17], and several researchers have presented diverse schemes to create cryptosystems. One commonly employed method is the chaotic Arnold map [18]. For instance, Zhu et al. [19] utilized the Arnold map in combination with XOR operations [20] to produce chaotic images. Tang et al. [21] fused the Arnold map with stochastic techniques, introducing a secure

encryption approach that circumvents image size restrictions. Apart from the application of the Arnold transform, numerous alternative techniques have been introduced in the past few decades. For example, Tang et al. [22] divided the eight-bit pixel group into two subgroups, specifically even and odd, generating a randomized image by swapping these subgroups. Martin et al. [23] utilized the wavelet encryption method [24] to encrypt grayscale images at the pixel level. Lin et al. [25] employed chaos for the simultaneous encryption of multiple images. Meanwhile, Liu and Wang [26] put forward a method for encrypting three-dimensional (3-D) color images through the utilization of tent map [27], logistic map [28], and sine map [29]. Wang et al. [30] introduced a cryptosystem based on the perceptron model [31] and the Lorenz chaotic system [32]. Wang et al. [33] deployed chaotic systems to encrypt the color components simultaneously, aiming to decrease computational complexity. Zhang et al. [34] utilized a 1-D chaotic map to generate a randomized image to alter the pixel values, thus ensuring digital image security. In [35], Yin et al. presented a new model to secure the privacy of text data. By combining attribute-based encryption and searchable encryption, this model provides a robust solution for secure and privacy-preserving information retrieval in a multiparty setting. In [36], Liu et al. introduced a novel approach for image encryption, leveraging the synergies between chaotic systems and artificial fish swarm intelligence. The integration of evolutionary intelligence enhances the encryption process, contributing to heightened security in image communication and storage. In [37], Shi et al. proposed a model for precise medical image segmentation. By combining the power of convolutional neural networks and fuzzy active contours, this model demonstrates advanced capabilities in accurately delineating structures within medical images. Liu et al. [38] adopted a linear chaotic map [39] for bit-level pixel permutation. Wang et al. [40] combined linear blending procedures with random phase encoding, resulting in the transformation of multiple images into a singular composite. The encryption algorithm proposed by Wang et al. [41] can simultaneously encrypt multiple images, relying on both chaos and frequency domain encryption techniques [42], [43]. Ping et al. [44] introduced an encryption scheme based on cellular automata (CA) [45]. In [46], Setiadi et al. presented an image encryption scheme, integrating different encryption techniques based on multiple chaotic logistic map methods. The encryption involves six stages to encrypt the digital images. In [47], Winarno et al. proposed a study introducing a combination of Zigzag, Hilbert, and Morton patterns for enhancing digital image security. The keystream, generated from improved logistic and 6D hyperchaotic maps, contributes highly random and nonlinear keystreams. In [48], Winarno et al. introduced an enhanced image encryption technique focusing on 3D confusion and diffusion patterns. The method combines multiple chaotic maps, and a hash function across four phases to achieve maximum confusion and diffusion performance. Wang et al. [49] employed cycle shift operations in conjunction with chaotic maps to formulate a novel cryptosystem. Enayatifar et al. [50] simultaneously incorporated the Tinkerbell chaotic map [51], CA, and DNA to develop a secure framework for encrypting digital images. Tang et al. [52] utilized chaotic systems and block scrambling operations securing digital images. In [53], Wang et al. employed a bit-planes encryption approach to introduce an encryption framework aimed at securing digital data. Alongside bit-plane extraction, they also leveraged chaotic maps for high security. They sequentially employed two well-established encryption methods: diffusion and confusion. Although the authors successfully achieved a commendable level of security in their proposed encryption scheme through the use of multiple encryption methods, the sequential execution of all these encryption steps resulted in longer processing times, rendering it unsuitable for real-time applications. In [54], Sun et al. proposed a chaos-based encryption framework incorporating bit-plane extraction methodology. The plaintext image initially underwent the extraction of eight bit-planes, forming a new three-dimensional (3-D) matrix with dimensions of 256×256. Subsequently, this 3-D matrix underwent various rotations controlled by random sequences generated using chaotic maps. Additionally, the seed values for these chaotic maps are generated using the MD5 hash algorithm. Through experimentation, the authors demonstrated that their encryption framework could withstand brute force attacks due to its large key size, exceeding 2^{150}. In [55], Waseso et al. utilized the innovative machine learning methodology for phishing detection to protect the digital data, which incorporates K-Nearest Neighbour and Naïve Bayes, to effectively classify phishing websites and address the shortcomings inherent in each individual method. Similarly, Ojugo et al. also presented fraud detection technique in [56].

In [57], Liu et al. presented quantum-based encryption integrated with the logistic map and permutation operation, which are applied to the extracted bit-planes. Initially, the image is represented in a quantum model, followed by the application of the Arnold transform to rearrange pixel positions. Then, XOR operations are applied to the extracted bit planes. Finally, the encrypted image is obtained by applying a diffusion operation to the image obtained after the XOR operation. Simulation results indicated that the integration of quantum-based encryption with chaos and bit-plane extraction methods provided enhanced security for digital data. In [58], Chai et al. presented a color image encryption scheme that is based on the bit-plane extraction method. The bit-plane extraction technique is combined with chaos-based scrambling. In their proposed framework, the color components are extracted from the original image, and then bit-planes are extracted from each component. Random sequences are used to permute the bits within the bit planes. Subsequently, three 2-D matrices are generated to perform XOR operations with each color component. In [59], Kumar et al. presented an innovative approach to fortify the security of medical images through the integration of Deep Learning, Chaotic Map, and Hash Table. The synergistic

application of these techniques enhances the robustness of image protection, ensuring the confidentiality and integrity in medical data. In [60], Chakraborty et al. introduced a cutting-edge enhanced with Masi entropy. Leveraging the Intelligent Fish Optimization and Discrete Particle Swarm Optimization, coupled with Masi entropy, this scheme offers an advanced solution for multi-level image segmentation, promising improved accuracy and efficiency in image analysis. In [61], Deng et al. unveiled a problem-based cybersecurity lab featuring a knowledge graph as a guiding framework. The integration of problem-oriented scenarios and knowledge graphs provides a robust and practical learning environment, enhancing the effectiveness of cybersecurity education and skill development. Similarly, and other techniques to secure digital data can be found in [62]–[65]

A. ENHANCEMENTS TO EXISTING APPROACHES

To address the limitations of existing encryption schemes, this research proposes an extended version of the Bit-Plane Extraction, Chaotic Permutation, and Diffusion (BPCPD) approach. The proposed contributions can be summarized as follows:

1) **Enhanced Key Distinctiveness:** To mitigate the risk of equivalent keys, a novel algorithm is introduced, serving the dual purpose of generating both random sequences and key images. This approach ensures a higher degree of key distinctiveness, thereby bolstering the overall security of the system.
2) **Complex Diffusion Operations:** To enhance the complexity of the diffusion operation within the proposed encryption scheme, a nonlinear transformation is introduced, involving the substitution of image pixels. Additionally, the bit-level diffusion technique is integrated with the XOR operation, creating a more robust security framework.
3) **Innovative Permutation Techniques:** In the process of permutation, the proposed encryption technique incorporates three distinct methods: multi-layer permutation, multi-round permutation, and recursive permutation. These techniques aim to address the shortcomings of conventional permutation approaches, providing heightened security and diversity.
4) **Reinforcing the Confusion-Diffusion Framework:** The new encryption approach introduces a novel technique that successfully addresses the limitations of the conventional confusion-diffusion framework. This accomplishment is attained by incorporating complex permutation and diffusion processes, resulting in a substantial enhancement of both the security and efficiency of the encryption procedure.

These enhancements collectively guide the development of an advanced image protection mechanism, offering enhanced security and efficiency in response to the identified limitations and security challenges in existing encryption methods.

III. RECAP OF THE BPCPD

This section provides a brief overview of the encryption framework known as BPCPD. The recap of BPCPD involves a brief explanation of the chaotic maps employed in the encryption scheme proposed in [5], along with the procedural steps utilized in the development of BPCPD.

A. CHAOTIC MAPS USED IN BPCPD

BPCPD employs a couple of distinct chaotic maps, namely the logistic map and the cubic logistic map. The mathematical expressions for these two chaotic maps are presented in Equations 1 and 2, respectively.

$$\Xi_{m+1} = \alpha \times \Xi_m(1 - \Xi_m) \tag{1}$$

$$\beta_{m+1} = \gamma\beta_m(1 - \beta_m)(2 + \beta_m) \tag{2}$$

In Equation 1 the state variable Ξ takes values within the interval (0, 1), while the control parameter α falls within the range (3.57, 4). At α = 3.99, Equation 1 enters a chaotic state.

In Equation 2, the state variable β takes values within the range of (0, 1), while the control parameter γ is situated between the values of 1.41 and 1.59. At γ = 1.58, Equation 2 exhibits chaotic behavior. The bifurcation diagrams of the chaotic behaviors are given in [5].

B. EXPLANATION OF BPCPD

The explanation for the secret keys and the encryption process of BPCPD is presented as follows:

1) Secrete keys used in BPCPD

There is a very simple structure of the secret keys used in BPCPD. The author only utlized the pair of initial values such as Ξ_m and β_m, and the pair of control parameters such as α and γ are used as the secret keys.

2) Encryption process of BPCPD

The encryption process of BPCPD is initialized by breaking down a plaintext image with dimensions $L \times B$ into its individual eight-bit planes. Here, L and B denote the number of rows and columns in the plaintext image, respectively.

The same encryption method (BPCPD) is also applicable to color images with dimensions $B \times 3L$. The schematic overview of BPCPD is illustrated in Figure 1, where three primary notations $I = \underset{i=0\to B, j=0\to L,}{I(i,j)}$, $S = \underset{i=0\to B, j=0\to L,}{S(i,j)}$, and $C = \underset{i=0\to B, j=0\to L}{C(i,j)}$ represent the plaintext, scrambled, and final ciphertext images generated through BPCPD, respectively.

BPCPD comprises three fundamental stages: (a) decomposition of the plaintext image, (b) bit-wise scrambling, and (c) decomposition of a random image into its eight-bit planes, followed by applying the XOR operation with the permuted bit-planes of the plaintext image. The details of these three stages are provided below:

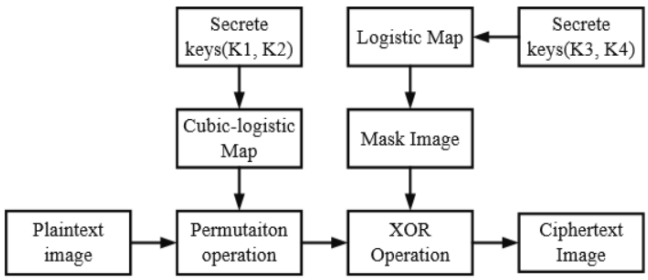


FIGURE 1: The schematic overview of BPCPD

Satge-1: In the first stage of BPCPD, the plaintext image is divided into eight bit-planes using Equation 3.

$$\begin{cases} I_{b1} = (\frac{I}{1})mod2, & I_{b2} = (\frac{I}{2})mod2, \\ I_{b3} = (\frac{I}{4})mod2, & I_{b4} = (\frac{I}{8})mod2, \\ I_{b5} = (\frac{I}{16})mod2, & I_{b6} = (\frac{I}{32})mod2, \\ I_{b7} = (\frac{I}{64})mod2, & I_{b8} = (\frac{I}{128})mod2 \end{cases} \tag{3}$$

Where I_{b8} through I_{b5} represent the most significant bit planes ($MSBPs$), and I_{b4} to I_{b1} denote the least significant bit planes ($LSBPs$). Each individual bit-plane encompasses distinct information levels, which can be computed utilizing Equation 4. The distribution of varying information levels can also be observed visually in Figure 2.

$$I_{(b_j)} = \frac{2^{j-1}}{\sum_{j=1}^{8} 2^{j-1}} \tag{4}$$

Bit-wise permutation: The bitwise operation is performed on all the MSBPs and the LSBPs. The rows and the columns of the MSBPs and the LSBPs are permuted according to the random sequences ($X_i = x_1, x_2, x_3, \cdots x_B$), ($Y_i = y_1, y_2, y_3, \cdots y_B$), respectively. This stage of the BPCPD is named as confusion stage.

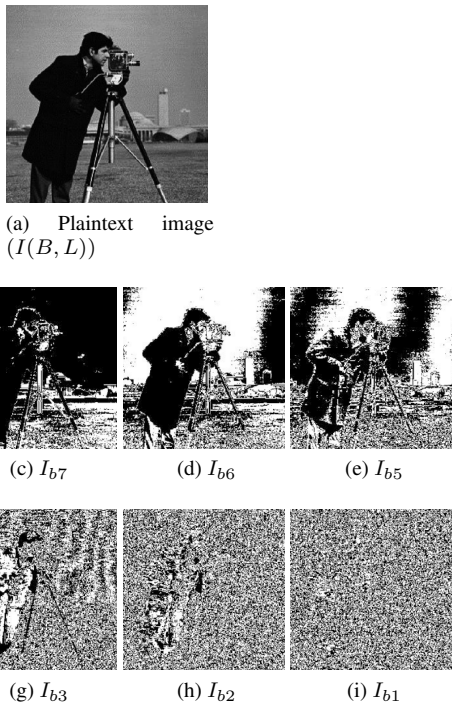
Diffusion stage: The diffusion in the permuted bit-planes is created using only the XOR operation. A new random image is generated using chaos and decomposed into eight-bit planes using Equation 3. Such bitplanes are then XORed with the permuted MSBPs and the LSBPs. In this step, all the manipulated bit-planes (M_{bj}) are combined using Equation 5 to generate the final ciphertext (**C**) image.

$$\begin{aligned} C = 2 \times (2 \times (2 \times (2 \times (2 \times (2 \times M_{b8} + M_{b7}) \\ + M_{b6}) + M_{b5}) + M_{b4}) + M_{b3}) + M_{b2}) + M_{b1}) \end{aligned} \tag{5}$$

IV. INCORPORATION OF CHAOTIC MAPS WITHIN THE PROPOSED ENCRYPTION SCHEME

There are multiple chaotic maps for the purpose of creating confusion and diffusion are used in the proposed encryption scheme. This section presents a brief overview of these chaotic maps.

The first chaotic map used in this research is the hyper-chaotic map. Its mathematical form is described in Equation 6.



(a) Plaintext image ($I(B, L)$)

(b) I_{b8} (c) I_{b7} (d) I_{b6} (e) I_{b5}

(f) I_{b4} (g) I_{b3} (h) I_{b2} (i) I_{b1}

FIGURE 2: Decomposition of $I(B, L)$ into its eight bit planes (I_{bj})

$$\begin{aligned} \alpha^{\cdot} &= \phi(\beta - \alpha) \\ \beta^{\cdot} &= -\alpha \cdot \gamma + \Omega \cdot \alpha + \omega\beta - \mu \\ \gamma^{\cdot} &= \alpha \cdot \beta - \theta \cdot \gamma \\ \mu^{\cdot} &= \alpha + \lambda \end{aligned} \tag{6}$$

In Equation 6 $\phi, \theta, \omega, \Omega$ and λ are the parameters of system. At ϕ = 36, θ = 3, ω = 28, Ω = 16, and $-0.7 \leq \lambda \leq 0.7$, the system enters a chaotic state. This state results in the creation of four distinct chaotic sequences. In the proposed encryption scheme, a hyper-chaotic system is employed to create the hyper-chaotic sequences for permutation purposes.

The other chaotic map used in the proposed work is the chaotic CAT map. The conventional Cat map is a 2-D chaotic system, depicted as follows:

$$\begin{bmatrix} \delta_{i+1} \\ \Delta_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} \delta_i \\ \Delta_i \end{bmatrix} \cdot mod(1) \tag{7}$$

Given that δ_i and Δ_i belong to the interval $[0, 1)$, the notation $(\cdot)$ $mod(1)$ signifies the fractional parts of a real value.

Following this, the Arnold Cat map transforms into an area-preserving and invertible chaotic map upon the introduction of two control parameters denoted as X and Y The resulting expression is as follows:

$$\begin{bmatrix} \delta_{i+1} \\ \Delta_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & X \\ Y & 1 + XY \end{bmatrix} \begin{bmatrix} \delta_i \\ \Delta_i \end{bmatrix} \cdot mod(B \times L) \tag{8}$$

X and Y represents the control paramter, and $B \times L$ is the size of the original image.

V. PROPOSED ENCRYPTION ALGORITHM

The proposed encryption algorithm introduces several new elements: (i) It integrates multiple high-dimensional chaotic maps to counter the risk of equivalent keys; (ii) It integrates non-linear transformation with an XOR operation to create diffusion in the plaintext image; and (iii) It incorporates three separate permutation techniques—multi-layer permutation, recursive permutation, and multi-round permutation—with the intention of increasing the complexity of the proposed encryption scheme's structure. These additions aim to address the vulnerabilities identified in the encryption approach proposed in [5].

A. ENCRYPTION PROCESS

In the development of the proposed cryptosystem, two essential factors are considered: robust security and low computational time. The step-by-step block diagram of the suggested encryption scheme is depicted in Figure 3. The specifics of each step within the proposed scheme are elaborated upon below.

- Load the plaintext image with dimensions $B \times L$ and then break it down into eight individual bit-planes. In the proposed encryption process, only $MSPs$ are considered for encryption, as they contain over 90% of the plaintext information as displayed in Table **??**. As a result, encrypting every individual bit is unnecessary, as this would lead to a higher overall computational time for the encryption algorithm.
- After extracting the bit-planes, apply permutation operations according to the generated random sequences (R_1 and R_2) using a hyperchaotic map and a chaotic CAT map. The permutation operation is applied to the rows and columns of the bit-planes. Therefore, the values in the random sequence will lie in the range 0 to $B-1$ and 0 to $L-1$, respectively i.e. ($R_1 \in [0, B-1], R_2 \in [0, L-1]$). The steps to generate the random sequences are given in Algorithm 1.

Algorithm 1 Algorithm for the generation of random sequences and random image

Start

Input $\theta, \phi, \omega, \Omega, \lambda, X, Y, \delta_1, \delta_1$

for i = 1: $B \times L$

$$\begin{cases} \text{Implement Equation 6} \\ \delta_{i+1} = \left(\delta_i + X \cdot \Delta_i\right) \cdot mode(\times L) \\ \Delta_{i+1} = \left(\delta_i \cdot Y + \Delta_i + XY\Delta_{i)} \cdot mode(\times L)\right. \end{cases}$$

{ Implementation of chaotic maps}

$$\text{E(i+1)} = 989 \times \begin{cases} \text{Equation 6} \\ \delta_{i+1} \\ \Delta_{i+1} \end{cases}$$ { Enlarge the values generated in the previous step}

$$\text{F(i+1)} = \text{floor}\left[\text{ E(i+1)}\right]$$ { Convert the fractional values into integer values}

$$R_1 = \text{mod}\left[\text{ F(i+1)}, B \times L\right]$$ { Random Sequence # 1}

end

$$\text{R}_{image} = reshape\left[R_1, B, L\right]$$

{ Figure 4 shows the random image (R_{img})}

End =0

B. PERMUTATION MODULE

- Apply the permutation operation on the bit-lanes according to the generated random sequence (R_1). The permutation operation is completed in three stages. The first stage is the multi-layer permutation.

  Multi-layer permutation: In multi-layer permutation, a sequence of scrambling operations is carried out for each individual layer. In this paper, each bit plane is considered a different layer and a unique permutation sequence is applied to each layer, resulting in more complex pixel arrangements. The implementation of this multilayer permutation process significantly increases the level of complexity within the positions of image pixels, as opposed to relying only on a single-layer permutation technique.

  The permutation process is applied in the proposed encryption scheme as follows:

  Layer 1: The plaintext image pixels undergo permutation based on a specific pattern (in this case, R_1 is considered).

  Layer 2: The outcome from Layer 1 serves as the input for Layer 2. A new set of random values is created for the purpose of shuffling the pixel values within the image that are generated from the permutation procedure of Layer 1.

  Layer 3: Transform the image produced within layer 2 into distinct blocks, subsequently applying permutation to these blocks to produce the final permuted image within the framework of the multi-layer permutation process.

  Different sequences are employed for the permutation process in each layer, as opposed to using identical random sequences across all layers. This approach significantly enhances the security level, surpassing the effectiveness of employing the same random sequences for all layers in the permutation process. The complete permutation process is elaborated step-by-step as follows:

- Let the R_1 is: $\begin{bmatrix} 4 & 3 & 1 & 2 \end{bmatrix}$ and the plaintext image I is: $\begin{bmatrix} 137 & 241 & 112 & 106 \\ 29 & 167 & 39 & 29 \\ 167 & 59 & 21 & 236 \\ 96 & 23 & 196 & 209 \end{bmatrix}$

  The binary version of the image I will be I_b:

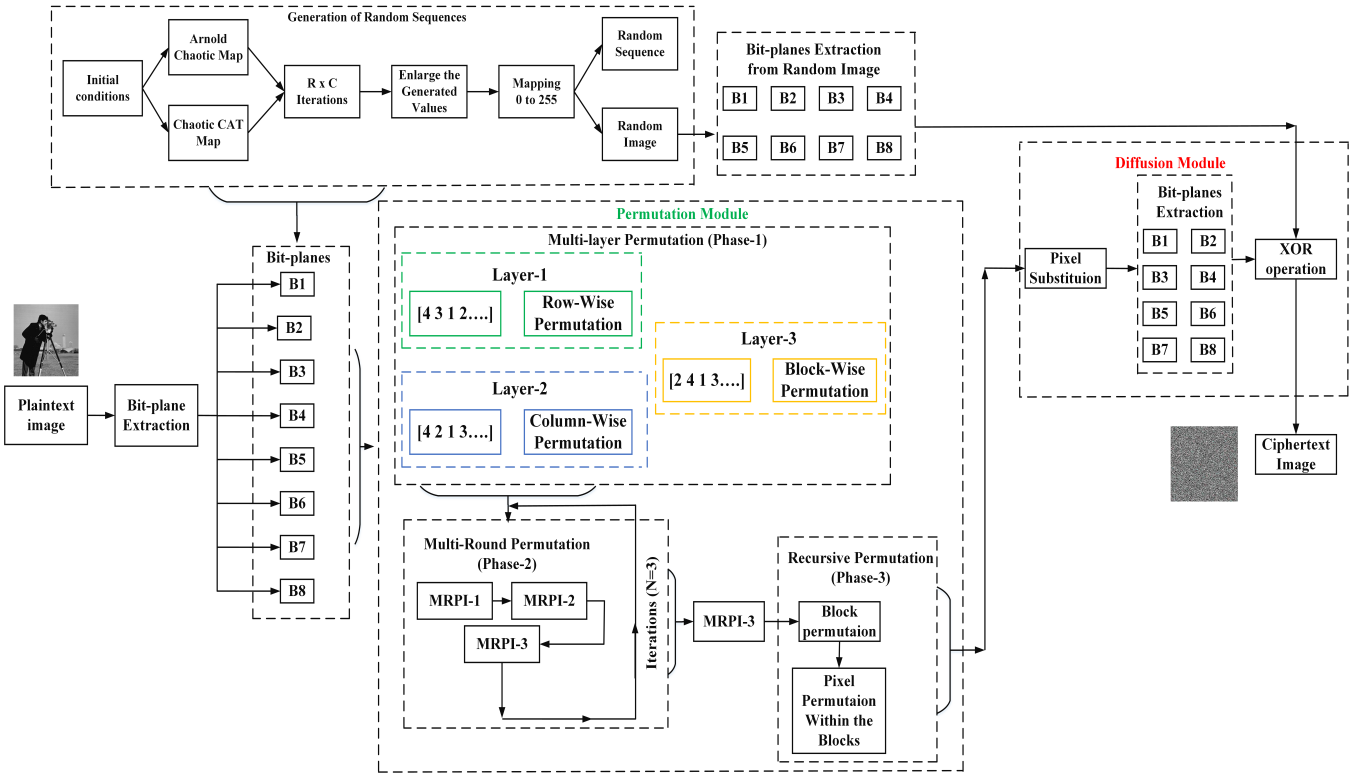


FIGURE 3: The encryption process of the proposed algorithm

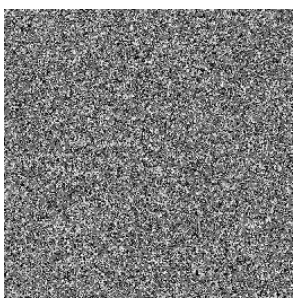


FIGURE 4: Random image

$$I' = \begin{bmatrix} 10001001 & 11110001 & 01110000 & 01101010 \\ 00011101 & 10100111 & 00100111 & 00011101 \\ 10100111 & 00111011 & 00010101 & 11101100 \\ 01100000 & 00010111 & 11000100 & 11010001 \end{bmatrix}$$

By extracting the binary bitplanes from I', the process involves assigning the 1st most significant bit (MSB) of every pixel value to the 8th bit-plane. Similarly, the 2nd MSB of pixel values contributes to the 7th bit-plane, and this sequence persists. As a result, the resulting bit-planes of the image I are organized as follows:

$$B_8 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, B_7 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

$$, B_6 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, B_5 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$B_4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, B_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$, B_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, B_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Considering the matrix R_1 as: $\begin{bmatrix} 4 & 3 & 1 & 2 \end{bmatrix}$ for the permutation of layer 1, the resultant scrambled bit-planes at layer-1 (P_{iL1}) will be:

- **Row-wise Permutation (Layer-1)**

$$P_{8L1} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, P_{7L1} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$, P_{6L1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, P_{5L1} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$P_{4L1} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}, P_{3L1} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$, P_{2L1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, P_{1L1} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Considering the matrix R_2 as: $\begin{bmatrix} 4 & 2 & 1 & 3 \end{bmatrix}$ for the permutation of layer 2, the resultant scrambled bit-planes (SB_s) will be:

- **Column-wise Permutation (Layer-2)**

$$P_{8L2} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, P_{7L2} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$, P_{6L2} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, P_{5L2} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$P_{4L2} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}, P_{3L2} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$, P_{2L2} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, P_{1L2} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Following the execution of the multi-layer permutation operation, merge the corresponding bits to create the permuted image. The resulting image ($I^{'}$) can be expressed as:

$$I'' = \begin{bmatrix} 10111011 & 00100111 & 00010101 & 11000100 \\ 11110001 & 10001001 & 01110000 & 00010101 \\ 10100111 & 00011101 & 00100111 & 01110000 \\ 00011101 & 10100111 & 00011101 & 00100111 \end{bmatrix}$$

$$I'' = \begin{bmatrix} 187 & 39 & 21 & 196 \\ 241 & 137 & 112 & 21 \\ 167 & 29 & 39 & 112 \\ 29 & 167 & 29 & 39 \end{bmatrix}$$

- **Block-wise Permutation (Layer-2)**
Convert the image I'' into blocks of size 2×2 as follows: Block-1 = $\begin{bmatrix} 187 & 39 \\ 241 & 137 \end{bmatrix}$, Block-2 = $\begin{bmatrix} 21 & 196 \\ 112 & 21 \end{bmatrix}$, Block-3 = $\begin{bmatrix} 167 & 29 \\ 29 & 167 \end{bmatrix}$ and Block-4 = $\begin{bmatrix} 39 & 112 \\ 29 & 39 \end{bmatrix}$. For the block permutation, the new random sequence let's say $R_3 = \begin{bmatrix} 2 & 1 & 4 & 3 \end{bmatrix}$. The new block-wise permuted (B_P) image will be: $B_P = \begin{bmatrix} 21 & 196 & 187 & 39 \\ 112 & 21 & 241 & 137 \\ 39 & 112 & 167 & 29 \\ 29 & 39 & 29 & 167 \end{bmatrix}$.
- **Multi-round permutation:** The second phase involves a multi-round permutation, which is applied to the output (B_P) produced in the multi-layer permutation process. This stage encompasses three iterations, each contributing to the generation of the multi-round permuted images upon completing all the steps within the multi-layer permutation process, i.e., multi-round permuted image-1 ($MRPI-1$), multi-round permuted image-2 ($MRPI-2$), and multi-round permuted image-3 ($MRPI-3$). The resulting $MRPIs$ are given below:

$$MRPI-1 = \begin{bmatrix} 214 & 197 & 33 & 13 \\ 29 & 167 & 210 & 219 \\ 156 & 27 & 19 & 187 \\ 213 & 201 & 14 & 29 \end{bmatrix}, MRPI-2 = \begin{bmatrix} 21 & 15 & 145 & 210 \\ 15 & 22 & 96 & 187 \\ 296 & 156 & 31 & 66 \\ 25 & 198 & 153 & 32 \end{bmatrix}$$

$$MRPI-3 = \begin{bmatrix} 31 & 196 & 201 & 39 \\ 49 & 168 & 20 & 38 \\ 159 & 136 & 198 & 235 \\ 198 & 163 & 29 & 198 \end{bmatrix}$$

- **Recursive permutation:** The third stage of the permutation process in the proposed encryption scheme is the recursive permutation. In this process, two rounds of permutation are performed: First round is devoted to the block-wise permutation while in the second round, pixel permutation within the block is performed. In this recursive permutation process, $MRPI-3$ is taken as input. The first block of $MRPI-3$ is: ($B_1MRPI-3$) = $\begin{bmatrix} 31 & 196 \\ 49 & 168 \end{bmatrix}$, second block of of $MRPI-3$ is: ($B_2MRPI-3$) = $\begin{bmatrix} 201 & 39 \\ 20 & 38 \end{bmatrix}$, third block of of $MRPI-3$ is: ($B_3MRPI-3$) $\begin{bmatrix} 159 & 136 \\ 198 & 163 \end{bmatrix}$= and forth block of of $MRPI-3$ is: ($B_4MRPI-4$) = $\begin{bmatrix} 198 & 235 \\ 29 & 198 \end{bmatrix}$. For the block permutation, consider R_4 a permutation vector i.e. R_4 $\begin{bmatrix} 2 & 1 & 4 & 3 \end{bmatrix}$, and permute the block accordingly. The Pre-permuted image (P_{pi}) is: P_{pi} = $\begin{bmatrix} 201 & 39 & 31 & 196 \\ 20 & 38 & 49 & 168 \\ 198 & 235 & 159 & 136 \\ 29 & 198 & 198 & 163 \end{bmatrix}$. In the last, permutation

within the block is performed according to random vector $R_5 = \begin{bmatrix}2 & 3 & 4 & 1\end{bmatrix}$. The final permuted image (F_{pi}) is: $\begin{bmatrix}39 & 38 & 196 & 168\\ 20 & 201 & 49 & 31\\ 235 & 29 & 136 & 198\\ 198 & 198 & 163 & 159\end{bmatrix}$

C. DIFFUSION MODULE

- To create the diffusion in the final permuted images, a non-linear transformation using multiple substitution boxes (S-boxes), and then XOR operation is performed with the generated random image using the chaotic map. The steps to perform the substitution of F_{pi} using multiple substitution box is given in Algorithm 2

Algorithm 2 Modified multiple S-boxes process

```
Start
Input F_pi and Multiple S-boxes
[B L] =size(F_pi)
  for i = 1 : B
    for j = 1 : L
      bin_p = dec2bin(F_pi(i,j),8);
      sboxx_r_b = [bin_p(1) bin_p(2) bin_p(3) bin_p(4)];
      sboxx_c_b = [bin_p(5) bin_p(6) bin_p(7) bin_p(8)];
      sboxx_r_d = bin2dec(sboxx_r_b) + 1;
      sboxx_c_d = bin2dec(sboxx_c_b) + 1;
      if (d(n)==0)
        I(i,j)= Skipjack_Sbocx(sboxx_r_d,sboxx_c_d);
      elseif (d(n)==1)
        I(i,j)= S8_Sbox(sboxx_r_d,sboxx_c_d);
      elseif (d(n)==2)
        S_box(i,j)= AES_Sbox(sboxx_r_d,sboxx_c_d);
      end
      n=n+1;
    end
    end
End =0
```

- Extract the bit-planes from S_{box} and the random image R_{image} and perform XOR operation. The XOR operation between the bit-planes is given Equation 9.

$$\begin{cases} X_1 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S1} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im1}}, \\ X_2 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S2} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im2}}, \\ X_3 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S3} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im3}}, \\ X_4 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S4} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im4}}, \\ X_5 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S5} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im5}}, \\ X_6 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S6} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im6}}, \\ X_7 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S7} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im7}}, \\ X_8 = \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{S8} \oplus \sum_{i=1}^{L=1}\sum_{j=1}^{B=1} B_{R_{im8}} \end{cases} \tag{9}$$

Where, $X_1, X_2, \cdots, X_8$,$B_{S1}, B_{S2}, \cdots, B_{S8}$, and B_{R_im1}, B_{R_im2}, $\cdots$, B_{R_im8} are the diffused images, bit-planes extracted from $S_{box}(i, j)$, and the bit-planes extracted form R_{im}, respectively. L and B represent the dimensions of the image in terms of its rows and columns.

- To produced the final encrypted image (**E**), Equation 5 becomes:

$$\begin{aligned} E = 2 \times (2 \times (2 \times (2 \times (2 \times (2 \times (2 \times \\ X_8 + X_7) + X_6) + X_5) + X_4) + X_3) \\ +X_2) + X_1) \end{aligned} \tag{10}$$

- To obtain the plaintext image from the ciphered image, the reverse steps of the proposed encryption scheme will be executed.

Figure 5(m-x) shows the encrypted results achieved by applying the proposed encryption algorithm to the test plaintext images as shown in Figure 5(a-l). Furthermore, Figure 5 provides the evidence that the proposed framework possesses the ability to entirely conceal the plaintext data.

Details regarding the implementation setup for this encryption algorithm are provided in Section VI-A.

D. KEY MANAGEMENT AND ENTITIES

The proposed work involves key management carried out by the following entities and methods:

- In the initial phase, random sequences, and a random image are generated using multiple chaotic maps, such as the chaotic Arnold map and the chaotic CAT map. Key management is performed here through the generation and secure storage of these chaotic maps, which are used in the encryption process. The parameters and seeds for these chaotic maps act as keys.
- The second phase involves permutation operations, including multi-layer permutation, multi-round permutation, and recursive permutation. These permutations are controlled by the random sequences generated using chaotic maps, in which parameters such as control and initial values are used as secret keys.
- The third phase introduces diffusion to the permuted image through pixel substitution and XOR operations performed on the respective bit planes of the random image. The keys used in this phase are essential to controlling the XOR operations and pixel substitution, ensuring the reversible transformation of data.

VI. EXPERIMENTAL ANALYSIS

Experimental analysis offers valuable insights into the performance and security of the extended BPCPD approach in information security. In this section, the empirical evaluation of the proposed encryption framework is carried out, aiming to shed light on its real-world effectiveness. Through a series of experiments and assessments, the strengths and capabilities of the proposed cybersecurity solution is revealed. The test images (standard images), including Lena and Cameramen, used for the experimental results and analysis are not sourced from a specific dataset; instead, they are obtained from publicly available resources on Google.

FIGURE 5: Plaintext and their corresponding ciphertext

A. EXPERIMENTAL ENVIRONMENT

The experimentation, results, and analysis are carried out using MATLAB 2014a on a computer system equipped with 8GB RAM, a Core i-5 processor running at 2.4 GHz, a 64-bit operating system, and Windows 11.

Multimedia data can be vulnerable to a range of attacks, such as chosen ciphertext, known plaintext, statistical attacks, brute-force attacks, and differential attacks. A robust cryptosystem should possess the capability to withstand all these attacks. The proposed algorithm has undergone an extensive battery of assessments, encompassing key sensitivity, key space, NIST tests, histogram, information entropy, correlation, differential attack, contrast, ciphertext image quality, cropping, noise attack, and computational time analyses. Detailed results and findings from these analyses are presented in the subsequent subsections.

B. KEY SENSITIVITY ANALYSIS

To prevent brute-force attacks, the cryptosystem must exhibit sensitivity to the secret key. To assess key sensitivity, an experiment is conducted involving the encryption and subsequent decryption of a plain image. In this process, the original key is slightly altered and then employed for the analysis. The original secret keys utilized in the proposed encryption algorithm are as follows: $\theta = 3.000000000000000, \phi = 36.000000000000000, \omega = 28.000000000000000, \Omega = 16.000000000000000, \lambda = 0.6000000000000000, X = 1.2300000000000000, Y = 1.8000000000000000, \delta_1 = 0.3000000000000000,$ and $\Delta_1 = 0.5000000000000000$. The analysis of key sensitivity is conducted through two approaches:

- **Case-1:** Encrypting the plaintext images using a set of accurate and inaccurate keys,
- **Case-2:** Decrypting the plaintext image from the encrypted image using both sets of keys, i.e., accurate and

inaccurate secret keys.

In the first scenario (Case-1), the original secret keys are used to encrypt the plaintext image, followed by another encryption using the slightly modified keys: $\theta = 3.00000000000001, \phi = 36.00000000000001, \omega = 28.00000000000001, \Omega = 16.00000000000001, \lambda = 0.600000000000001, X = 1.2300000000000001, Y = 1.800000000000001, \delta_1 = 0.300000000000001$, and $\Delta_1 = 0.500000000000001$. The encrypted images using correct and incorrect keys are denoted by E_1 and E_2, respectively. By calculating the difference ($D_{key} = E_1 - E_2$) between the images obtained from the correct and modified keys, it is evident that 98% of pixel values in E_1 and E_2 are dissimilar, as shown in Table 1. Several plaintext images are tested to conduct the key sensitivity analysis, the difference (D_{key}) is more than 97%.

TABLE 1: Percentage difference between E_1 and E_2

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
Proposed	98.64	97.67	97.91	97.99	97.84
BPCPD [5]	93.33	92.48	94.67	94.78	94.83
Ref [66]	89.36	91.67	90.66	96.45	94.64
Ref [67]	91.61	90.52	91.15	95.36	92.37
Ref [68]	90.36	92.12	91.78	95.17	93.44
Ref [53]	89.73	92.58	91.24	94.81	93.11
Ref [54]	90.89	92.07	91.98	95.62	93.75
Ref [57]	90.02	91.45	91.76	95.28	93.33

In the second scenario (Case-2), decryption of the plaintext image is attempted using both the original and slightly altered secret keys. It became evident that the utilization of incorrect keys for decryption resulted in an outcome that significantly diverged from the original plaintext image. This difference in the decrypted and plaintext image is visually represented in Figure 6.

C. KEY SPACE ANALYSIS

Keyspace analysis provides information on whether an encryption algorithm can withstand a brute-force attack or not. In brute force attack analysis, the attacker tries each combination of secret keys to find the correct key to recover the plaintext information. In this proposed encryption scheme, there are nine secret keys are used and each key has the sensitivity of 10^{-14} as demonstrated in section VI-B. Therefore, the key space for each individual key is 10^{+14}. As a result, the combined key space for the secret keys utilized in the proposed cryptosystem will be $10^{+14\times 9}$, which can be expressed as 2^x," as illustrated below:

$$\begin{aligned} log2^x &= log10^{126} \\ x \cdot log2 &= 126 \cdot log10 \\ x &= \frac{135}{0.3010} \\ x &= 418 \end{aligned} \tag{11}$$

According to Alvazari [69], the key size should be no less than 2^{100} to effectively resist brute force attack. In the proposed cryptosystem, the secret keys employed possess a key space of 2^{448}, rendering them exceptionally resilient against brute force attacks. This extensive key space not only suffices to resist such an attack but also aligns with Alvazari's criteria for the keyspace.

D. NIST TEST ANALYSIS

The NIST test is conducted to evaluate the randomness of the sequences generated using chaotic maps. NIST testing is typically designed for binary sequences, and chaotic sequences often produce continuous or floating-point values. To apply NIST tests to chaotic sequences generated in the proposed work, an approach known as binarization [70], [71] is applied to convert the continuous values into binary sequences. The detailed steps of applying NIST analysis can be found in [72], [73].

This comprehensive set of statistical tests encompasses 15 individual assessments. For a given test, if the resulting P-value exceeds 0.01, it confirms the randomness of the sequence [74]. The NIST test outcomes for random sequences are presented in Table 2, which exhibits that all the conducted tests have achieved successful validation.

TABLE 2: NIST test analysis

Test	P-value of enciphered images	Passed/Failed
Frequency	0.8345	Passed
Approximation entropy	0.5301	Passed
Freq Rank test	0.4398	Passed
frequency within blocks	0.7653	Passed
Cumulative sum	0.9291	Passed
Longest run of ones	0.6159	Passed
Serial test	0.8371	Passed
Run test	0.5632	Passed
Linear complexity	0.4297	Passed
Non-overlapping template	0.5130	Passed
Random excursions variant	0.8738	Passed
Random excursions	0.5391	Passed

E. HISTOGRAM ANALYSIS

To access the proposed framework, histogram analysis are conducted on both the original and encrypted images. Evidently, there is no similarity between the two as shown in Figure 7. The histograms of the original images exhibit uneven distributions with elongated peaks, whereas their encrypted counterparts display flat and uniform histograms. Visual representation of this distinction is presented in Figure 7 showing 2D histograms. It is evident that there is a substantial difference observed in the histograms of the encrypted images when compared to those of the original plaintext images.

F. HISTOGRAM VARIANCE ANALYSIS

To assess the uniformity of the ciphered images quantitatively, the variance γ of the histograms is utilized as a measure [75]. This variance is determined using Equation 12 by accounting for the pixel counts γ_i and γ_j corresponding to gray values i and j, respectively.

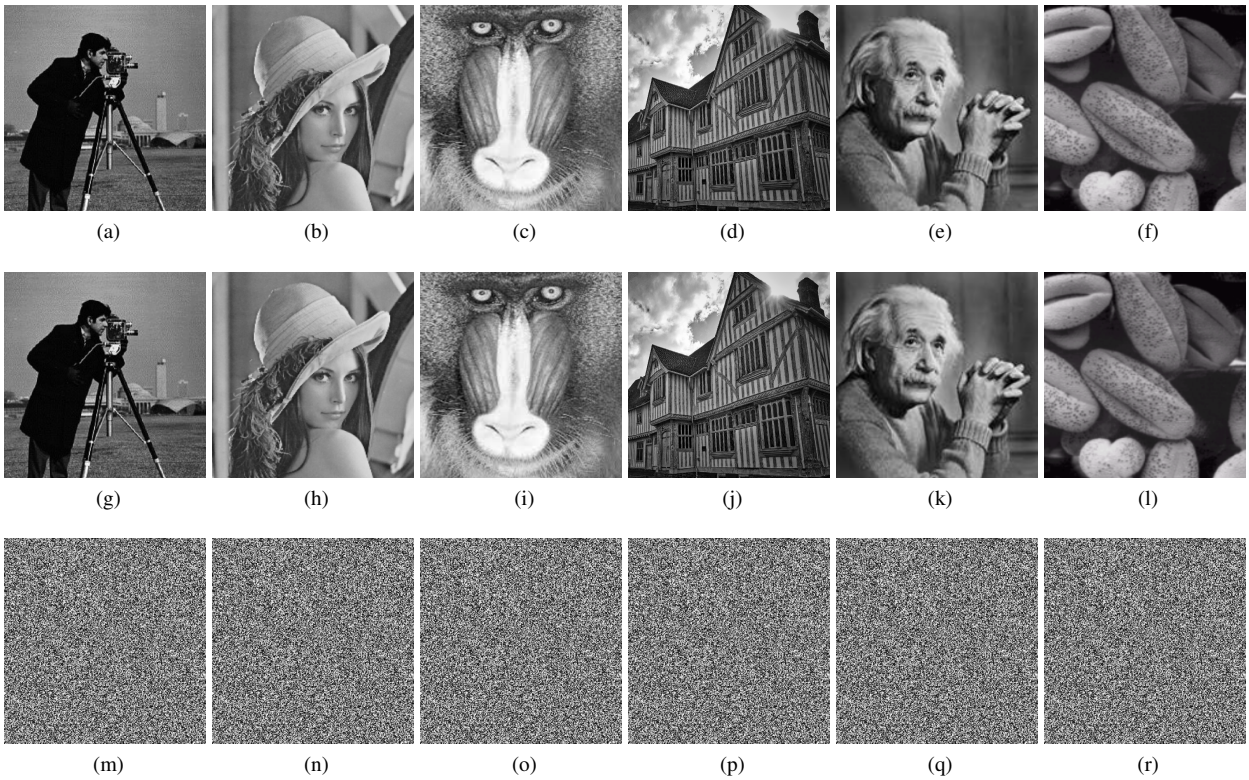


FIGURE 6: Key sensitivity analysis: (a-h) Plaintext images, (i-p) Decryption with correct keys, (q-x) Decryption with incorrect keys

$$Var(\gamma) = \frac{1}{m}\sum_{i=1}^{m}\sum_{j=1}^{m}\left[\frac{1}{2}\left(\gamma_i - \gamma_j\right)^2\right] \tag{12}$$

Where m shows the number of gray levels. The smaller variance values correspond to higher uniformity in the ciphered images. The variance values for the cipher images are tabulated in Table 3, confirming that the simulation outcomes indicate uniform distribution in the histograms of encrypted images. Additionally, a comparative analysis with other schemes emphasizes that the proposed algorithm's variance values are consistently lower. This attribute enhances its resilience against statistical attacks, making the proposed scheme robust to counter such threats.

TABLE 3: Histogram variance analysis

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
BPCPD [5]	275.87	273.78	271.89	276.34	271.09
Proposed	256.10	256.43	264.39	263.11	255.37
Ref [66]	266.19	265.78	275.27	276.48	273.33
Ref [67]	275.20	277.16	270.39	271.65	270.19
Ref [68]	273.37	270.36	273.87	272.66	273.91
Ref [53]	267.58	265.92	274.33	277.14	273.89
Ref [54]	267.35	266.74	275.01	276.33	273.47
Ref [57]	266.81	266.23	275.68	276.95	274.07

G. CHI-SQUARE TEST ANALYSIS

The quantification of grayscale uniformity in pixel gray values is also assessed through the Chi-square (χ^2) test analysis. Mathematically, it can be calculated using Equation 13.

$$\begin{cases} \chi^2 = \sum_{i=0}^{m}\left[\frac{\left(H_i - \varpi\right)^2}{\varpi}\right] \\ \varpi = \frac{B\times L}{m} \end{cases} \tag{13}$$

Where H represents the histogram of the encrypted image, with H_i representing the histogram value at index i, ϖ indicating the anticipated value (mean) of the encrypted image, and B and L symbolizing the image's width and height respectively.

A lower χ^2 value signifies a higher level of grayscale uniformity. The outcomes presented in Table 4 reveal that the χ^2 values for the encrypted images produced using our suggested technique are exceptionally minimal. As a result, the histograms of encrypted images, generated through the proposed encryption scheme, demonstrate more similarity to a uniform distribution.

H. INFORMATION ENTROPY ANALYSIS

Entropy analysis serves a dual role: (i) it reflects the uncertainty in the image's information and (ii) gauges the distribution of its gray values. Information entropy varies between a

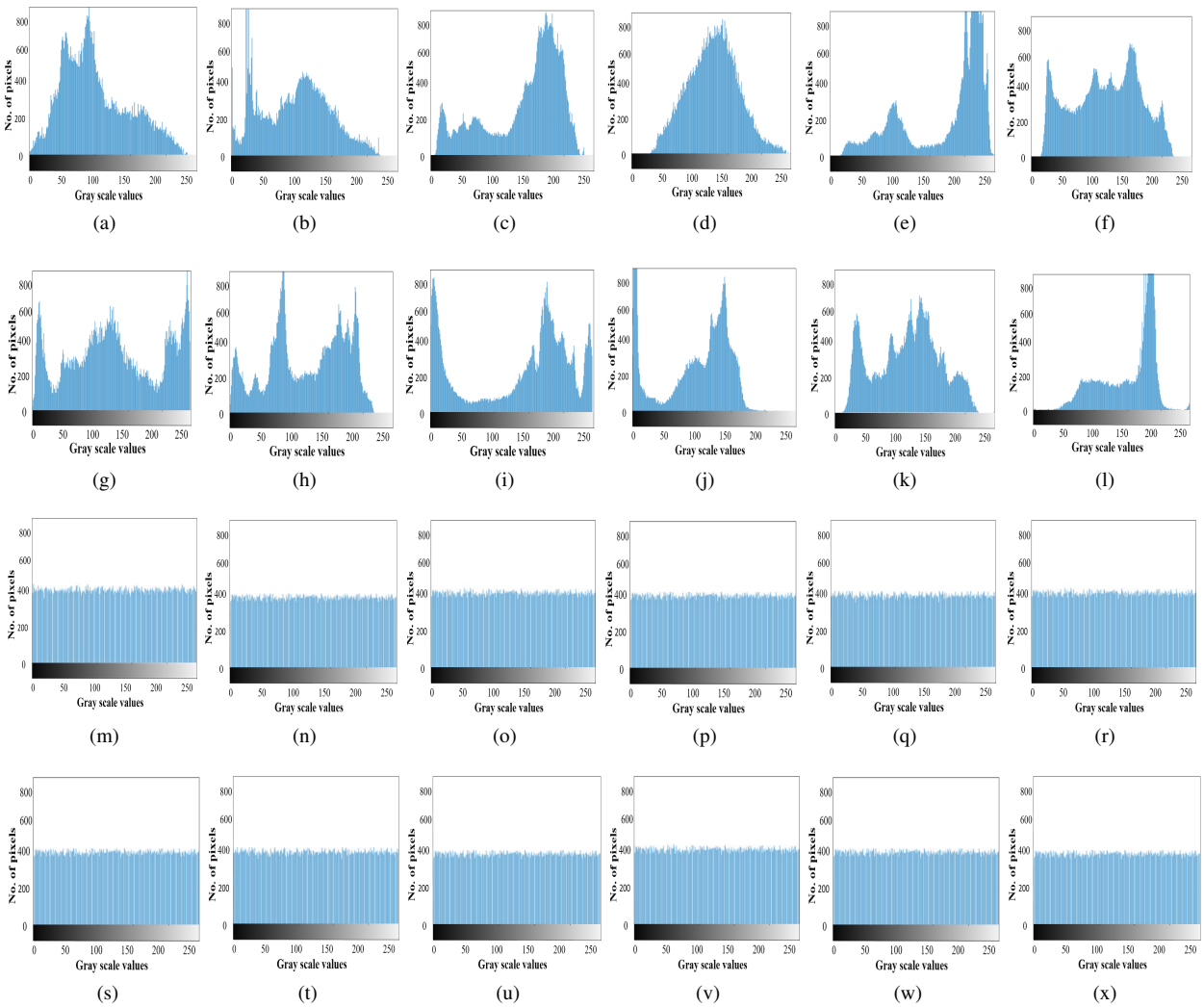


FIGURE 7: Histogram analysis

TABLE 4: Chi-square test analysis

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
Proposed	232.47	230.22	216.37	221.17	229.31
BPCPD [5]	266.34	260.67	260.58	261.8	263.48
Ref [66]	261.18	256.64	251.64	255.20	260.76
Ref [67]	261.72	251.04	251.34	276.51	265.36
Ref [68]	261.32	259.64	260.74	273.60	264.66
Ref [53]	261.25	256.49	252.07	255.38	260.59
Ref [54]	260.88	255.73	251.91	255.64	261.09
Ref [57]	260.42	256.92	251.77	255.97	261.18

minimum of zero and a maximum of eight. Thus, an efficient encryption algorithm should aim to bring the information entropy closer to a value of 8 [76]. Information entropy can be computed using Equation 14.

$$\Xi = \sum_{i=1}^{B \times L} \rho(S_i) log_2 \rho(S_i) \tag{14}$$

Where $B \times L$ represents the total number of symbols S, and $\rho(X_i)$ denotes the probability of symbol X_i occurrence. Table 5 presents a comparison of information entropy for cipher images encrypted using the proposed and existing encryption algorithms. Notably, the information entropy of the cipher image encrypted with the proposed scheme closely approaches the ideal value of 8. Furthermore, the proposed encryption scheme outperforms other algorithms with better results as compared to the existing work. This emphasizes that the suggested scheme yields optimal outcomes, implying that images encrypted using this scheme boast a distribution of random pixel values.

I. CORRELATION ANALYSIS

To assess the degree of similarity between two images, a correlation analysis is employed. Typically, neighboring pixels exhibit adjacency, resulting in a high degree of similarity and a high correlation. An effective cryptosystem must disrupt

TABLE 5: Entropy analysis

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
Proposed	7.9991	7.9992	7.9991	7.9989	7.9988
BPCD [5]	7.9870	7.9841	7.9966	7.9826	7.9972
Ref [66]	7.9371	7.9753	7.9820	7.9635	7.9771
Ref [67]	7.9865	7.9863	7.9815	7.9988	7.9886
Ref [68]	7.9896	7.9870	7.9703	7.9963	7.9995
Ref [53]	7.9879	7.9832	7.9734	7.9868	7.9880
Ref [54]	7.9896	7.9875	7.9871	7.9882	7.9951
Ref [57]	7.9988	7.9861	7.9889	7.9961	7.9988

this adjacency-based correlation to enhance security. Therefore, an encryption algorithm's effectiveness is indicated by a correlation coefficient nearing zero [77], [78]. The correlation coefficient is computed using Equation 15 in either the vertical, horizontal, or diagonal directions.

$$\begin{aligned} \sigma_{bl} &= \frac{C_{cov}(b,l)}{\sqrt{D(b)} \cdot \sqrt{D(l)}} \\ C_{cov}(b,l) &= \frac{1}{N}\sum_{i=1}^{N}\Big[b_i - E(b_i)\Big]\Big[l_i - E(l_i)\Big] \\ E(b) &= \frac{1}{N}\sum_{i=1}^{N} b_i \\ D(b) &= \frac{1}{N}\sum_{i=1}^{N}\Big[x_i - E(b_i)\Big]^2 \end{aligned} \tag{15}$$

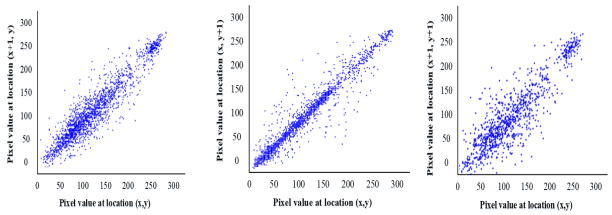
σ_{bl} denotes the correlation coefficient, whereas C_{cov} stands for the covariance between pixels b and l. Here, b signifies the pixel value in the plaintext image, and l corresponds to the pixel value in the cipher-text image, both represented using grayscale values. Furthermore, $D(b)$ represents the variance, and $E(b)$ signifies the mean of these pixel values.

The depiction of the correlation among adjacent pixels is presented in Figure 8 for both the original plaintext image and the encrypted image, observed in three distinct orientations (vertical, horizontal, and diagonal). Notably, a substantial reduction in pixel correlation is noticeable within the encrypted image.

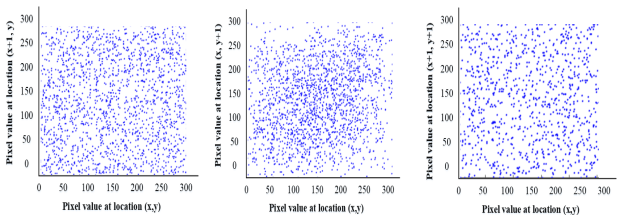
Displayed in Table 6 are the correlation distributions of diverse images encrypted utilizing the proposed algorithm, juxtaposed with outcomes from images encrypted through established algorithms. In the plaintext image, the correlation approaches unity, while in the encrypted image, it tends towards zero, exhibiting superior performance compared to other algorithms. This underscores the efficacy of the proposed algorithm in significantly diminishing the correlation among neighboring pixels within the encrypted image.

J. DIFFERENTIAL ATTACK ANALYSIS

To evaluate the consequences of a one-bit distinction between the original image and its encrypted counterpart, two metrics are utilized, such as NPCR (Number of Pixels Change Rate) and Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR), crucial for analyzing



(a) Horizontal correlation (b) Vertical correlation (c) Diagonal correlation



(d) Horizontal correlation (e) Vertical correlation (f) Diagonal correlation

FIGURE 8: Correlation analysis: (b-d) Correlation of plaintext image, (e-g) Correlation of ciphertext image

TABLE 6: Correlation analysis

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
Proposed	0.0001	-0.0027	-0.0002	-0.0018	-0.0019
BPCD [5]	0.0022	0.0032	-0.0030	0.0021	-0.0033
Ref [66]	0.0017	0.0065	0.0058	0.0031	0.0025
Ref [67]	0.0049	0.0031	-0.0011	-0.0026	0.0021
Ref [68]	0.0033	-0.0031	-0.0025	0.0031	-0.0025
Ref [53]	0.0017	-0.0025	-0.0033	-0.0033	0.0022
Ref [54]	0.0061	-0.0058	-0.0033	0.0031	0.0025
Ref [57]	0.0058	-0.0049	0.0034	0.0021	0.006

differential attacks [79]. Their computations are outlined in Equations 16 and 17.

$$UACI = \frac{\sum_{i,j} D(i,j)}{B \times L} \times 100\% \tag{16}$$

$$NPCR = \frac{\sum_{i,j} E_1(i,j) - E_2(i,j)}{255} \times 100\% \tag{17}$$

Where B and L denote the width and height of the cipher image, respectively. $E_1(i,j)$ represents the encrypted image prior to the alteration of one pixel from the plain image, while $E_2(i,j)$ corresponds to the image after the alteration.

Table 7 enumerates the values of both UACI and NPCR, both of which closely approach optimum values. NPCR reaches 99.6094%, while UACI is at 33.4635%. This substantiates the proposed encryption algorithm's heightened sensitivity to even minute alterations in the original image, indicating its resilience against differential attacks.

K. CIPHERTEXT IMAGE QUALITY TEST

To evaluate the ciphertext image quality, two metrics, such as PSNR and MSE, are frequently used. Both PSNR and

TABLE 7: Differential attack analysis

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
NPCR analysis					
Proposed	33.35	33.46	33.43	33.53	33.46
BPCD [5]	32.67	32.64	32.45	32.67	31.66
Ref [66]	31.6050	31.6572	30.4325	32.3431	32.345
Ref [67]	30.4250	31.3272	32.5125	32.3831	31.678
Ref [68]	31.4350	31.2572	32.4625	32.4531	32.314
Ref [53]	30.2450	31.6572	31.4325	30.2331	32.178
Ref [54]	32.9850	31.4572	32.3525	32.6431	32.647
Ref [57]	3.6798	32.0468	32.6478	32.8874	32.9846
UACI analysis					
Proposed	99.62	99.57	99.57	99.63	99.56
BPCD [5]	96.34	96.31	97.66	97.68	97.68
Ref [66]	96.241	94.215	91.656	94.348	96.315
Ref [67]	93.991	96.125	94.342	95.545	95.678
Ref [68]	98.241	94.546	94.631	98.444	97.648
Ref [53]	97.455	98.968	97.428	97.228	97.331
Ref [54]	96.215	98.546	97.345	98.769	97.346
Ref [57]	97.86	96.88	98.49	97.68	98.64

TABLE 8: Ciphertext image quality test

Encryption schemes ↓	Camera-man	Lina	Baboon	boat	House
PSNR analysis					
Proposed	10.36	9.64	10.03	10.78	9.99
BPCD [5]	16.98	20.99	11.78	19.61	20.16
Ref [66]	10.68	15.91	16.86	18.13	20.18
Ref [67]	9.97	10.93	11.68	10.90	11.54
Ref [68]	12.67	15.54	16.16	19.48	18.66
Ref [53]	19.97	20.87	19.18	15.99	17.97
Ref [54]	19.97	20.38	19.94	18.033	19.08
Ref [57]	28.64	17.64	19.66	15.67	18.88
MSE analysis					
Proposed	317.56	367.03	303.21	316.91	301.67
BPCD [5]	215.19	204.48	214.63	204.13	224.44
Ref [66]	203.15	204.37	181.31	198.46	191.37
Ref [67]	213.21	213.49	194.66	205.49	205.19
Ref [68]	204.49	236.16	205.98	214.37	205.38
Ref [53]	224.5712	213.5387	212.5780	203.4965	211.2687
Ref [54]	214.1715	213.3363	205.4985	224.4981	212.4319
Ref [57]	216.6483	230.4912	264.2467	251.6784	269.1972

MSE reflect the variation in pixel values between the original and cipher images. The PSNR and MSE are calculated using Equations 18 and 19, while the relationship between the MSE and PSNR is given in Equation 20.

$$PSNR = 10log\left[\frac{B \times L \times G^2}{\sum_{i=1}^{B}\sum_{j=1}^{L}\Big(O(i,j) - E(i,j)\Big)^2}\right] \tag{18}$$

$$MSE = \frac{1}{B \times L}\left[\sum_{i=1}^{B}\sum_{j=1}^{L}\Big(O(i,j) - E(i,j)\Big)^2\right] \tag{19}$$

$$PSNR \propto \frac{1}{MSE} \tag{20}$$

G' stands for a number of gray levels. B signifies the width, and L represents the length of the image. $O(i,j)$ represents the pixel value in the original image, while $E(i,j)$ stands for the pixel value in the encrypted image. The ideal encryption quality corresponds to lower PSNR and higher MSE values. The comparison of PSNR and MSE between the proposed encryption scheme and the existing ones is presented in Table 8.

L. CONTRAST

Contrast is a metric that quantifies the variation in intensity between pixels and their adjacent counterparts. A higher contrast value signifies the effectiveness of the encryption scheme. Mathematically, it is expressed in Equation 21.

$$Contrast = \sum |i,j|^2 O(i,j) \tag{21}$$

Here, $O(i,j)$ denotes the pixel positions within the gray-level co-occurrence matrix (GLCM). The detailed contrast analysis, presented in Table 9, shows the exceptional performance of the proposed algorithm in contrast to existing encryption schemes.

TABLE 9: Contrast analysis

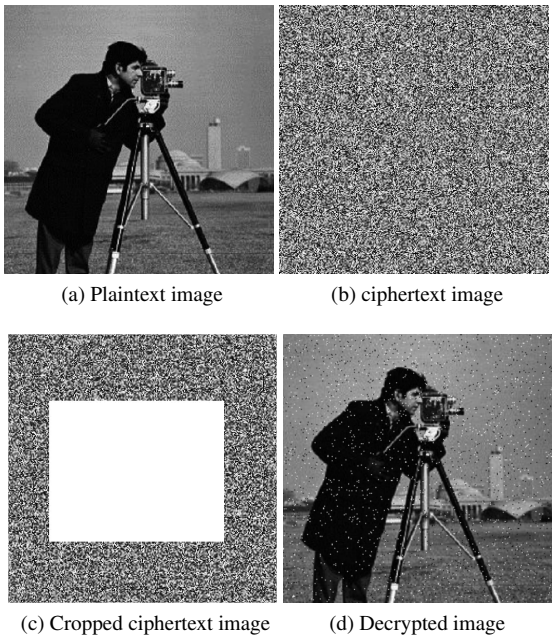
Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
Proposed	10.96	10.15	10.77	10.63	10.64
BPCPD [5]	9.34	9.32	9.96	9.96	9.98
Ref [66]	9.59	9.29	9.49	9.80	9.87
Ref [67]	9.86	9.70	9.90	9.91	9.82
Ref [68]	9.84	9.92	9.80	9.97	9.95
Ref [53]	9.8941	9.9880	9.8910	9.8920	9.9911
Ref [54]	9.9746	9.7692	9.8740	9.8601	9.9880
Ref [57]	9.9834	9.8864	9.9957	9.8743	9.8691

M. ANALYSIS OF IMAGE CROPPING ATTACK

During image transmission, there is a possibility for attackers to crop the image, potentially leading to the compromise of the plaintext information. To evaluate how well the suggested method withstands cropping attacks, a portion of the ciphertext image is removed, as depicted in Figure 9(a). The cropped image is then decrypted, and an analysis is conducted to determine the algorithm's ability to retrieve the plaintext information. The results demonstrate that even when the attacker has cropped the encrypted image, the proposed algorithm can effectively decrypt the original image with negligible loss of information. This cropping attack analysis is visually illustrated in Figure 9, where Figure 9(b) displays the decrypted image recovered from the cropped encrypted version. This demonstrates the capability to withstand the proposed encryption scheme against cropping attacks.

N. ANALYSIS OF NOISE-BASED ATTACK

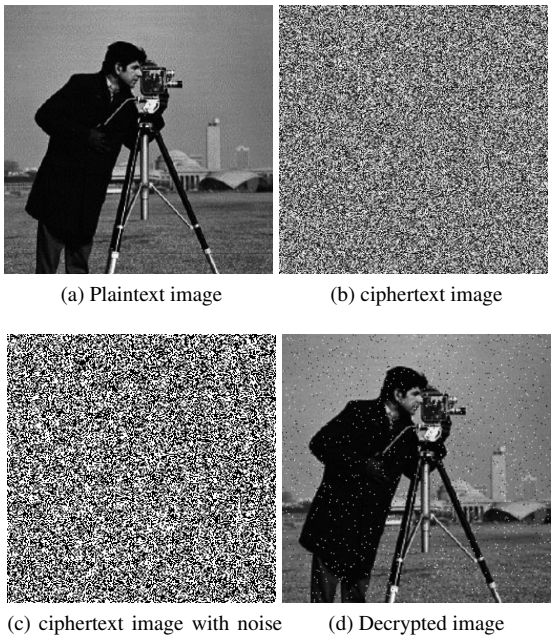
Noise-based attacks can take several forms, including salt (S) and pepper (P) noise. Noise-based attacks aim to exploit vulnerabilities in the encryption scheme by analyzing how the encryption process reacts to the introduction of noise. The attacker's goal may be to recover the original image, reveal sensitive information, or detect weaknesses in the encryption algorithm. Equation 22 shows the induction of noise in an encrypted image ($E(i,j)$).



(a) Plaintext image (b) ciphertext image

(c) Cropped ciphertext image (d) Decrypted image

FIGURE 9: Analysis of image cropping attack



(a) Plaintext image (b) ciphertext image

(c) ciphertext image with noise image (d) Decrypted image

FIGURE 10: Analysis of noise-based attack

$$\text{Noise encrypted image}(N_{im}) = S + P + E(i,j) \quad (22)$$

In the enciphered image E, noise in the form of salt (S) and pepper (P) is introduced at the pixel position i, j. Following the incorporation of noise into the ciphertext image, the proposed decryption algorithm is executed. The results reveal that the decrypted image preserves the information, as evident in Figure 10. Despite some minor noise in the decrypted image, there is virtually a very minor perceptible distinction between the original and ciphertext images.

TABLE 10: Computational complexity analysis

Encryption schemes ↓	Camera-man	Lina	Baboon	Boat	House
Proposed	0.004	0.002	0.003	0.005	0.004
BPCPD [5]	0.387	0.777	0.557	0.906	0.803
Ref [66]	1.481	0.469	0.231	0.769	0.764
Ref [67]	2.8810	0.631	0.427	0.917	0.751
Ref [68]	3.961	0.718	0.797	0.814	0.727
Ref [53]	2.7192	0.8812	0.3187	0.7278	0.8949
Ref [54]	2.7213	0.6913	0.7075	0.7960	0.7036
Ref [57]	1.9864	1.9966	2.0198	2.1312	1.9983

O. COMPUTATIONAL COMPLEXITY ANALYSIS

Apart from security evaluation, time analysis serves as a crucial criterion in assessing the performance of an encryption algorithm. To analyze encryption computations, the built-in MATLAB command "tic toc" is utilized to measure processing time for both encryption and decryption stages. The computational complexity assessment is carried out using identical platforms for both the proposed and existing methods. The processing times for these schemes are presented in Table 10. The data in Table 10 demonstrates the superiority of the proposed approach over existing encryption methods in terms of computational complexity.

P. CIPHERTEXT ONLY ATTACK

In this type of attack, attempting a decryption attack, where the attacker only possesses the ciphertext image without insights into the encryption algorithm employed, becomes notably formidable. The decryption of the original plaintext image becomes arduous under such circumstances. The proposed cryptosystem leverages a robust confusion-diffusion mechanism to generate the ciphertext image. This mechanism is realized through a fusion of operations including bit-plane extraction, XOR operations, substitution techniques, and intricate permutation processes. An analysis of statistical analysis, including contrast, correlation, energy, and entropy, highlights the substantial challenge of reconstructing the original image only from its ciphertext. As a result, the efficiency of the proposed encryption scheme significantly prevents the feasibility of carrying out such an attack.

Q. KNOWN PLAINTEXT ATTACK

In this scenario, the attackers possess a limited number of plaintext-ciphertext pairs. Using this knowledge, they attempt to deduce the secret keys employed within the cryptosystem, aiming to reconstruct the plaintext message accurately. Demonstrating the strength of the proposed cryptosystem against this attack necessitates a comprehensive analysis of the key space. The results of this key-space analysis highlight the challenge of determining the correct encryption keys within a reasonable timeframe. Therefore,

the proposed framework for securing digital data effectively counters known plaintext attacks.

R. CHOSEN PLAINTEXT ATTACK

For potential attackers or cryptanalysts to effectively carry out this attack, they would be required to encrypt numerous plaintext images using the encryption algorithm to uncover the confidential keys. Delving into a key-sensitivity examination brings to light the remarkable sensitivity of the secret keys employed within the proposed cryptosystem. Even a slight modification can lead to a significant deviation in the decrypted output. As a result of this enlarging key sensitivity, the proposed scheme effectively thwarts the feasibility of such an attack.

S. CHOSEN CIPHERTEXT ATTACK

In this type of attack, the attackers hold separate ciphertext images with the intention of deciphering them via the decryption process. The underlying goal of this attack is to uncover the secret keys employed in encrypting meaningful information. Notably, the random sequences integrated into the proposed methodology stem from seed values of the chaotic maps. Conducting a detailed assessment via key-sensitivity analysis emphasizes the high sensitivity of these conditions. Consequently, the proposed approach, fortified by this analysis, is designed to withstand a chosen ciphertext attack.

VII. DISCUSSION AND CONCLUSION

Numerous cryptosystems have emerged in recent years, varying in their robustness and suitability for real-time applications based on computational time. The balance between robust security and low-time complexity is an ongoing consideration, prompting researchers to devise encryption methods that address this trade-off. For instance, the BPCPD scheme, built on binary plane extraction and chaos, aimed to provide a high level of security with reduced computational time. However, while BPCPD presented a fast encryption algorithm, its security was significantly compromised.

For instance, Wen et al. conducted a thorough cryptanalysis of BPCPD, revealing that the security of the scheme could be compromised with just a chosen-plaintext attack. Their cryptanalysis yielded valuable suggestions to enhance the BPCPD scheme. Building on these recommendations, this paper introduces an extended version of BPCPD. The proposed enhanced cryptosystem integrates bit-plane extraction, multiple chaotic maps, such as chaotic Arnold and chaotic CAT maps, as well as a permutation-diffusion structure. In the permutation phase, a combination of methodologies—multi-layer permutation, multi-round permutation, and recursive permutation—is implemented to heighten complexity and render decryption nearly unfeasible for attackers. Moreover, in the diffusion phase, instead of only relying on the XOR operation as used in BPCPD, a substitution operation is integrated with XOR to create diffusion within the image. The efficiency of the proposed encryption scheme is gauged through multiple experimental analyses and comparisons with BPCPD and other encryption methods, ensuring its superiority. Furthermore, the proposed encryption cryptosystem not only offers enhanced security for digital images but also proves suitable for real-time applications by achieving fast image encryption. We acknowledge Heping Wen for the valuable suggestions provided.

In the future, the integration of quantum encryption will enhance the proposed scheme's robustness. In addition, the incorporation of frequency domain encryption holds the potential to reduce computational complexity.

FUNDING STATEMENT

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RG23052).

ACKNOWLEDGEMENT

The authors extend their appreciation to the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) for funding this work through Research Group grant number IMSIU-RG23052.

REFERENCES

[1] D. B. Rawat, R. Doku, and M. Garuba, "Cybersecurity in big data era: From securing big data to data-driven security," IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 2055–2072, 2019.

[2] P. N. Lone, D. Singh, and U. H. Mir, "Image encryption using dna coding and three-dimensional chaotic systems," Multimedia tools and Applications, vol. 81, no. 4, pp. 5669–5693, 2022.

[3] 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, p. 111989, 2022.

[4] A. Paul, S. Kandar, and B. C. Dhara, "Image encryption using permutation generated by modified regula-falsi method," Applied Intelligence, vol. 52, no. 10, pp. 10979–10998, 2022.

[5] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," The European Physical Journal Plus, vol. 133, no. 8, p. 331, 2018.

[6] O. Kuchai, K. Skyba, A. Demchenko, N. Savchenko, Y. Necheporuk, and O. Rezvan, "The importance of multimedia education in the informatization of society," IJCSNS, vol. 797, 2022.

[7] D. K. Citron, The fight for privacy: Protecting dignity, identity and love in the digital age. Random House, 2022.

[8] P. M. Rao and B. Deebak, "Security and privacy issues in smart cities/industries: technologies, applications, and challenges," Journal of Ambient Intelligence and Humanized Computing, pp. 1–37, 2022.

[9] A. Al-Hyari, I. Al-Taharwa, B. Al-Ahmad, Z. Alqadi, et al., "Casdc: A cryptographically secure data system based on two private key images," IEEE Access, vol. 10, pp. 126304–126314, 2022.

[10] S. Nooh, "Combining encryption and preservation in information security to secure sending a message," International Journal of Computer Science & Network Security, vol. 22, no. 4, pp. 285–291, 2022.

[11] M. U. Rehman, A. Shafique, Y. Y. Ghadi, W. Boulila, S. U. Jan, T. R. Gadekallu, M. Driss, and J. Ahmad, "A novel chaos-based privacy-preserving deep learning model for cancer diagnosis," IEEE Transactions on Network Science and Engineering, vol. 9, no. 6, pp. 4322–4337, 2022.

[12] F. Yu, S. Qian, X. Chen, Y. Huang, S. Cai, J. Jin, and S. Du, "Chaos-based engineering applications with a 6d memristive multistable hyperchaotic system and a 2d sf-simm hyperchaotic map," Complexity, vol. 2021, pp. 1–21, 2021.

[13] J. Yu, W. Xie, Z. Zhong, and H. Wang, "Image encryption algorithm based on hyperchaotic system and a new dna sequence operation," Chaos, Solitons & Fractals, vol. 162, p. 112456, 2022.

[14] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey," Computer Science Review, vol. 47, p. 100530, 2023.

[15] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A technique for digital steganography using chaotic maps," Nonlinear Dynamics, vol. 75, pp. 807–816, 2014.

[16] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 9, pp. 3106–3118, 2014.

[17] A. Shafique, "A noise-tolerant cryptosystem based on the decomposition of bit-planes and the analysis of chaotic gauss iterated map," Neural Computing and Applications, vol. 34, no. 19, pp. 16805–16828, 2022.

[18] D. J. S. Manoharan, "A novel user layer cloud security model based on chaotic arnold transformation using fingerprint biometric traits," Journal of Innovative Image Processing, vol. 3, no. 1, pp. 36–51, 2021.

[19] L. Zhu, W. Li, L. Liao, and H. Li, "A novel algorithm for scrambling digital image based on cat chaotic mapping," in 2006 International Conference on Intelligent Information Hiding and Multimedia, pp. 601–604, IEEE, 2006.

[20] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, "Enhancing image encryption with the kronecker xor product, the hill cipher, and the sigmoid logistic map," Applied Sciences, vol. 13, no. 6, p. 4034, 2023.

[21] Z. Tang and X. Zhang, "Secure image encryption without size limitation using arnold transform and random strategies," Journal of multimedia, vol. 6, no. 2, p. 202, 2011.

[22] Z. Tang, X. Lu, and W. Wei, "Image scrambling based on bit shuffling of pixels," Journal of Optoelectronics Laser, vol. 18, no. 12, p. 1486, 2007.

[23] K. Martin, R. Lukac, and K. N. Plataniotis, "Efficient encryption of wavelet-based coded color images," Pattern Recognition, vol. 38, no. 7, pp. 1111–1115, 2005.

[24] D. Vignesh, N. A. A. Fataf, and S. Banerjee, "A novel fractional sine chaotic map and its application to image encryption and watermarking," Applied Sciences, vol. 13, no. 11, p. 6556, 2023.

[25] Q.-H. Lin, F.-L. Yin, T.-M. Mei, and H. Liang, "A blind source separation-based method for multiple images encryption," Image and Vision Computing, vol. 26, no. 6, pp. 788–798, 2008.

[26] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," Computers & Mathematics with Applications, vol. 59, no. 10, pp. 3320–3327, 2010.

[27] M. Akraam, T. Rashid, and S. Zafar, "An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers," Multimedia Tools and Applications, vol. 82, no. 11, pp. 16861–16879, 2023.

[28] A. A. Rashid and K. A. Hussein, "Image encryption algorithm based on the density and 6d logistic map.," International Journal of Electrical & Computer Engineering (2088-8708), vol. 13, no. 2, 2023.

[29] S. Shao, J. Li, P. Shao, and G. Xu, "Chaotic image encryption using piecewise-logistic-sine map," IEEE Access, vol. 11, pp. 27477–27488, 2023.

[30] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," Nonlinear Dynamics, vol. 62, pp. 615–621, 2010.

[31] M.-r. Jiang, X.-f. Feng, C.-p. Wang, H. Zhang, et al., "Robust color image watermarking algorithm based on synchronization correction with multi-layer perceptron and cauchy distribution model," Applied Soft Computing, vol. 140, p. 110271, 2023.

[32] P. Rashmi, M. Supriya, and Q. Hua, "Enhanced lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare," Security and Communication Networks, vol. 2022, pp. 1–9, 2022.

[33] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," Signal processing, vol. 92, no. 4, pp. 1101–1108, 2012.

[34] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics communications, vol. 284, no. 12, pp. 2775–2780, 2011.

[35] S. Yin, H. Li, L. Teng, A. A. Laghari, and V. V. Estrela, "Attribute-based multiparty searchable encryption model for privacy protection of text data," Multimedia Tools and Applications, pp. 1–22, 2023.

[36] J. Liu, J. Zhang, and S. Yin, "Hybrid chaotic system-oriented artificial fish swarm neural network for image encryption," Evolutionary Intelligence, pp. 1–11, 2021.

[37] Q. Shi, S. Yin, K. Wang, L. Teng, and H. Li, "Multichannel convolutional neural network-based fuzzy active contour model for medical image segmentation," Evolving Systems, vol. 13, no. 4, pp. 535–549, 2022.

[38] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Optics Communications, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[39] K. K. Raghuvanshi, S. Kumar, S. Kumar, and S. Kumar, "Investigation of piecewise linear chaotic map as a diffusion model for image encryption," Multimedia Tools and Applications, pp. 1–18, 2023.

[40] Q. Wang, Q. Guo, and J. Zhou, "Double image encryption based on linear blend operation and random phase encoding in fractional fourier domain," Optics Communications, vol. 285, no. 21-22, pp. 4317–4323, 2012.

[41] Y. Wang, C. Quan, and C. Tay, "Nonlinear multiple-image encryption based on mixture retrieval algorithm in fresnel domain," Optics Communications, vol. 330, pp. 91–98, 2014.

[42] H. Mahalingam, T. Veeramalai, A. R. Menon, and R. Amirtharajan, "Dual-domain image encryption in unsecure medium—a secure communication perspective," Mathematics, vol. 11, no. 2, p. 457, 2023.

[43] A. Shafique and F. Ahmed, "Image encryption using dynamic s-box substitution in the wavelet domain," Wireless Personal Communications, vol. 115, pp. 2243–2268, 2020.

[44] P. Ping, F. Xu, and Z.-J. Wang, "Image encryption based on non-affine and balanced cellular automata," Signal Processing, vol. 105, pp. 419–429, 2014.

[45] W. Lv, J. Chen, X. Chai, and C. Fu, "A robustness-improved image encryption scheme utilizing life-liked cellular automaton," Nonlinear Dynamics, vol. 111, no. 4, pp. 3887–3907, 2023.

[46] D. R. I. M. Setiadi and N. Rijati, "An image encryption scheme combining 2d cascaded logistic map and permutation-substitution operations," Computation, vol. 11, no. 9, p. 178, 2023.

[47] E. Winarno, K. Nugroho, P. W. Adi, et al., "Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system," IEEE Access, 2023.

[48] E. Winarno, K. Nugroho, P. W. Adi, et al., "Integrated dual hyperchaotic and josephus traversing based 3d confusion-diffusion pattern for image encryption," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 9, p. 101790, 2023.

[49] X.-Y. Wang, S.-X. Gu, and Y.-Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," Optics and Lasers in Engineering, vol. 68, pp. 126–134, 2015.

[50] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," Optics and Lasers in Engineering, vol. 71, pp. 33–41, 2015.

[51] T. A. Dhopavkar, S. K. Nayak, and S. Roy, "Ietd: a novel image encryption technique using tinkerbell map and duffing map for iot applications," Multimedia Tools and Applications, vol. 81, no. 30, pp. 43189–43228, 2022.

[52] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," Multimedia tools and applications, vol. 74, pp. 5429–5448, 2015.

[53] X. Wang, M. Zhao, S. Feng, and X. Chen, "An image encryption scheme using bit-plane cross-diffusion and spatiotemporal chaos system with nonlinear perturbation," Soft Computing, vol. 27, no. 3, pp. 1223–1240, 2023.

[54] C. Xu, J. Sun, and C. Wang, "A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems," Multimedia Tools and Applications, vol. 79, no. 9-10, pp. 5573–5593, 2020.

[55] B. M. P. Waseso and N. A. Setiyanto, "Web phishing classification using combined machine learning methods," Journal of Computing Theories and Applications, vol. 1, no. 1, pp. 11–18, 2023.

[56] A. A. Ojugo, M. I. Akazue, P. O. Ejeh, N. C. Ashioba, C. C. Odiakaose, R. E. Ako, and F. U. Emordi, "Forging a user-trust memetic modular neural network card fraud detection ensemble: A pilot study," Journal of Computing Theories and Applications, vol. 1, no. 2, pp. 1–11, 2023.

[57] X. Liu, D. Xiao, and C. Liu, "Quantum image encryption algorithm based on bit-plane permutation and sine logistic map," Quantum Information Processing, vol. 19, pp. 1–23, 2020.

[58] Z.-h. Gan, X.-l. Chai, D.-j. Han, and Y.-r. Chen, "A chaotic image encryption algorithm based on 3-d bit-plane permutation," Neural Computing and Applications, vol. 31, pp. 7111–7130, 2019.

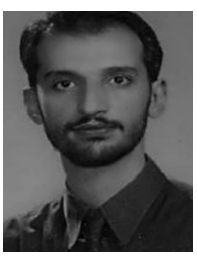
[59] P. Kumar, M. Rahman, S. Namasudra, and N. R. Moparthi, "Enhancing security of medical images using deep learning, chaotic map, and hash table," Mobile Networks and Applications, pp. 1–15, 2023.

[60] R. Chakraborty, G. Verma, and S. Namasudra, "Ifodpso-based multi-level image segmentation scheme aided with masi entropy," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 7793–7811, 2021.

[61] Y. Deng, Z. Zeng, K. Jha, and D. Huang, "Problem-based cybersecurity lab with knowledge graph as guidance," Journal of Artificial Intelligence and Technology, 2021.
[62] M. K. Hooshmand and D. Hosahalli, "Network anomaly detection using deep learning techniques," CAAI Transactions on Intelligence Technology, vol. 7, no. 2, pp. 228–243, 2022.
[63] M. Sahu, N. Padhy, S. S. Gantayat, and A. K. Sahu, "Local binary pattern-based reversible data hiding," CAAI Transactions on Intelligence Technology, vol. 7, no. 4, pp. 695–709, 2022.
[64] M. Zheng, K. Zhi, J. Zeng, C. Tian, and L. You, "A hybrid cnn for image denoising," Journal of Artificial Intelligence and Technology, vol. 2, no. 3, pp. 93–99, 2022.
[65] S. Scherrer and A. Perrig, "Security, anonymity, privacy, and trust," Future Networks, Services and Management: Underlay and Overlay, Edge, Applications, Slicing, Cloud, Space, AI/ML, and Quantum Computing, pp. 367–381, 2021.
[66] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," IEEE Access, vol. 9, pp. 59108–59130, 2021.
[67] H. Chang, E. Wang, and J. Liu, "A novel chaotic image encryption algorithm based on propositional logic coding," International Journal of Bifurcation and Chaos, vol. 33, no. 08, p. 2350089, 2023.
[68] D. Sravanthi, K. Abhimanyu Kumar Patro, B. Acharya, and S. Majumder, "A secure chaotic image encryption based on bit-plane operation," in Soft Computing in Data Analytics: Proceedings of International Conference on SCDA 2018, pp. 717–726, Springer, 2019.
[69] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," International journal of bifurcation and chaos, vol. 16, no. 08, pp. 2129–2151, 2006.
[70] S.-I. Pae, "Binarization trees and random number generation," IEEE Transactions on Information Theory, vol. 66, no. 4, pp. 2581–2587, 2019.
[71] C. Wolf and D. Doermann, "Binarization of low quality text using a markov random field model," in 2002 International Conference on Pattern Recognition, vol. 3, pp. 160–163, IEEE, 2002.
[72] D. Xu and D. E. Tamir, "Pseudo-random number generators based on the collatz conjecture," International Journal of Information Technology, vol. 11, no. 3, pp. 453–459, 2019.
[73] K. Marton and A. Suciu, "On the interpretation of results from the nist statistical test suite," Science and Technology, vol. 18, no. 1, pp. 18–32, 2015.
[74] Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," Physical Review X, vol. 6, no. 1, p. 011020, 2016.
[75] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," Signal Processing, vol. 167, p. 107280, 2020.
[76] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems s-boxes and their applications," Chinese Journal of Physics, vol. 56, no. 4, pp. 1609–1621, 2018.
[77] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," Entropy, vol. 23, no. 3, p. 341, 2021.
[78] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic s-boxes based on mobius transformation and chaotic tent-sine system," IEEE Access, vol. 7, pp. 173273–173285, 2019.
[79] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," Multimedia Tools and Applications, vol. 81, no. 18, pp. 25497–25518, 2022.

MUJEEB UR REHMAN received the Ph.D. degree with distinction (AI and Cybersecurity) in 2022. He is currently a Lecturer with the Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, UK. He is also a Professional Engineer.He has numerous high-impact factor publications, including contributions to prestigious transactions within his area of expertise. His research interests include artificial intelligence, Cybersecurity, non-invasive health care, the Internet of Things (IoT), and multimedia encryption.

ARSLAN SHAFIQUE currently serves as a Researcher at University of Glasgow, United Kingdom. He earned Ph.D. from Riphah International University in Pakistan. He has more than 20 high-impact factor publications, including contributions to prestigious transactions within his area of expertise. Arslan's research encompasses a wide range of topics, including cybersecurity, machine learning, artificial intelligence, and the Internet of Things (IoT).



KAHIF HESHAM KHAN received the B.S. and M.S. degrees (Hons.) in computer science from the COMSATS Institute of Information Technology (CIIT), in 2008 and 2010, respectively, and the Ph.D. degree in industrial process from the Royal Melbourne Institute of Technology, Melbourne, Australia. His M.S. thesis concentrated on enhancing grid-scheduling approaches for data-parallel applications in the context of industrial and sustainable buildings. He is currently with RMIT University, Deakin University, and Federation University, Australia. His research interests include cyber security, image processing, and machine learning.

MALAK OLAMAIE is a theoretical astrophysicist and my research is in the area of cosmology and studying clusters of galaxies using fully Bayesian approach. She studied Physics with theoretical astrophysics at the University of Nottingham under the supervision of Professor Peter Coles. After graduation in 2008, she started a doctorate in the astrophysics group at Cavendish Laboratory in Cambridge under the supervision of Professor Mike Hobson and Professor Keith Grainge specializing in constraining physical properties of galaxy clusters using multi-waveband observations of clusters of galaxies. After completing her Ph.D. in 2012, she was awarded a John & Delia Agar research fellowship in science and engineering at Sidney Sussex College, University of Cambridge to continue my research. She then moved to Imperial College, London as a postdoctoral research fellow to work on developing Bayesian Hierarchical models to analyze data from large-scale structures of the Universe. In July 2019, she was appointed as a senior lecturer in Bayesian Data Science at York St. John University, a position I currently hold.

DR. SAAD NASSER ALTAMIMI , Assistant Professor at the Department of Information Systems, Imam Mohammad Bin Saud Islamic University, KSA. brings profound expertise to the field of information security. Holding a Ph.D. in Cybersecurity from the University of Glasgow, UK, his focus includes end user behavioral security, InfoSec Awareness and Compliance, Privacy, and IoT Security. His contributions play a pivotal role in enhancing digital safeguarding.

SULTAN NOUMAN QASEM received the B.Sc. degree (Hons.) from the Computer Science Department, Faculty of Science, Al-Mustansiriya University, Baghdad, Iraq, in 2002, and the M.Sc. and Ph.D. degrees from the Faculty of Computer Science and Information Systems, University Technology Malaysia, Johor, Malaysia, in 2008 and 2011, respectively. He is currently an Associate Professor with the Department of Computer Science, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University. He has authored/co-authored more than 55 research publications in peer-reviewed reputed journals, book chapters, and conference proceedings. His research interests include, applied artificial intelligence, data science, multi-objective machine learning, object recognition, and health informatics. He has served as the program committee member for various international conferences and a reviewer for various international journals.

MUHAMMED AL-SAREM received the M.S. degree in information technology from the Faculty of Informatics and Computer Engineering, Volgograd State Technical University, Volgograd, Russia, and the Ph.D. degree from the Faculty of Informatics, University of Hassan II Casablanca, Mohammedia, Morocco, in 2007 and 2014, respectively. He is currently an Assistant Professor with the IS Department, Taibah University, Medina, Saudi Arabia. He has published several papers and participated in managing several international conferences. His current research interests include group decision making, multicriteria decision making, data mining, E-learning, natural language processing, and social analysis.