Hindawi
Security and Communication Networks
Volume 2022, Article ID 5680357, 16 pages
https://doi.org/10.1155/2022/5680357

Research Article

An Efficient Lightweight Image Encryption Scheme Using Multichaos

Asad Ullah,[1] Awais Aziz Shah,[1,2] Jan Sher Khan,[3] Mazhar Sajjad,[4] Wadii Boulila,[5,6] Akif Akgul,[7] Junaid Masood,[8] Fuad A. Ghaleb,[9,10] Syed Aziz Shah,[10] and Jawad Ahmad[11]

[1]*School of Computing, Engineering and Physical Sciences, University of the West of Scotland, Paisely PA12BE, UK*
[2]*Department of Electrical and Informational Engineering (DEI), Polytechnic University of Bari, Bari, Italy*
[3]*Department of Electrical and Electronics Engineering, University of Gaziantep, Gaziantep, Turkey*
[4]*Department of Computer Science, Comsats University, Islamabad 45550, Pakistan*
[5]*RIADI Laboratory, University of Manouba, Manouba, Tunisia*
[6]*Robotics and Internet of Things Laboratory, Prince Sultan University, Riyadh 12435, Saudi Arabia*
[7]*Department of Computer Engineering, Faculty of Engineering, Hitit University, Corum 19030, Turkey*
[8]*Department of Computer Science, IQRA National University, Peshawar, Pakistan*
[9]*Department of Computer and Electronic Engineering, Sana'a Community College, Sana'a, Yemen*
[10]*School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia*
[11]*Research Centre for Intelligent Healthcare, Coventry University, Coventry, UK*

Correspondence should be addressed to Fuad A. Ghaleb; fuadeng@gmail.com

Received 28 July 2021; Revised 18 August 2021; Accepted 27 July 2022; Published 14 October 2022

Academic Editor: Farhan Ullah

With an immense increase in Internet multimedia applications over the past few years, digital content such as digital images are stored and shared over global networks, the probability for information leakage and illegal modifications to the digital content is at high risk. These digital images are transferred using the network bandwidth; therefore, secure encryption schemes facilitate both information security and bandwidth issues. Hence, a state-of-the-art lightweight information security methodology is required to address this challenge. The main objective of this work is to develop a lightweight nonlinear mechanism for digital image security using chaos theory. The proposed scheme starts by changing a plain image into an encrypted image to improve its security. A block cipher, using lightweight chaos, has been added to achieve this objective for digital image security. We utilized multiple chaotic maps to generate random keys for each channel. Also, Arnold cat map and chaotic gingerbread map are used to add confusion and diffusion. During the permutation stage, image pixels are permuted, while in diffusion stage, pixels are distorted utilizing gingerbread map to add more security. The proposed scheme has been validated using different security parameter tests such as correlation coefficient tests (CC), whose results have been observed closer to zero and information entropy (IE) value is 7.99, respectively, which is almost equal to the ideal value of 8. Moreover, number of pixels changing rate (NPCR) obtained value is higher than 99.50%, while the unified average changing intensity (UACI) is 33.33. Other parameters such as mean absolute error (MAE), mean square error (MSE), lower value of peak to signal noise ratio (PSNR), structural content (SC), maximum difference (MD), average difference (AD), normalized cross-correlation (NCC), and histogram analysis (HA) is tested. The computed values of the proposed scheme are better. The achieved results after comparison with existing schemes highlight that the proposed scheme is highly secure, lightweight, and feasible for real-time communications.

1. Introduction

There has been a rapid growth in the computers, Internet, social media, and communications during the last decade. The information revolution consists of digital media transmitted from billions of users and devices globally using network bandwidth. This increase in digital media transmission poses numerous challenges in terms of privacy and security as hacking incidents have occurred in the last decade that consists of hacking the content for information leakage and modifications [1–4]. More recently, numerous cryptographic methods have been proposed to enable secure image encryption. However, these methods often have an ordinary structure that performs the permutation and diffusion stages of decryption. Most of these algorithms deal with issues such as lack of robustness and security. Additionally, these encryption techniques were unsuitable for images with certain features, i.e., huge capacity, high redundancy, and high correlation among pixels. In addition to these characteristics, images also tend to be much larger than other media that might require decryption. These encryption plans require additional operations on compressed image data, demanding long computational time and high computing power. This translates to low encryption and decryption speeds in real-time communications, and images may present significant latency [5, 6].

With recent advancements in social media platforms, many images are transmitted over the web daily. Securing such images against unauthorized access becomes considerably more critical for authorized people and various fields to confront their unique security issues. Biology, military sciences, banking, and online shopping are just a few fields to name. In these cases, information transmitted as or via images is very different from information transmitted as or via text [7]. Images deal with greater data redundancy and more excellent information coverage while having a higher correlation between adjacent pixels. They also require real-time and robust security for communication purpose. Thus, numerous techniques are used to secure confidential image data transmitted over an insecure channel [8–12]. Data sharing is increased using social networks that are expanding in size and traffic, which has altered the underlying infrastructure of communication.

Today, much effort and research have created a complicated and robust cryptosystem providing the best possible security. Such a system uses several highly desired cryptographic properties, such as randomness, ergodicity, and sensitivity to original values [8].

As technology's scope ascends, new methods are developed, including special techniques such as deoxyribonucleic acid (DNA) coding [13], quantum theory, compression, and chaos theory. Though all of these have their advantages, chaos theory, in particular, has played a critical role in encryption research over the last 20 years [14–17]. By definition, the chaos theory uses mathematics and physics to deal with the behavior of NLDSs, i.e., nonlinear dynamical systems. The typical characteristics of chaotic systems are ergodicity, unpredictability, and initial value sensitivity. One advantage of employing chaos-based image encryption is that it offers higher security even though the mathematical complexity involved is much lower [18]. However, such systems' narrow and discontinuous range causes massive differences in chaotic properties due to minor disturbances such as noise factors. Two major factors that controls the performance of chaos-based encryption algorithms for imaging. The first such factor is based upon the robustness of the encryption algorithm against cryptanalysis. The second factor is based upon the real-time performance of chaotic maps. If the obtained performance is lower, this means that the achieved security robustness and efficiency of chaotic maps is lower. When both these factors are combined to attempt better results, many new challenges and difficulties also arise. So, their balance is essential in this regard.

This paper presents an efficient and lightweight image encryption technique based on multiple chaos algorithms. The work includes designing a novel and efficient information safety scheme based on various chaotic maps. Numerous encryption techniques are proposed and analyzed for their computational speed, reliability, robustness, and nonlinearity, which has been found exceptional. Our primary research objective is to achieve a high level of security. The security of a given system depends upon ensuring its cryptographic services. Several services of protection are provided by the International Telecommunication and Union's Telecommunication Standardization. We investigate the chaotic properties, including topology mixing, strange attractor, ergodicity, randomness, and dependence on its initial condition. After that, we evaluated the proposed cryptosystem using different tests, such as histogram analysis (HA), correlation coefficient (CC), the mean absolute error (MAE), differential attacks analysis (DAA), number of pixels changing rate (NPCR), unified average changing intensity (UACI), the mean square error (MSE), peak to signal noise ratio (PSNR), information entropy (IE), structural content (SC), normalized cross-correlation (NCC), maximum difference (MD), and average difference (AD). The comparison of proposed algorithms results in existing algorithms for all tests. The results highlight that calculated CC value is closer to zero, and IE value is 7.99, respectively, which is almost equal to the ideal value of 8. Moreover, NPCR is higher than 99.50%, while the UACI is 33.33. Other parameters such as MAE, MSE, lower value of PSNR, SC, MD, AD, and NCC showed better result in the proposed scheme. The offered scheme is compared to the existing schemes. It is concluded that the proposed scheme is highly secure, lightweight, and feasible for real-time communications.

The rest of the article has been organized as follows: Section 2 gives an overview and relation between chaos and cryptography, Section 3 deeply describes the proposed methodology of the lightweight image encryption scheme. The statistical analysis and experimental results are discussed in Section 4 and finally, Section 5 concludes the paper.

2. Chaos and Cryptography

It has been made clear that data transmitted over any public network is susceptible to malicious attacks and might become a target to be a break. For the sole purpose of protecting communications in general, several encryption techniques have been suggested. This has emphasized dynamic cryptosystems, such as chaos systems, that transmit plain data into unintelligible cipher data. Sensitivity is one of the unique features of such systems, i.e., any minor change in the original condition will result in drastically random output formulas such as the Lyapunov exponent help calculate the parameters of a map. Randomness, initial sensitivity, and periodicity are more beneficial properties that cryptographer use to design well-built cryptographic algorithms that provide security against unauthorized users. Among these systems, chaotic systems stand out due to their random output and other unique features [19]. As chaotic systems can perform without any dependence on parameters [19], they demonstrate in-determinism, thus helping other creators to design better algorithms. A chaotic output can be determined using its initial values for the system, making the chaotic more deterministic. When combined, these features help to diversify cryptosystems meticulously. When equipped with diffusion and confusion, a nonlinear system can effectively encounter cryptanalysis. Due to this robust infrastructure involved in chaotic cryptosystems, these processes are now being employed in other fields such as biological sciences, chemistry, and physics to build a new set of hybrid systems to achieve better security. Figure 1 illustrates the basic schematic chart of chaos-based encryption schemes.

In an NLDS, i.e., a nonlinear dynamical system, initial conditions significantly impact chaos, which seems to work upon and show pseudo-random behavior. Consider the stability of the system as an essential parameter when considering Lyapunov exponents. When the observer is aware of the system's initial conditions, the observer seems to understand the system output. However, if the preliminary requirements are unknown, the overall production seems to be highly erratic and random. When the source owner knows the pseudo-random order of the data, then the plain text can be easily substituted and diffused to be protected against malicious attacks and invasion. Several data formats can also be utilized in telecommunication channels that require protection.

2.1. Fundamental Properties of Chaotic System. Many technical and industrial areas within natural structures witness the chaos. These areas often exhibit well-defined possessions marking them as complicated and highly volatile. The chaos theory is concerned with situations that move through time toward a specific type of dynamic action. Multiple authors across various fields have discussed the chaos theory's mathematical background due to its wide variety of applications. In broad terms, some specific procedures are followed by these schemes for improvement. Individual nonlinear deterministic systems are usually potential sources of chaos. A long-term progression that is continuous, erratic, and fulfills mathematical benchmarks will display chaos phenomena. The features of a chaotic system can be described as a set of properties that measure mathematical principles that are used to describe chaos. The most notable of these characteristics include the following:

(1) Nonlinearity: The output is changed unproportionally concerning input.

(2) Deterministic: Every state of the system must follow some deterministic fundamental rules.

(3) Sensitivity to initial conditions: Slight deviation in its early state can lead to a dissimilar performance in its last state.

(4) Continued irregularity in the system's actions: The framework of chaotic systems is based upon a secret order combined with an infinite number of unstable random designs. This unseen direction forms the structure of irregular, chaotic systems.

(5) Long-term prediction: It can only be comprehended with limited accuracy as chaos is sensitive to the initial state.

2.2. Elementary Possessions of Chaotic Systems. Chaos has been measured in various laboratories, and natural systems [20, 21], covering many engineering and scientific areas, including fields such as biology, physics, ecology, meteorology, economics, and computer science, among others. All the techniques above provide valuable assets, which create certain unpredictability and a complex system. Systems that display such erratic and dynamic behavior over time are explained by chaos theory. For a broader overview, the concerned reader is directed to (Robinson, 1995). Generally, these systems are deterministic, and they follow a specific set of laws of evolution. Unfortunately, it must be said that chaos only occurs in a certain deterministic NLDS (nonregular linear dynamic systems). The most relevant of these criteria are dynamic instability, topological mixing, aperiodicity, and ergodicity:

Now let us examine the interaction and connection of chaos with cryptography properties of diffusion and confusion (Shannon, 1949). Suggesting to review chaotic systems features, like ergodicity, topology mixing property, and auto-similarity that are directly connected to the confusion phase of chaotic systems. The dynamics, or dynamical behavior in the chaotic output attractor, is concerned with nonperiodic orbits that produce identical patterns. The output patterns can be utilized to mask clear messages using substitution-like techniques. On the other hand, diffusion is directly connected to the system's sensitive parameters and initial conditions. Small changes in control parameters give rise to avalanche effects and produce random outputs.

As a conclusion, it would be best to list the benefits of chaotic cryptosystems that are being used and to offer strong security in cryptography. Firstly, chaotic systems seem to happen on their own and can be used for lightweight security in cryptography. These maps may show nonlinear behaviours that are used to make communication more secure. These systems have the advantage of having simple,

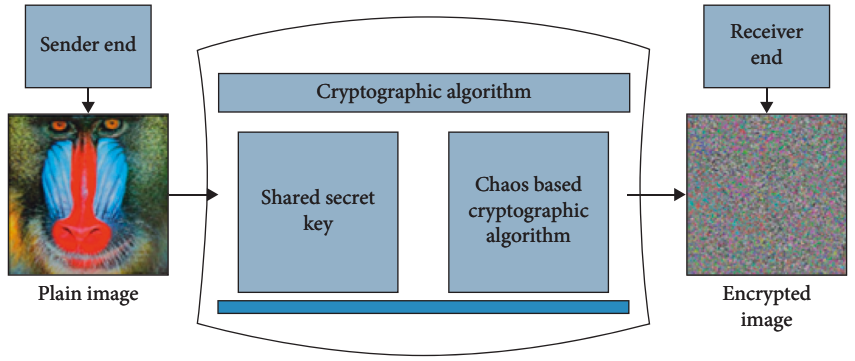

Figure 1: Basic schematic chart of chaos-based encryption process.

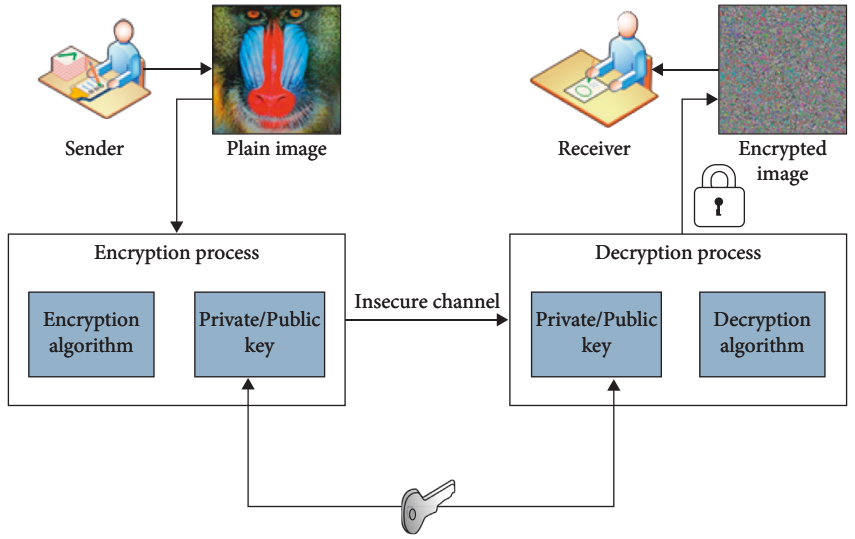

Figure 2: The process of encryption and decryption.

deterministic algorithms that are easy to use. Three basic ideas can be used to build a security infrastructure: confidentiality, integrity, and authentication. Confidentiality means that only people who are allowed to can see the data and people who are not should not. Integrity makes sure that the information available has not been changed. Availability means that there are resources that can be used.

3. The Proposed Methodology of Lightweight Image Encryption Scheme

Figure 2 shows the general process of encryption and decryption. Lightweight cryptosystems that operate based on chaos principles are designed by utilizing confusion and diffusion characteristics noted by Claude Shannon [22], as discussed earlier in Section 2. Such lightweight encryption systems work by using several chaotic maps to build hybrid systems that bring together several initial systems' best characteristics. The suggested method is then subjected to robust testing parameters compared with other existing techniques to determine its efficiency and efficacy.

In this section, the design of such a cryptosystem is discussed. This discussion will include all requirements that are mandatory for creating a truly secure cryptosystem. The proposed system is then investigated using several tests to secure the image and its transmission remains. During this process, we evaluate the performance of the proposed algorithm. We have conducted statistical tests including HA, CC tests between pixels along three primary axes, i.e., horizontal, diagonal, and vertical for each channel. MSE, PSNR, IE against each channel, sensitivity analysis which interpolates NPCR, and UACI. Other tests such as an AD, MD, SC, and NCC are performed. Our experiments enabled us to instantly examine output bit pixel, input bit pixel, and their behavior after investigation. Our primary goal is to create algorithms that include confusion and diffusion (randomness) since these are two essential properties for optimal security service.

3.1. Utilized Chaotic Maps. To help develop and implement encryption algorithms, general chaotic maps will be defined and discussed.

3.1.1. Arnold Scrambling Cat Map. Arnold's method is a standard technique for scrambling an image. This method is secure because of its high computational rate and quick processing time. Moreover, this method facilitates data scrambling in an array as a data stream using a chaotic Arnold transformation. Arnold's transformation chaotic map can be defined as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod} 1, \tag{1}$$

where x and $y \in 0, 1$. The aforementioned formula of the Arnold chaotic map is for unit square and can be extended to multiple rows and columns depends upon the pixels of the image to be encrypted having a size of $N_{1(i,j)} \times N_{2(i,j)}$ In this case, then the above matrix can be extended to the finite number of pixels.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod} N, \tag{2}$$

where x and $y \in \{0, 1, 2, 3, \ldots, N-1\}$ are the original images pixels scrambled and transformed to new positions, i.e., $\{x', y'\}$.

3.1.2. Gingerbread Man Chaotic Map. The gingerbread man is a 2D chaotic map that is one of the most widely utilized choices in chaotic, random sequencing. However, it is also essential to have a robust cryptosystem to satisfy all the designed algorithm's security needs when using this option. The formula for this 2D piecewise chaotic linear map is as follows:

$$\begin{aligned} x_{n+1} &= 1 - y_n + |x_n|, \\ y_{n+1} &= x_n. \end{aligned} \tag{3}$$

3.2. Image Encryption Process

3.2.1. Steps Involved in the Process of Image Encryption. The step wise flowchart of the proposed scheme is illustrated in Figure 3. The pseudo code of the image encryption process is illustrated in Algorithm 1. Let us consider a baboon test image measuring $256 \times 256 \times 3$ pixels that will be encrypted in the following process:

(1) First, this test image is fragmented into three channels (red, green, and blue) with an image size of 256×256 pixels.

(2) To make the scheme plaintext dependent, each layer is passed through SHA-512. Then, the utilized chaotic maps such as logistic map, Gaussian map, and Chebyshev chaotic map initial conditions (keys) are computed using the calculated hash values.

(3) In this phase, the original image is permuted (confused) using 2D Arnold scrambling. The plaintext channels are permuted row- and column-wise from their initial position to the maximum iterative state.

(4) Next, two random and arbitrary chaotic matrices are generated using a gingerbread man chaotic map. These two random matrices are bitwise XORed with each other to develop diffused channels, and the resultant matrix is bitwise XORed with the red permuted channel.

(5) To make the scheme ciphertext dependent, the resultant red channel diffused channel is bitwise XORed with a green permuted channel. Their result matrix is bitwise XORed with a blue permuted channel.

(6) The multi-layered cryptosystem then produced three sets of encrypted images by applying different chaotic maps.

(7) For the final step, the cat command module is employed to combine the three encrypted channels and generate the final ciphertext image.

3.2.2. Steps Involved for Image Decryption

(1) Initially, the encrypted image is divided into its respective three parts (R, *G*, B).

(2) The green and blue cipher channels are bitwise XORed to get a blue permuted channel. Then the red and blue cipher channels are bitwise XORed to obtain a blue permuted channel.

(3) Two random matrices are generated using a gingerbread man chaotic map. These two random matrices are bitwise XORed with each other, and the resultant matrix is bitwise XORed with the red cipher channel to produce a red permuted layer.

(4) The 2D Arnold chaotic map is then used to reiterate the three different layers row- and column-wise from maximum permuted (iterated) state to the original condition.

(5) Three plain channels are recovered after employing Arnold cat scrambling for the reiteration process.

(6) The plain grey channels are combined using cat command

(7) The decrypted full-colored image is retrieved.

4. Statistical Analysis and Experimental Results

Experiments are conducted utilizing multiple plain images to demonstrate the effectiveness of the proposed scheme. A good encryption strategy should be robust to address the needs engendered by cryptanalysis, statistics, and brute force attacks, respectively. Along with these considerations, the goal is to analyze security investigations to demonstrate the effectiveness of the proposed approach against widely-recognized attacks. To illustrate the strength of our developed methodology, a statistical investigation has been conducted by creating a schematic histogram and correlating the nearby pixels in both plain and cipher images.

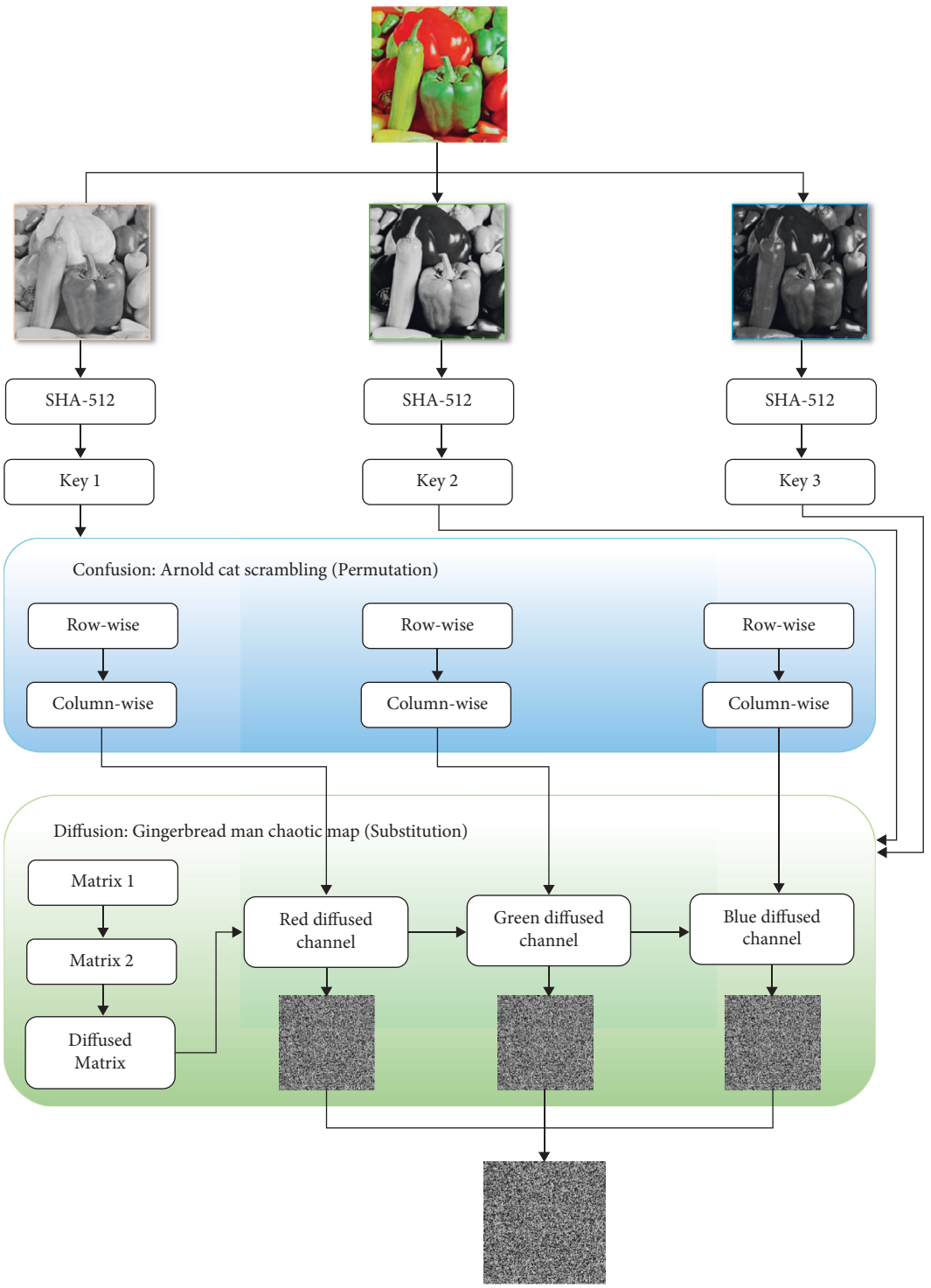

Figure 3: Flow chart of the proposed scheme.

4.1. Histogram Analysis (HA). It is widely used as a tool for analyzing the security of encrypted images. The original content in the plain image must be secure. This test explains that the grey-level pixel value should be equally distributed in its defined range depending on the image. In the cipher image, the distribution of pixels is always uniform, while in the case of a plain image, these pixels are bumpy. The bumpy pixels demonstrate that anyone can access the pixel information easily. High peaks of pixels reveal that maximum information lies at those points while low peaks indicate that minimum information lies at this point. A secure image histogram

Inputs: Plaintext image P, its row and column numbers row, col,
Outputs: Ciphertext image C
(1) for $i = 1$ *to* row
(2) for $j = 1$ to col
(3) $R, G, B \leftarrow P$
(4) Key1, Key2, Key3$\leftarrow SHA256(R, G, B)$
(5) $R, G, B \leftarrow$Row- and column −wisepermutation
(6) Permuted$(R, G, B) \leftarrow$bit − wiseXORed
(7) **Endfor**
(8) **Endfor**
(9) $C \leftarrow$Diffused(R, G, B)

Algorithm 1: Image encryption.

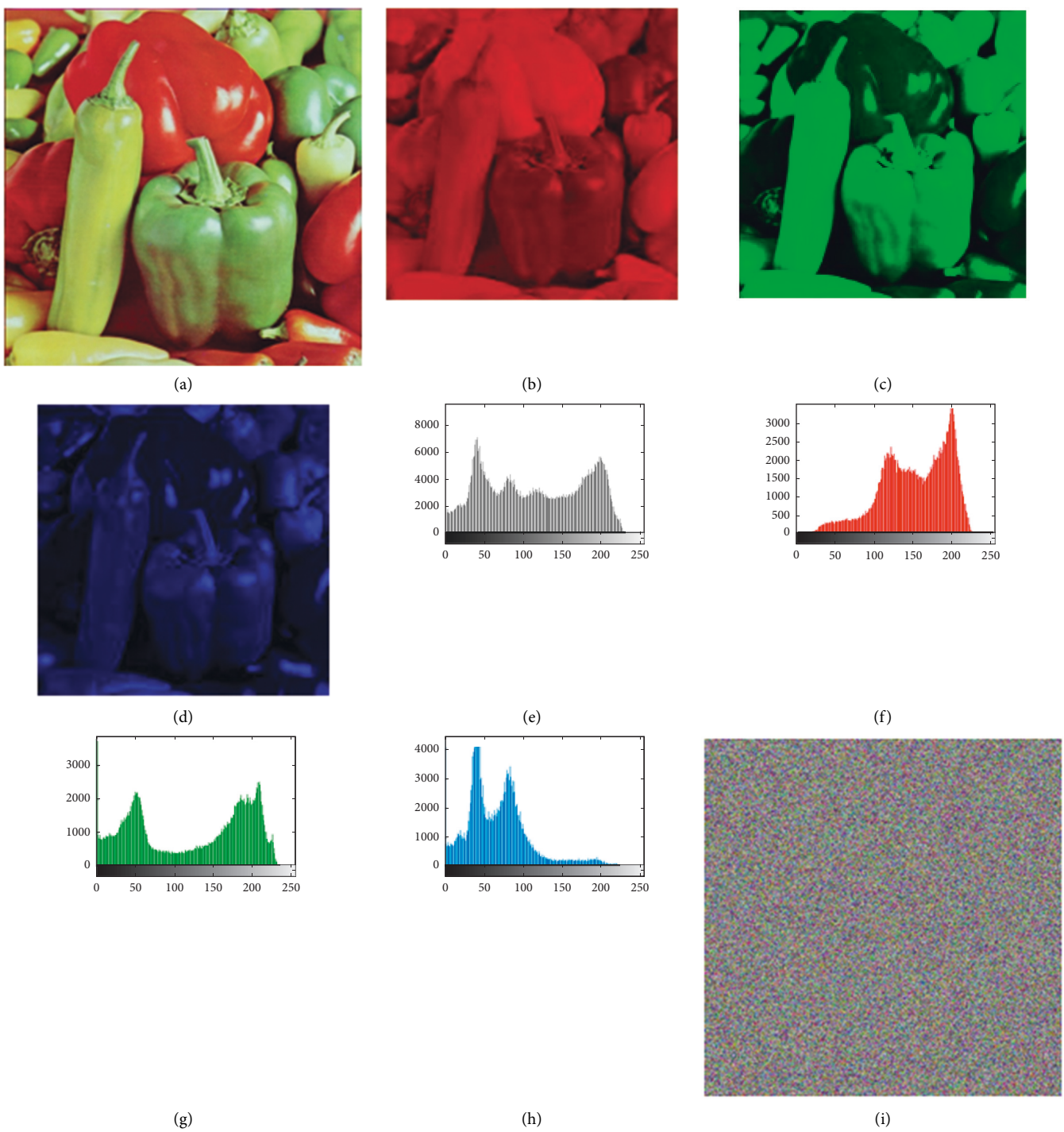

Figure 4: Continued.

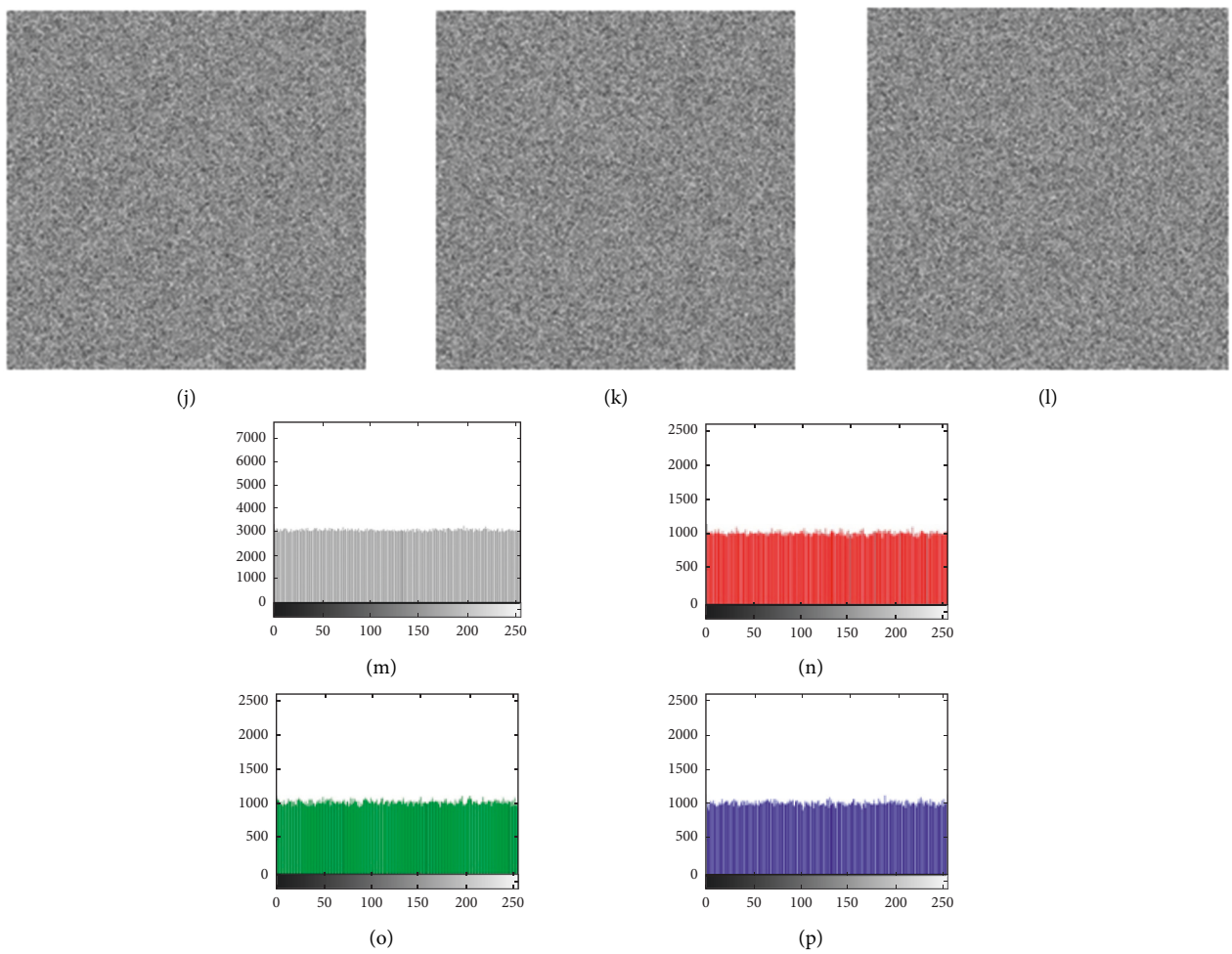

Figure 4: Encryption, decryption, and histogram results of the proposed scheme. (a, b, c, and d) Plaintext Pepper, plaintext red layer Pepper, plaintext green layer Pepper, and plaintext blue layer Pepper images, respectively; (e, f, g, and h) corresponding histograms; (i, j, k, and l) corresponding ciphertext images; (m, n, o, and p) ciphertext histograms.

creates a uniform pattern with minimal peaks and valleys, making it difficult for hackers to read the actual content due to pixel uniformity. The histogram shows the statistical quality of various images. It also discloses how arbitrary numbers created from chaotic maps, such as white noise, are uniformly dispersed. The histograms of plain images and encrypted images are given in Figure 4.

4.2. Correlation Coefficient Analysis (CC). It is used to determine the relationship between two variables. To discover the relationship between two variables, in our case, CC analysis is used. CC finds the quality of encrypted image by analyzing pixels distribution [23]. How effective a cryptosystem is can be measured by the encryption algorithm's ability to mask all plain image characteristics. Furthermore, it relies on an image's randomness and how uncorrelated the cipher image is [23–25]. If the CC for the two images (i.e., plain and encrypted) is low or close to zero, the proposed system is secure. In comparison, in the case of highly similar pixels between the two images, this demonstrates that the system is insecure. The defined range of correlation falls within [−1 1]. The high correlation of pixels between the two images reveals that the system is susceptible to many types of attacks and that malicious third parties can easily detect an image's original confidential content. In the case of encrypted images, the pixels are scattered in its defined range, depicting that the proposed system is secure. Figure 5 demonstrates the correlation plots for Pepper image. The test is applied on color and a channel-wise image with an image size of $512 \times 512 \times 3$ and 512×512 for three grey channels, respectively. Thus, one can confirm that in case of plaintext, the correlation among the adjacent pixels is very much strong and the plots are diagonally condensed. While in case of ciphertext, the plots are highly scattered which confirms high dissimilarity and randomness generated using the presented

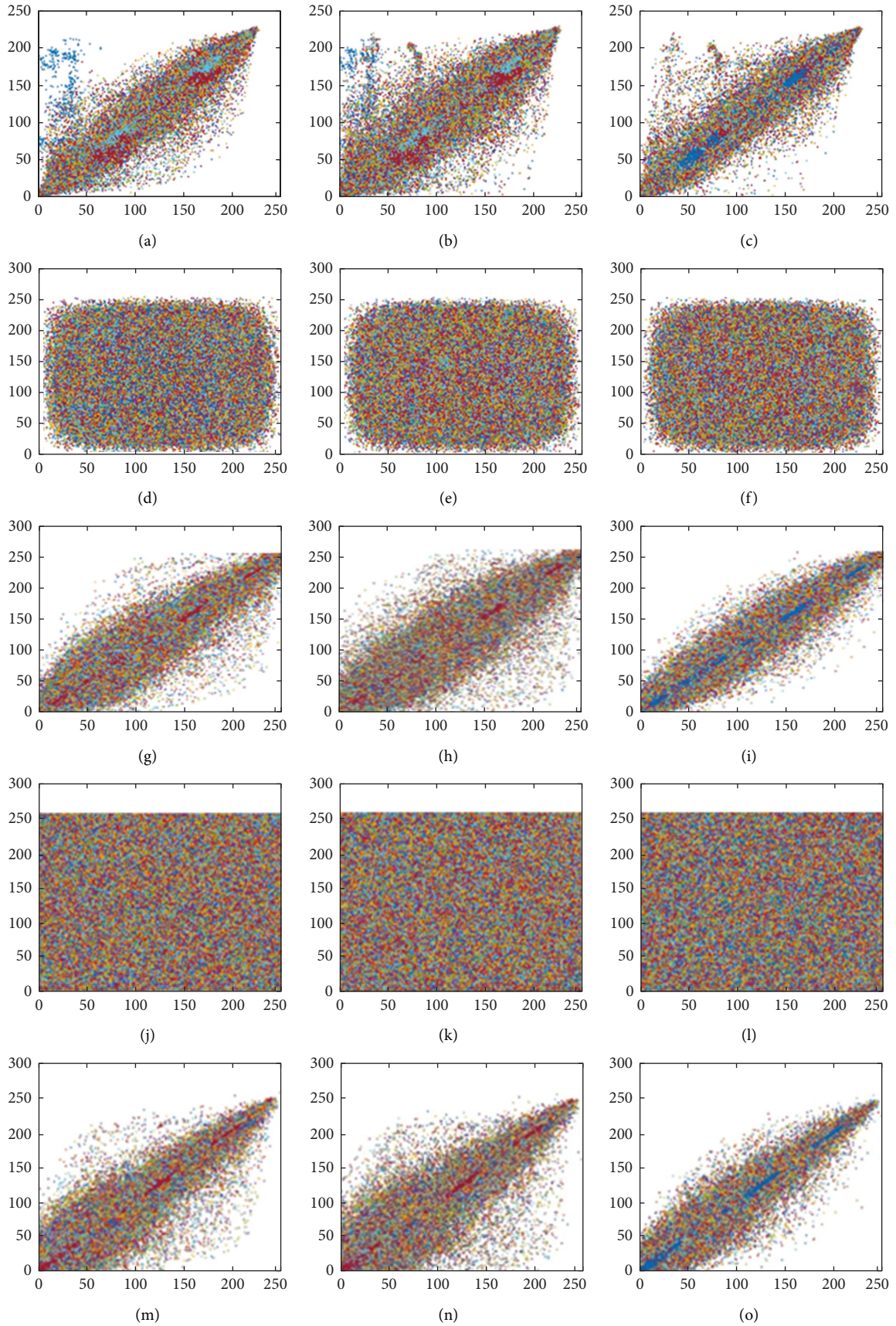

Figure 5: Continued.

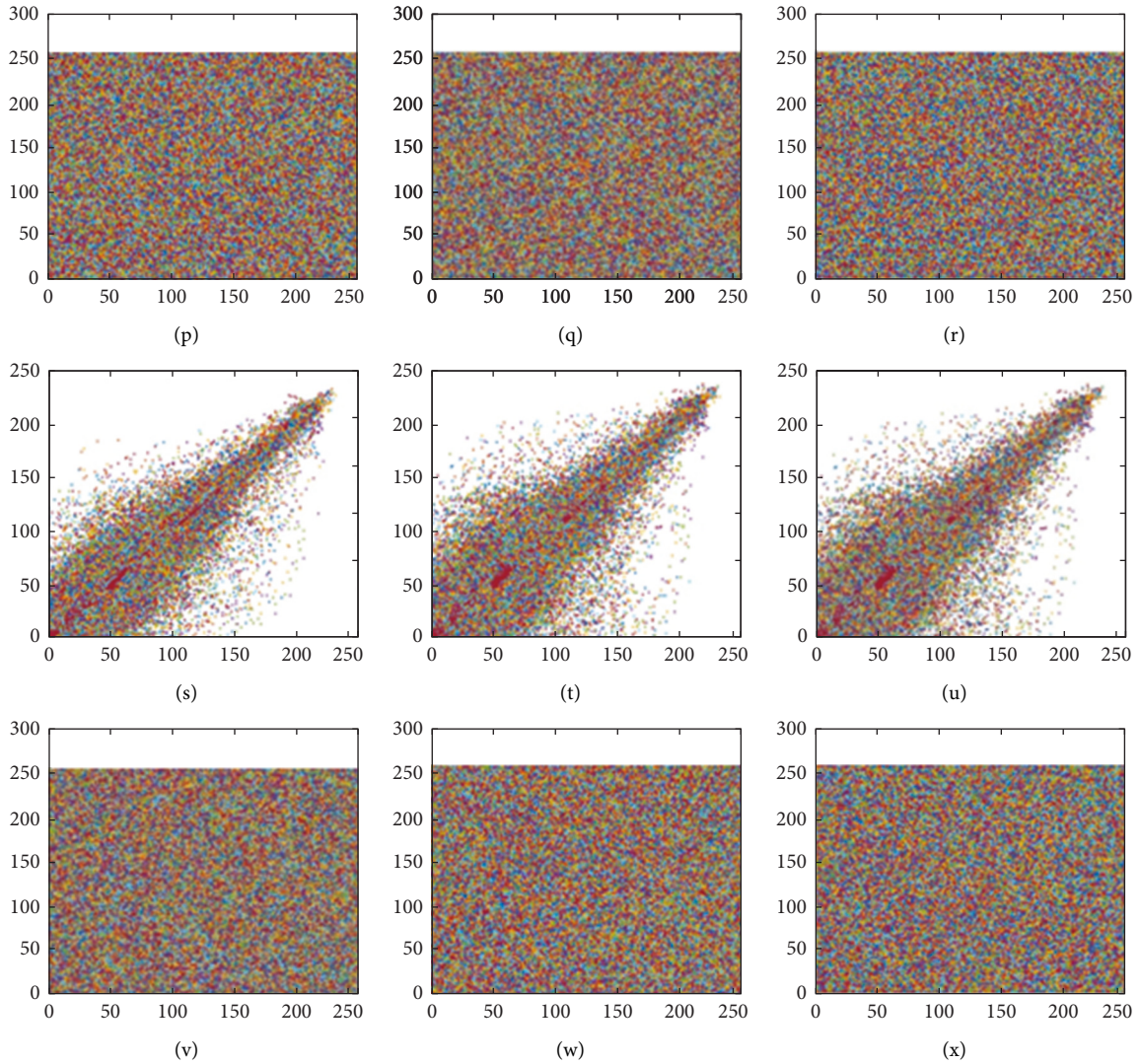

Figure 5: Pepper image correlation plots: (a, b, and c) plaintext Pepper correlation plots in horizontal, diagonal and vertical direction while row (1) (d, e, and f) corresponding ciphertext plots; (g, h, and i) plaintext Pepper red layer correlation plots in horizontal, diagonal and vertical direction; (j, k, and l) corresponding ciphertext plots; (m, n, and o) plaintext Pepper green layer correlation plots in horizontal, diagonal and vertical direction; (p, q, and r) corresponding ciphertext plots; (s, t, and u) plaintext Pepper blue layer correlation plots in horizontal, diagonal and vertical direction; (v, w, and x) corresponding ciphertext plots.

Table 1: Correlation coefficient values for Pepper image of size 512×512.

	Plaintext image			Encrypted image		
	Directions			Directions		
	HC	DC	VC	HC	DC	VC
Ideal	1	1	1	−1	−1	−1
Pepper	0.9635	0.9564	0.9663	−0.0033	0.0011	0.007
Ref. [28]	—	—	—	0.0075	0.0012	0.0049
Ref. [29]	—	—	—	0.0005	0.0008	0.0011
Ref. [30]	—	—	—	0.0117	0.0026	0.0010
Ref. [31]	—	—	—	0.0043	0.0054	0.0072
Ref. [32]	—	—	—	0.0108	0.0181	0.0061
Ref. [33]	—	—	—	0.0032	0.0042	0.0018
Ref. [34]	—	—	—	0.0204	−0.0174	0.0231
Ref. [35]	—	—	—	0.0053	−0.0027	0.0016

HC : Horizontally correlated; DC : Diagonally correlated; VC : Vertically correlated.

scheme. These scattered plots verify the scheme resistant to an attack. Correlation can be mathematically described as [26, 27]

$$r = \frac{S_{xy}}{S_x S_y}. \tag{4}$$

where the system's covariance is S_{xy}, while standard deviations of random variables of S_x, S_y, are x, and y, respectively. We applied the CC on the grey images of the same size as having a length of subsequently combined all the encrypted grey channels for the colored image. We also applied the CC test for the second time on colored images having a size of respectively. The computed values of the CC are shown in Table 1.

4.3. The Mean Absolute Error (MAE). MAE is one of the most important criteria required to determine an image's quality. It is also used to test how resistant a method is toward differential attacks. To analyze, let's consider the image being the total size of a test image. Let the C denotes the ciphered image, and P denotes the grey pixels of a plain image at the i th row and J th column. The equation used to find the mean absolute error is

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left| C_{(i,j)} - P_{(i,j)} \right|. \tag{5}$$

It is essential to obtain a higher value of MAE to validate the cryptosystem's robustness. If the evaluated MAE value is not higher than the existing scheme's average values, then the system has not resisted the differential attack. In other words, the higher the MAE, the stronger the security level of the designed cryptosystem. However, the resistant differential attack may still be fulfilled if the MAE computed value is not higher than the existing cryptosystems' values. The minimum value should be 75, which means that value higher than 75 demonstrates a high-security level. Our findings show that the proposed algorithm's calculated values are higher than 75: specifically, the estimated MAE value for the pepper image is 80, while the MAE for the Airplane image is 92, both of which are significantly higher than 75. Meanwhile, the MAE value of the "Tiffany" image over is two times higher than either of those, as shown in Table 2.

4.4. Differential Attacks Analysis. The randomness of the proposed encryption scheme can be evaluated using permutation method. Permutation's ability is to highlight even small changes in plain images. To check the proposed system's sensitivity level, we change a single pixel in the plain image and then calculate its respective outcome. As discussed in previous sections, small changes in the plain image can lead to drastic changes in the encrypted image, making the connection between original and cipher images very difficult and makes it more difficult for unauthorized third parties to decode them. Thus, the alteration of pixels in the plain image allows us to expand the encryption algorithm.

Table 2: MAE test values.

Image	Size	MAE
Pepper	512 × 512	80
Tiffany	512 × 512	182
Airplane	512 × 512	92
Ref. [36] pepper	256 × 256	74.93
Ref. [36] tiffany	256 × 256	94.36
Ref. [36] airplane	256 × 256	82.88

Table 3: AND UACI test values for different image (512 × 512) channels.

Image	Test type	R–C	G–C	B–C
Pepper	UACI	99.613%	99.613%	99.613%
Pepper		33.01	33.39	33.75
Tiffany	UACI	99.626%	99.626%	99.626%
Tiffany		36.13	36.13	36.13

Table 4: Computed and UACI values comparison with other schemes.

Image	Test type	Combined value
Pepper	UACI	99.613%
Pepper		33.38
Tiffany		99.626%
Tiffany		36.13
Ref. [37] pepper	UACI	99.589%
Ref. [37] pepper		33.373
Ref. [38] pepper	UACI	99.01%
Ref. [38] pepper		33.51
Ref. [39] pepper	UACI	99.22%
Ref. [39] pepper		33.12
Ref. [34] pepper	UACI	99.61%
Ref. [34] pepper		33.48
Ref. [40] pepper	UACI	99.60%
Ref. [40] pepper		33.41

The techniques of UACI and NPCR are usually employed to measure the effectiveness of pixel alteration.

4.4.1. Number of Pixels Changing Rate (NPCR). Several pixels' change rate examines how many pixels transmute when a single pixel alters in the plaintext image. This value reaches 99.60% in NPCR, showing us that the system has approached cautiously as it can easily defend itself against plain text attack. Ideally, the value for NPCR should be 100%. Tables 3 and 4 indicate that our proposed system achieves a calculated value of 99.613% for the encrypted pepper image across all three channels. In contrast, the Tiffany image's calculated; value is 99.626% for its all respective channels, as shown in Table 3. The proposed values and preexisting algorithms values are subsequently shown in Table 4, which compares the values we achieve to the values achievable by other existing systems. Table 4 reveals that both images achieve a higher proposed calculated value than those achieved by existing methods.

Two cipher images we consider for this evaluation are C1 and C2. However, their source image differs from a single

pixel. The equation used to calculate the value is as follows [41]:

$$= \frac{\sum_{i,j} D_{i,j}}{W \times H} \times 100, \tag{6}$$

where $W \times H$ denotes the total dimension of an image and can be illustrated as follows:

Case 1:

$$\begin{aligned} D_{(i,j)} &= 0, \\ C_{1(i,j)} &= C_{2(i,j)}. \end{aligned} \tag{7}$$

Case 2:

$$\begin{aligned} D_{(i,j)} &= 1, \\ C_{1(i,j)} &\neq C_{2(i,j)}. \end{aligned} \tag{8}$$

4.4.2. Unified Average Changing Intensity (UCAI). UACI is used to test and compare the intermediate intensities of both plain and encrypted images. UACI can be defined as [42] follows:

$$\text{UACI} = \frac{1}{W \times H} \sum_{i,j} \left[\frac{C_{1(i,j)} - C_{2(i,j)}}{255} \right] 100\%. \tag{9}$$

Here, $C_{1(i,j)}$ and $C_{2(i,j)}$ are the two ciphered images, while $W \times H$ denotes the total dimension of an image. We have considered a colored image that is divided into three layers of the same size. The evaluated results for all the images are higher than the average value of 33%, which indicates that the system has added a great deal of randomness into the proposed cryptosystem. For the pepper image, the algorithmic proposed value for those three channels (R, G, B) is 33.01, 33.39, and 33.75, respectively, as tabulated in Table 3. The Tiffany image's evaluated average values, and its three channels (R, G, B) are 36 for all three channels. Table 4 compares the values shown with preexisting values from [34, 37–40], which are reported as 33.373, 33.51, 33.12, 33.48, and 33.41, respectively. These results indicate that the presented scheme has produced a higher security level against any type of external attack.

4.5. The Mean Square Error (MSE). MSE can be evaluated using the difference between the two images. When the pixels of the plain and encrypted images are squared and then averaged, we get MSE that is calculated as follows [34, 37–40]:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{(i,j)} - C_{(i,j)} \right)^2, \tag{10}$$

where $M \times N$ represents the cumulative size of an image, while i and j represent image rows and columns, p and C are the plain and ciphered images at the ith row and jth column, respectively. A higher value of MSE shows that our suggested scheme has a greater level of robustness. Table 5 contains several values for MSE and PSNR, including an average layer value of 10,000. Thus, we conclude that the proposed algorithm has excellent potential in the field of secure communications.

Table 5: MSE and PSNR values for different channels of Pepper and Tiffany image.

Image	Image channel	Size	MSE	PSNR
Pepper	Red	512 × 512	11117.33	7.70
	Green	512 × 512	11222.95	7.66
	Blue	512 × 512	7988.03	9.14
Tiffany	Red	256 × 256	177701.01	5.67
	Green	256 × 256	13143.97	6.89
	Blue	256 × 256	7347.84	9.50

4.6. Peak to Signal Noise Ratio (PSNR). The image quality can be measured by utilizing the PSNR test. PSNR can be calculated as follows [34, 37–40]:

$$\text{PSNR} = 10 \log_2 \left(\frac{I_{\max^2}}{MSE} \right). \tag{11}$$

Here I_max denotes the maximum number of pixels of the test image. of pixels of the test image. PSNR is usually calculated in terms of decibels (dB). While MSE achieved value is better to ensure robustness of the cryptosystem's security, PSNR should have a lower value for better data protection. The aforementioned Table 5 shows different PSNR numbers for a set of additional test images. The average comes out to be 7, which satisfies the requirements of a robust cryptosystem.

4.7. Information Entropy (IE). This test provides key points regarding self-information. A report of any encryption channel requires entropy, and uncertainty itself relies upon entropy that is commonly known as randomness. IE can explain the degree to which uncertainties are present in communication channels [43]. According to Claude Shannon, as early as 1949, information theory is based on the mathematics of data transfer and storage [28]. Today, information theory is linked to communication systems, cryptology, data compression, and many other similar topics [44, 45]. Thus, entropy is the most significant characteristic of uncertainty and unpredictability since it demonstrates irregularity in the behavior of both plain and encrypted data. For the best-encrypted result, the cryptosystem must achieve a value of entropy as near eight as possible. IE of any message can be calculated as follows [46]:

$$H(m) = \sum_{j=0}^{N-1} p\left(x_j\right) \log_b p\left(x_j\right). \tag{12}$$

This explains the probability of any symbol to occur. Suppose there is a truly random source generating about 28 symbols with an equal probability m will be $= m_1 \ldots\ldots\ldots m_{28}$, where every symbol is shown by 8 bits. Upon applying this for Eq. (10), an IE value of $H(m) = 8$ bits will be attained corresponding to a uniform random source. As a whole, the ideal value is always greater than the IE of the actual source. This is because actual data rarely sends out randomized information. In this case, as mentioned above, a

Table 6: Entropy values for different channels of Pepper and Tiffany image.

Image	Image channel	Size	Computed entropy
Pepper	Red	512 × 512	7.999
	Green	512 × 512	7.999
	Blue	512 × 512	7.999
dTiffany	Red	256 × 256	7.999
	Green	256 × 256	7.999
	Blue	256 × 256	7.999
Splash	Red	512 × 512	7.999
	Green	512 × 512	7.999
	Blue	512 × 512	7.999
Tiffany	Red	256 × 256	7.997
	Green	256 × 256	7.997
	Blue	256 × 256	7.997
Airplane	Red	512 × 512	7.999
	Green	512 × 512	7.999
	Blue	512 × 512	7.999

Table 7: Comparison of computed entropy values and pre-existing algorithms.

Image	Dimension	Entropy
Proposed	512 × 512	7.999
Reference [47]-lena	512 × 512	7.996
Reference [48]-lena	512 × 512	7.997
Reference [40] (Sun's algorithm)	512 × 512	7.9965
Reference [40] (Baptista's algorithm)	256 × 256	7.9690
Reference [40] (Xiang's algorithm)	256 × 256	7.9950

Table 8: SC NCC, MD, and AD computed values.

Image	SC	NCC	MD	AD
Proposed	0.8004	1	223	34.1219
Tiffany	2.0954	1	255	89.1378

certain level of predictability arises when the IE comes out to be less than 8 bits [44, 45]. Entropy remaining close to the ideal value avoids IE attacks [44, 45]. Table 6 and 7 demonstrates the computed IE values for the proposed cryptosystem and its comparison with pre-existing schemes, respectively.

4.8. Structural Content (SC). SC is involved in the provision of aggregate weight regarding a specific plain signal to a coded or already present signal. A value of 1 for SC implicates that the image's quality is enhanced, while a more considerable value indicates that the image quality will be very low. Mathematically, SC is written as follows:

$$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(y_{(i,j)}\right)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x_{(i,j)}\right)^2}, \tag{13}$$

where, on account of the plain and encrypted images, SC estimation is not close to unity because the encryption scheme includes substitution, permutation-like noise, and commotion in the plain image. SC cannot be approximated as one if all of the shading images are advanced. SC calculated values for the proposed image encryption are illustrated in Table 8.

4.9. Normalized Cross-Correlation (NCC). NCC is a substantial test used to find the sets of similarity in image sets, particularly a plain image and its respective encryption of the same size. This test is widely utilized in image processing to find the quality of an image as well. The range of NCC falls between −1 and 1. Here −1 shows a strong correlation between the plain and encrypted images. Also, 1 shows that the correlation between two images is not strong, also known as a perfectly inverse correlation. Mathematically, NCC is defined as

$$NCC = \frac{1}{N} \times \frac{\text{sum}\left(\left[x_n - \text{mean}_x\right] \times \left[y_n - \text{mean}_y\right]\right)}{\sqrt{\text{var}_x \times var_y}}, \tag{14}$$

where $M \times N$ is the total size of an image and *var* shows variance of image between $x_{i,j}$ and $y_{i,j}$. Meanwhile, i and j show the actual position (row and column) of the pixels, and mean_x and mean_y show the mean level of the image x and y. The computed values for our two test images "pepper" and "baboon" are shown in Table 8. The value for both the test images is 1, which clearly demonstrates that the proposed work ensures higher security.

4.10. Maximum Difference (MD). MD is another criterion widely adapted for image security. This test is used to find the actual difference that has been created between the plain and encrypted images. The higher the value of MD depicts the fundamental difference between the plain and encrypted images. Mathematically, maximum distance is defined as:

$$MD = \text{MAX}\left|x_{(i,j)} - y_{(i,j)}\right|, \tag{15}$$

where MAX show the actual maximum difference between plain image $x_{(i,j)}$ at *ith* row and *jth* column and encrypted image $y_{(i,j)}$ at *ith* row and *jth* column. It is important to achieve maximum value for a secure system. The evaluated values for our test images "Pepper" and "Tiffany" are recounted in subsequent Table 8. The values of 223 for the pepper image and 255 for the Tiffany image (Table 8) validates the security of the proposed scheme.

4.11. Average Difference (AD). AD is another important test utilized by several research types in image processing, object detection and recognition, and security application. The test utilizes two images, i.e., the plain image and its encrypted image counterpart, in the formula that functions as follows:

$$AD = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x_{(i,j)} - y_{(i,j)}\right), \tag{16}$$

where $M \times N$ is the cumulative size of an image while $x_{(i,j)}$ and $y_{(i,j)}$ are two images at the *ith* row and *jth*

column, respectively. Table 8 shows the evaluated values of the average difference of Pepper and Tiffany images, which are 34.1219 and 89.1378, respectively. These results demonstrate that a high level of security is generated using the proposed system.

5. Ablation Study

The designed image encryption algorithm is based on chaotic maps. If there is a small change in key, it would not be possible to decrypt the original image. To reproduce the exact results obtained in this work is to use exact key. Moreover, if the size of the images is different than it would also be not possible to get exact same encryption results.

6. Conclusion and Future Work

This article discusses several security parameters that can be utilized to implement a robust encryption scheme and further perform evaluations using permutations to demonstrate how such methods would prevent various types of attacks and malicious interference. In the proposed work, we have also added multiple security layers, particularly multiple-dimensional chaotic iterative maps. Furthermore, in the permutation process, the actual value of image pixels was changed using the 2D gingerbread chaotic map to strengthen the security feature. The aforementioned chaotic maps generated a highly secure ciphertext image. The proposed scheme has been tested using various security parameters, i.e., histogram analysis, correlation coefficient, the mean absolute error, differential attacks analysis, number of pixels changing rate, unified average changing intensity, the mean square error, the peak to signal noise ratio, information entropy, structural content, normalized cross-correlation, maximum difference, and average difference. The results demonstrate the effectiveness of the proposed scheme against cryptographic and differential analysis attacks. The scheme presented in this paper uses various lightweight chaos maps, and hence it could also be tested in real-time applications. The proposed scheme is tested in MATLAB software; however, real-time implementation of FPGA should also be tested. Moreover, the proposed scheme should be tested for audio and video applications as well. [49–52] This work is developed for symmetric key encryption only. We aim to enhance the proposed scheme for asymmetric key encryption. In future, we will explore using our suggested cryptographic techniques to secure other kinds of data, such as diabetes classifications and biological data [53].

Data Availability

Data will be available upon request to the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Authors' Contributions

A. U., A. A. S., J. S. K., M. S., W. B., A. A., J. M., and F. A. G. performed formal analysis and original draft preparation. S. A. S. and J. A. proposed the main ideas and validated analysis. A. U., J. S. K., N. R., and J.A. crystallized framework and also revised the manuscript. All authors have read and agreed to the published version of the manuscript.

References

[1] A. Ghaleb, F. Saeed, M. Al-Sarem et al., "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics*, vol. 9, p. 1411, 2020.

[2] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification," *Remote Sensing*, vol. 13, p. 2221, 2021.

[3] M. Driss, D. Hasan, W. Boulila, and J. Ahmad, "Microservices in IoT security: current solutions, research challenges, and future directions," *Procedia Computer Science*, vol. 192, pp. 2385–2395, 2021.

[4] M. A. Khan, M. A. Khan Khattk, S. Latif et al., "Voting classifier-based intrusion detection for iot networks," *Advances On Smart And Soft Computing*, vol. 1399, pp. 313–328, 2022.

[5] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D lorenz chaotic map," *Entropy*, vol. 22, no. 3, pp. 274–709, 2020.

[6] F. Masood, M. Driss, W. Boulila et al., "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," *Wireless Personal Communications*, pp. 1–28, 2021.

[7] W. Stallings, *Cryptography and Network Security*, Vol. 4, E. Pearson Education India, Noida, India, 2006.

[8] H C. Cheng, Y Y. Zhi, L. GuoShiang, and H. ZengWei, "A virtual optical encryption software system for image security," *Journal of Convergence Information Technology*, vol. 6, no. 2, pp. 357–364, 2011.

[9] H. M. Al-Najjar, "Digital image encryption algorithm based on multi-dimensional chaotic system and pixels location," *International Journal of Computer Theory and Engineering*, vol. 4, no. 3, pp. 357–354, 2012.

[10] A. KrBanthia and N. Tiwari, "Image encryption using pseudo random number generators," *International Journal of Computer Application*, vol. 67, no. 20, pp. 1–8, 2013.

[11] R. L. Rivest, *Cryptography. In Algorithms and Complexity*, pp. 717–755, 1990.

[12] Z. Kartit, A. Azougaghe, H. K. Idrissi et al., "Applying encryption algorithm for data security in cloud storage," in *Advances in Ubiquitous Networking*, pp. 141–154, Springer, Singapore, 2016, [8].

[13] F. Masood, W. Boulila, J. Ahmad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos," *Remote Sensing*, vol. 12, p. 1893, 2020.

[14] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of an image encryption algorithm based on DNA encoding," *Optics & Laser Technology*, vol. 95, pp. 94–99, 2017.
[15] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1-2, pp. 50–54, 1998.
[16] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.
[17] E. Solak, R. Rhouma, and S. Belghith, "Cryptanalysis of a multi-chaotic systems based image cryptosystem," *Optics Communications*, vol. 283, no. 2, pp. 232–236, 2010.
[18] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.
[19] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, Article ID 26203, 2019.
[20] R. A. Thiétart and B. Forgues, "Chaos theory and organization," *Organization Science*, vol. 6, pp. 19–31, 1995.
[21] C. M. Reigeluth, "Chaos theory and the sciences of complexity: foundations for transforming education," in *Annual Meeting of the American Educational Research Association,* San Diego, CA, 2004.
[22] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, pp. 656–715, 1949.
[23] S. Bone and M. Castro, *A Brief History of Quantum Computing*, Imperial College in London, London, UK, 1997.
[24] F. Belkhouche and U. Qidwai, "Binary image encoding using one-dimensional chaotic map," *IEEE Annual Technical Conference IEEE Region*, vol. 5, pp. 39–43, 2003.
[25] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
[26] Y. Lu, W. Meier, and S. Vaudenay, "The conditional correlation attack: a practical attack on bluetooth encryption," in *Annual International Cryptology Conference*, pp. 97–117, Springer, Berlin, Heidelberg, 2005.
[27] L. Ballard, M. Green, B. De Medeiros, and F. Monrose, *Correlation-Resistant Storage via Keyword-Searchable Encryption*, p. 417, IACR Cryptology ePrint Archive, 2005.
[28] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons & Fractals*, vol. 42, no. 3, pp. 1745–1754, 2009.
[29] S. Mohammad Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Processing*, vol. 92, no. 5, pp. 1202–1215, 2012.
[30] S. Liu, J. Sun, and Z. Xu, "An improved image encryption algorithm based on chaotic system," *Journal of Computers*, vol. 4, pp. 1091–1100, 2009.
[31] A. Akhshani, A. Akhavan, S. C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, pp. 4653–4661, 2012.
[32] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, Article ID 18759, 2018.
[33] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, pp. 2986–3000, 2013.
[34] X. Wang and L. Yang, "A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models," *Optics Communications*, vol. 285, pp. 4033–4042, 2012.
[35] Y. Wu, Y. Zhou, J. P. Noonan, and S. Agaian, "Design of image cipher using Latin squares," *Information Sciences*, vol. 264, pp. 317–339, 2014.
[36] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools and Applications*, vol. 71, no. 3, pp. 1469–1497, 2014.
[37] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dynamics*, vol. 81, no. 1-2, pp. 511–529, 2015.
[38] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Information Security Journal: A Global Perspective*, vol. 25, no. 4-6, pp. 162–179, 2016.
[39] R. E. Boriga, A. C. Dascalescu, and A. V. Diaconu, "A new fast image encryption scheme based on 2D chaotic maps," *IAENG International Journal of Computer Science*, vol. 41, no. 4, pp. 249–258, 2014.
[40] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, pp. 2775–2780, 2011.
[41] J. S. Khan, W. Boulila, J. Ahmad et al., "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, Article ID 159732, 2020.
[42] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.
[43] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on the three-dimensional chaotic baker Map," *International Journal of Bifurcation and Chaos*, vol. 14, pp. 3613–3624, 2004.
[44] F. Sun, S. Liu, Z. Li, and Z. Lu, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons & Fractals*, vol. 38, no. 3, pp. 631–640, 2008.
[45] J. C. Yen and J. I. Guo, "A New chaotic key-based design for image encryption and decryption," *IEEE International Symposium on Circuits and Systems (ISCAS)*, vol. 4, pp. 49–52, 2000.
[46] J. S. Khan, J. Ahmad, S. F. Abbasi, and S. K. Kayhan, "DNA Sequence Based Medical Image Encryption Scheme," in *Proceedings of the 2018 10th IEEE Computer Science and Electronic Engineering (CEEC)*, pp. 24–29, IEEE, Colchester, UK, September 2018.
[47] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.
[48] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and DNA sequence," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 57–70, 2014.
[49] J. Ahmad, A. Tahir, J. S. Khan, M. A. Khan, F. A. Khan, and Z. Habib, "A Partial Ligt-Weight Image Encryption Scheme," in *Proceedings of the 2019 IEEE UK/China Emerging Technologies (UCET)*, pp. 1–3, Glasgow, UK, August 2019.
[50] B. A. Forouzan, *Cryptography & Network Security*, McGraw-Hill, New York, NY, USA, 2007.
[51] Y. Dodis, M. Stam, J. Steinberger, and T. Liu, "Indifferentiability of confusion-diffusion networks," in *Proceedings of the Annual International Conference on the Theory and*

Applications of Cryptographic Techniques, pp. 679–704, Springer, Berlin, Heidelberg, September 2016.

[52] J. x. Chen, Zl Zhu, C. Fu, Lb Zhang, and Y. Zhang, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dynamics*, vol. 81, no. 3, pp. 1151–1166, 2015.

[53] J. Masood, M. Shahzad, Z. A. Khan et al., "Effective Classification Algorithms and Feature Selection for Bio-Medical Data Using IoT," in *Proceedings of the 2020 Seventh International Conference on Information Technology Trends (ITT)*, pp. 42–47, Abu Dhabi, UAE, November 2020.