Aswan University Journal of Science and Technology Volume 4, issue 2, June 2024

Scrambled Encryption Approach for Color Images Based on 9-D Chaotic Systems with 3-D Substitution Bit Levels

Mohamed Abdel Hameed
Department of Computer Sciences, Faculty of Computers and Information, Luxor University, Luxor, Egypt

Abstract: Over the past few decades, the need for robust and secure communication has grown exponentially, particularly in image transmission over networks. This is due to the increasing reliance on digital technologies. This work demonstrates a novel "Scrambled Encryption Approach" that leverages the inherent unpredictability. To this end, nine-dimensional chaotic systems are combined with the innovative technique of 3-D substitution bit levels to verify strengths such as the confidentiality and integrity of visual data while maintaining fast encryption and decryption processes. This has the drawback of being vulnerable to known plaintext attacks and performing more sophisticated calculations than simpler encryption approaches. So, the proposed technique first separates the color input image into 24 bits to be categorized into 8 bits for each color channel (red, green, and blue). Then, 3-bit levels are used with position sequences for substitutions taken from the 9-D Lorenz chaotic system. After that, a multilayer differentiation technique produces three key matrices, which are then used to diffuse the scrambled components and produce the color cipher image. The simulation results show that our method has a high visual quality of decrypted images as well as high protection against brute force attacks because we have a large key space used for encryption data. Moreover, our proposed technique achieves more security against statistical attacks, including histogram analysis, information entropy, and correlation coefficients between pixels. Finally, the proposed encryption technique achieves a more secure transmission than state-of-the-art encryption approaches to guarantee integrity, privacy, and efficiency through global networks.

Keywords: Chaotic Map, Encryption, Scrambled, Lorenz Chaotic Map, Cipher Image.

1. INTRODUCTION

In a current generation of informatics that is characterized by high volumes of digital data, information security, and privacy have become paramount concerns [1]. The importance of information security and data protection has grown as a result of the quick migration of several services from local networks to the Internet. It is well-accepted that digital photos contain a huge quantity of information [2]. To meet the rising computational power of cryptanalysis, encryption methods have been considerably improved to increase their complexity, preventing attackers from quickly compromising encrypted data [3, 4]. As a result, digital picture scramblers are meant to convert clear images into unintelligible ones as an integral part of modern data protection measures such as image encryption [5, 6], steganography [7-11], and watermarking [12-14]. Encryption and cryptography stand at the forefront of efforts to protect sensitive information from unauthorized access, ensuring that data remains confidential and unaltered after transmission over networks. The challenges of securing digital media, particularly videos, and images, have spurred innovative approaches, such as the integration of chaotic maps, to enhance the robustness of encryption and scrambling techniques [15].

Corresponding author E-mail: m.abdelhamid@fci.luxor.edu.eg,
Received, January 09, 2024, received in revised form January 20, 2024, accepted January 22, 2024.
(ASWJST 2024/ printed ISSN: 2735-3087 and on-line ISSN: 2735-3095) https://journals.aswu.edu.eg/stjournal

Several encryption solutions for the image based on diverse methodologies have been presented during the last few decades [16]. For encryption, many methods are available, including the AES, DES algorithms, IDEA, RSA, and others. However, most of these techniques are restricted to textual data. The image features qualities, such as well-built inter-pixel correlation and high redundancy; hence, it cannot be utilized for image encryption. To resolve that issue, various researchers have developed several encryption algorithms [17-19]. The new 1D chaotic map was combined with a color image encoder introduced by Escobar et al. [20]. Moreover, Babaei's method [15] outperforms the majority of low-dimensional chaos-based image encrypting approaches in terms of image encryption method based on DNA computing. Aside from this, several image encryption techniques have evolved [21, 22] depend on different low-dimensional chaotic systems. Diaconu et al. [23], demonstrated a color image scrambling approach according to Knight's movement principles, where the pixels are transposed across RGB channels. Gao [24] indicated a color image encryption based on an upgraded Henon map, which has more complex chaotic actions and thus more efficient than the standard one, resulting in the superior performance of the technique. Li and Chen [25] have suggested a 6-D hyper-chaotic system merged with DNA encoding to enhance security.

In recent decades, many researchers [37–40] have established high-dimensional methods of encryption very quickly to address security issues that prevent low-dimensional encryption from meeting requirements, given the speed at which modern communication is developing. Moreover, in [41–45], good encryption and good statistical properties are achieved, which leads to good security and integrity for the data transmission but with high complexity and limited key space for encryption.

Since chaos is responsive to initial conditions and system settings, it performs better than standard encryption techniques with regard to randomness, unpredictability, and non-periodicity [10, 11]. The encryption technique based on chaos is given more importance in such systems compared to other encryption algorithms. The sequences are typically used by chaotic cryptosystems to change the location of each pixel in the original image. The operation of diffusion applied to chaotic patterns is another widely used technique for encrypting images. Consequently, the improvement of chaos-based encryption techniques has extended more rapidly.

Simultaneously, the incorporation of 3-D substitution bit levels offers a means of reorganizing three channels of RGB as image data dynamically and intricately, further encrypting the content. The scrambled encryption approach commences by generating chaotic sequences using the nine-dimensional chaotic system, infusing encryption with a layer of true randomness. In parallel, 3-D substitutions are applied to the color image data, introducing a unique form of shuffling that enhances security. The combined approach seeks to make it challenging for potential adversaries to decipher the encrypted data, ensuring that visual content remains protected.

The rest of the paper is structured as follows: In Section 2, we discuss 3-D substitution bit levels and the 9-dimensional chaotic system. In Section 3, the proposed image encryption and decryption techniques are described in detail. To demonstrate the security and outcomes, Section 4 has a few results and discussions. Finally, Section 5 illustrates the conclusion of our study.

2. PRELIMINARY

Here, we provide some pertinent theoretical information that was utilized across the paper.

Three Dimensional Substitution Bit Levels

In general, confusion and diffusion are the two phases in the conventional chaos-based image encryption process. In the confusion stage, pixel coordinates are substituted. The values of the pixels vary throughout the diffusion phase corresponding with the chaotic random sequence. Until the pixel values are all modified and the encryption is finished, repeat the two actions multiple times [25], [42-45].

Since the majority of the images have substantial relationships between adjacent pixels, we substitute the RGB image pixels using chaotic sequences to get rid of the correlations. Image substitution is the initial stage in the proposed approach. To reduce the correlation between them, the original color image RGB is transformed into three vectors: V_R, V_G, and V_B. These vectors are then substituted based on the three sequences—X_n, Y_n, and Z_n for R, G, B respectively. So, the sequences V_R, V_G, and V_B will be shuffled, causing all values in the vectors to change their positions [26]. To perform 3-D substitution bit levels on a color image, we can use the following steps:

1. Convert each pixel's RGB values to binary representation:
   R = (R7, R6, R5, R4, R3, R2, R1, R0)
   G = (G7, G6, G5, G4, G3, G2, G1, G0)
   B = (B7, B6, B5, B4, B3, B2, B1, B0)
2. Apply a substitution function to each bit of the RGB values using a key:
   R_ New = Substitution_Function(R)
   G_ New = Substitution_Function(G)
   B_ New = Substitution_Function(B)
3. Convert the new binary values back to decimal and update the pixel's RGB values:
   Pixel_New = (New_R(decimal), New_G(decimal), New_B(decimal)).

Example:

Let's say we have a pixel with RGB values (255, 127, 63).

1. Convert each pixel's RGB values to binary representation:
   R = (1, 1, 1, 1, 1, 1, 1, 1)
   G = (0, 1, 1, 1, 1, 1, 1, 0)
   B = (0, 0, 1, 1, 1, 1, 0 ,0)
2. Apply a substitution function to each bit of the RGB values using a key: Let's say our substitution function is to invert each bit (0 becomes 1 and vice versa).
   R_ New = (0 ,0 ,0 ,0 ,0 ,0 ,0 ,0)
   G_ New = (1 ,0 ,0 ,0 ,0 ,0 ,0 ,1)
   B_ New = (1 ,1 ,0 ,0 ,0 ,0 ,1 ,1)
3. Convert the new binary values back to decimal and update the pixel's RGB values:
   Pixel_New = (0(decimal),128(decimal),192(decimal)). So the updated pixel's RGB values are (0,128,192).

Lorenz Chaotic System

To make the following information easier for readers to understand, we first give an overview of chaotic systems in this part, along with various indicators and their features. Both continuous chaotic systems and discrete chaotic maps are categories of chaotic systems that can be distinguished by their temporal evolution [26]. Systems that are dynamic and display complicated and unpredictable behavior throughout time are known as continuous chaotic systems. Usually, a system of partial differential equations controls how state variables change over time to characterize these systems [27]. However, the 3-D Lorenz system has limitations in terms of its security. Its relatively low dimensionality makes it susceptible to certain cryptanalytic attacks. Additionally, its chaotic attractor, the butterfly curve, has been well-studied and characterized, which can aid attackers in breaking the encryption [28]. To address these limitations, researchers have developed higher-dimensional versions of the Lorenz system, such as the 6-D Lorenz system [25].

However, because the need for security is never restricted, the 9-D hyper-chaotic system was created to increase the complexity and unpredictability of the proposed chaotic system. So, they offer several advantages:

- Increased complexity: The higher dimensionality leads to a more complex and intricate chaotic attractor, making it significantly harder for attackers to analyze and predict the system's behavior.
- Larger key space: The additional dimensions allow for a larger number of possible initial conditions and parameter values, resulting in a much larger key space for encryption. This makes it exponentially more difficult for attackers to find the correct key to decrypt the message.
- Enhanced sensitivity to initial conditions: The 9-D Lorenz system exhibits even greater sensitivity to initial conditions than the 6-D system. This means that even tiny changes in the initial state can lead to vastly different trajectories, further boosting the security of the system.

The proposed approach in this paper uses the 9-D hyperchaotic system that can be generated in the following formulas:

$$\frac{dx}{dt} = A(Y - X) \quad (1)$$

$$\frac{dy}{dt} = B(X - Z) \quad (2)$$

$$\frac{dz}{dt} = C(X - Y) \quad (3)$$

$$\frac{dw}{dt} = D(X + Y + Z - W) \quad (4)$$

$$\frac{de}{dt} = E(W - Y) \quad (5)$$

$$\frac{df}{dt} = F(V - X) \quad (6)$$

$$\frac{dg}{dt} = G(X - V) \quad (7)$$

$$\frac{dh}{dt} = H(W - Z) \quad (8)$$

$$\frac{di}{dt} = I(Y + V - Z) \quad (9)$$

where A, B, C, D, E, F, G, H and I are the initial parameters of the system.
A large variety of parameter values result in the chaotic behavior of the 9-D Lorenz map. It has been demonstrated to have a minimum of nine positive Lyapunov exponents, a system's chaoticity metric. Additionally, because the system is sensitive to beginning conditions, even slight modifications to those variables can have a significant impact on the system's behavior in the future.

3 PROPOSED ENCRYPTION SYSTEM

In this section, the 9-D Lorenz chaotic system and 3-D substitution bit levels were used to create an encryption scheme for color images. As displayed in Figure 1, three major matrices comprise an original image, R, G, and B where each one has been cipher using nine keys achieved from the key space of Lorenz system. First, the size of the original image is defined as MxNx3. Then, using X, Y, and Z key streams generated from the key space, three-bit levels are permuted. After that, using the U, V, and W key streams we apply the scramble level for the permuted image to obtain the scrambled image. Furthermore, the Q, R, and S key streams are used in the forward diffusion level to get the diffused image. Finally, a cipher image is accomplished.

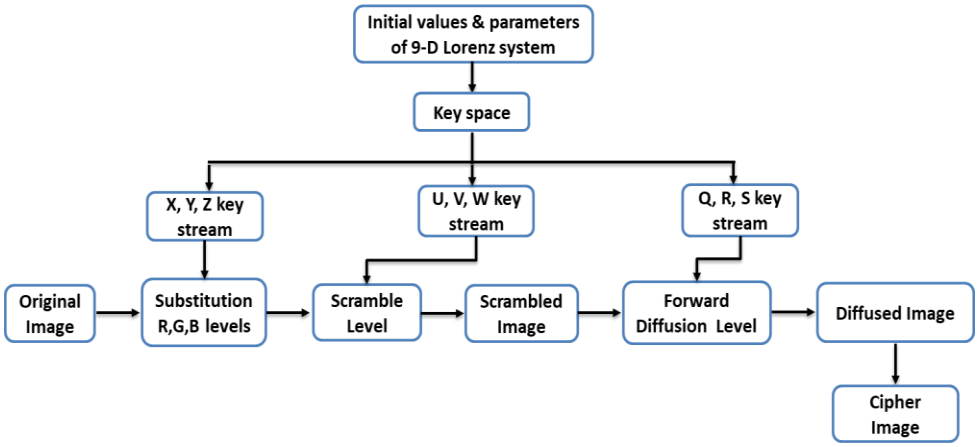


Figure 1: Framework of encryption algorithm.

4. PROPOSED DECRYPTION SYSTEM

Figure 2 illustrates the framework of the decryption algorithm. Hence, the decryption procedure is the inverse of the encryption phase. First, the size of the cipher image is defined as M`x N`x 3. Then, three keys, flip(X), flip(Y), and flip(Z) generated from the key space to obtain inverse substitution levels R, G, B. After that, using flip key stream (U, V, W) to enter descrambled level. Furthermore, using flip key stream (Q, R, S) to provide a backward diffusion level for the descrambled image. Finally, original image is obtained.

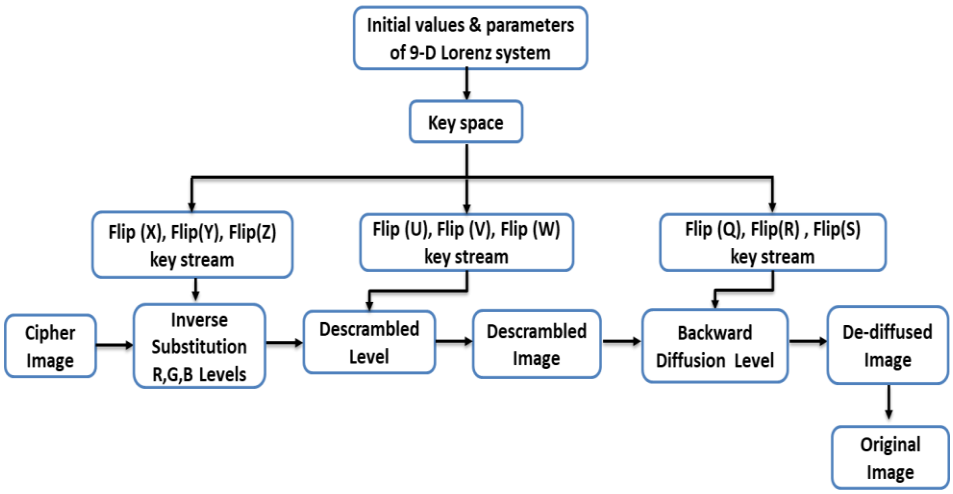


Figure 2: Framework of decryption algorithm

4. SIMULATION ANALYSIS AND DISCUSSION

In this section, we discuss a group of results for the proposed technique to test visual quality of cipher images and their robustness counter statistical attacks to prove dependability and effectiveness of the proposed approach. So, we have system parameters and initial values, images dataset and other discussions of the experimental results.

System Parameters

For a large range of parameter values, the 9-D Lorenz map exhibits chaotic behavior. It has been demonstrated to contain at least 9 positive Lyapunov exponents, which is a measure of a system's chaoticity. The system is also sensitive to initial parameters, which indicates that slight modifications in these parameters can cause massive and unpredictable changes in the system's long-term behavior. Here is a system parameters and values used in our system as shown in equations (10, 11, 12, 13, 14, 15, 16, 17, 18) where A = 10, B = 28, C = 8/3, D = 25, E = 8, F = 8, G= 6.7, H = 0.01, and I = 1.5 respectively.

Developmental Environment and Dataset

The hardware setup for these experiments contains an Intel processor Corei9, 3.2 GHz, with 16 GB of RAM. The operating system of the software environment is Windows 11 with MATLAB 2015b. We used a random sample of color images from the ImageNet [28] dataset. The original images have been resized to 512x512 pixels as introduced in Figure 3.

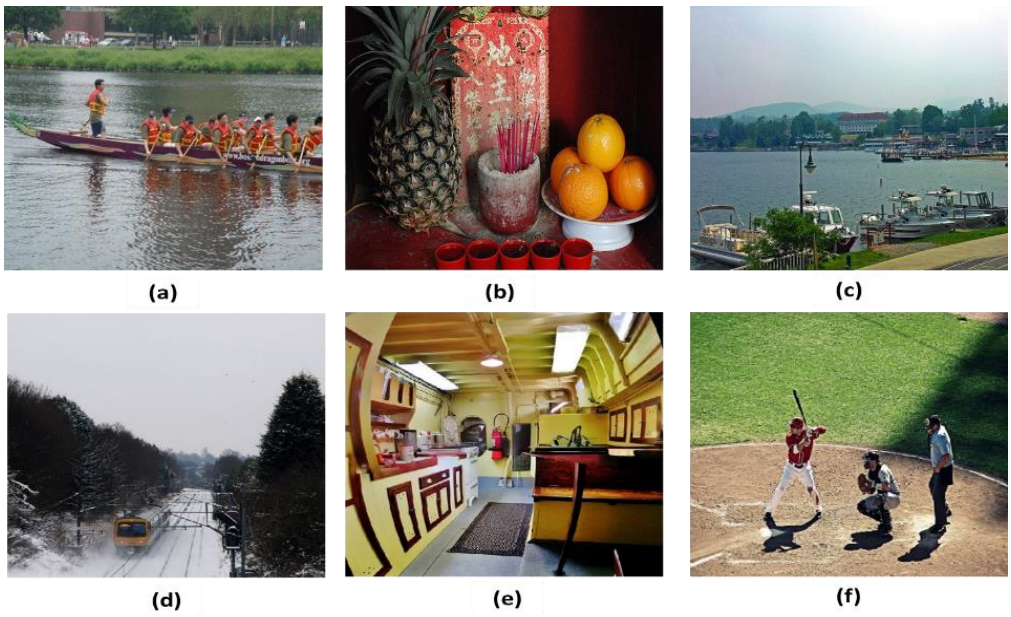


Figure 3: Sample images from the ImageNet dataset.

Analysis of Visual Quality

Many typical images from the ImageNet dataset [28] are tested for their encryption and decryption impact. Figures 4 and 5 depict the visual quality of original and retrieved images of the proposed scheme. It illustrates that the cipher image has no information that may be associated with the original image. Consequently, the proposed approach is effectively encrypted and can conceal data without the doubt that it has been hidden. Also, the retrieved image has the same visual quality as the original.

Analysis of Security

This section investigates the encryption system's security from several perspectives.

Analysis of Key Space

In a cryptosystem, the term "key space" describes the assembly of all possible, unique, and legitimate keys. The security of the cryptosystem is proportional to the size of the key space. For resistance to an exhaustive attack, a good encryption technique must have a big key space because the attacker will attempt to brute force every combination of keys to decipher the image. The proposed approach contains 9 keys in total: *X, Y, Z, U, V, W, Q, R, and S.* Assuming that the accuracy of the computer's calculation is 10^{-16} and *S* is between 0 and 255. Thus, the proposed approach has a range of keys equal to $[(10)^{16}]^9 \times 2^8$, and it is close to 2^{487}. So, our technique has more key space than [25], [29] and [30] as shown in Table 1. According to cryptography [31], the encryption algorithm is now secure when the key space exceeds $2^{100} \approx 10^{30}$. Therefore, the proposed technique has an excellent key space to stave off a brute-force attack.

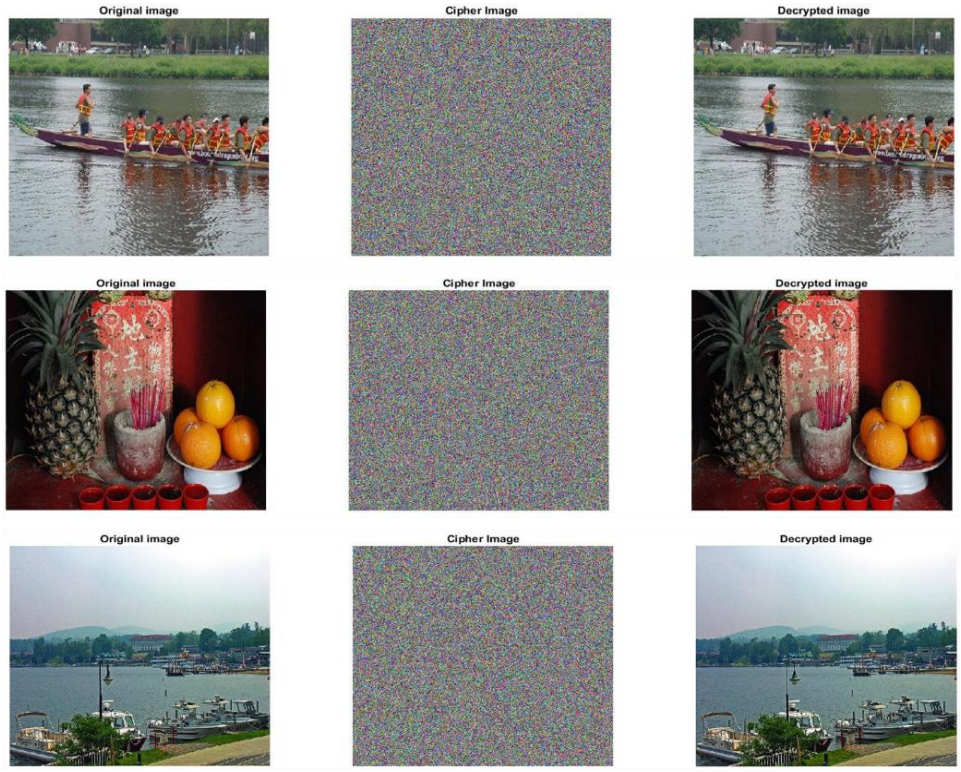


Figure 4: Visual quality results of cipher and decrypted images (a), (b) and (c).

Analytical Statistics

Histogram analysis, information entropy, and pixel correlation are the three primary benchmarks of the statistical analysis of images. The statistical analysis attack occurs when an attacker acquires the statistical properties of cipher images. First, histogram analysis is a crucial indicator of whether the encryption process can withstand a statistical analysis assault or not. Second, the entropy of information is a particularly important indicator of randomness since it measures the uncertainty of a random variable. An entropy attack can be used against a cryptosystem if it does not generate enough disorder at the output. Third, pixel correlation means that strong correlations exist between an image's pixels, which facilitate easier image manipulation. For instance, the correlation between neighboring pixels, which characterizes the relationship between neighboring pixels that is horizontal, vertical, or diagonal. Thus, the

cipher image must break the original image's pixel correlation, which leads to robustness against statistical analysis [40–45].

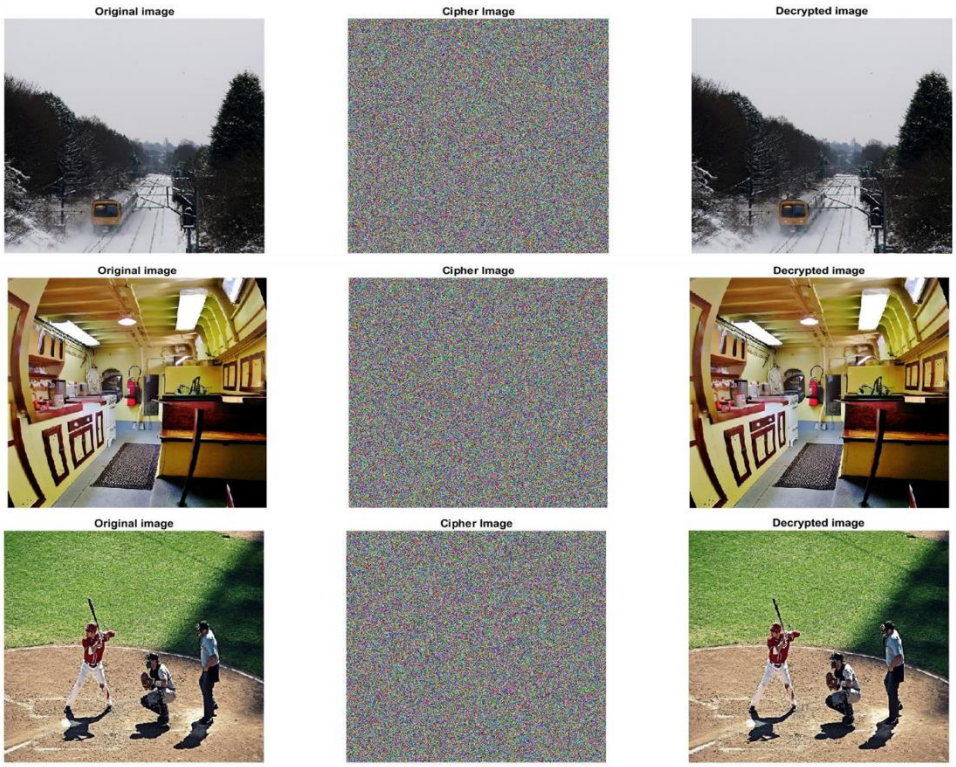


Figure 5: Visual quality results of encryption and decrypted images (d), (e) and (f).

Table 1: key spaces among various techniques.

Technique	Ref. [25]	Ref. [29]	Ref. [30]	Proposed Technique
Key space	2^{300}	2^{299}	2^{472}	$\mathbf{2^{487}}$

Analytical Histogram

A histogram analysis may provide insight into an image's pixel value distribution. Original images typically exhibit distinct patterns and biases in their histograms, reflecting features like dominant colors, shapes, and textures [33–36]. Secure encryption techniques aim to disrupt these patterns and create a more uniform distribution of pixel values in the encrypted image's histogram. This makes it challenging for attackers to infer meaningful information about the original image from its visual appearance or statistical properties [42–45].

If we achieve a safe encryption technique, we must spread the encrypted image's histogram evenly and withstand statistical attacks. As shown in Figures 6, 7, and 8, the original and cipher images with their corresponding histograms for 6 images The proposed approach illustrates that the cipher images exhibit an equitable and uniform distribution of pixel values for each RGB channel within the interval [0, 255]. As mentioned earlier, statistical attacks often rely on identifying patterns or biases within histograms to gain insights into the encryption process or reveal

characteristics of the original image. Thus, a uniform histogram effectively counters such attacks by concealing any exploitable patterns, which indicates that our proposed technique is highly resistant to histogram analysis.

Analytical Information Entropy

Analytical information entropy for an image may be calculated using the following formula [32]:

$$EN(p) = -\sum_{i=0}^{2^k-1} I\left(p_i \log_2\left(I(p_i)\right)\right) \qquad (10)$$

where EN is the entropy of an image *p*, 2^k is all possible values, *I(pi)* indicates the possibility of p_i, and $\log_2$ describes the logarithms at base two. The entropy is expressed in bits for each color channel using the same formula above but applied separately to three channels. For each channel, the maximum entropy is equal to 8. Table 2 demonstrates the information entropy of primary colors R, G, B and their cipher images of six images. The obtained outcomes of the red, green, and blue colors of each image illustrate that the entropy range is between 7.9992 and 7.9995, while the cipher images achieved an entropy range between 7.9992 and 7.9994. This indicates a high degree of randomness and unpredictability in pixel values. So, this leads to a positive sign for the encryption method's strength, as high entropy typically correlates with greater security and is harder to analyze for statistical attacks. In essence, the high entropy of the proposed technique acts as a powerful shield against various attacks, reinforcing the security of sensitive image data and implying a more thorough randomization and diffusion of pixel values.

As shown in Table 3, we compare our approach with the most recent chaotic algorithms using image (a) to demonstrate its strong performance and effectiveness against statistical attacks. Hence, the proposed approach of the R, G, B, and cipher image (a) is better than [25], [29], and [30] with entropy values of 7.9994, 7.9993, 7.9995, and 7.9994, respectively.

Table 2: The entropy of R, G, B and their cipher images.

Channels \ Images	(a)	(b)	(c)	(d)	(e)	(f)
Red Color	7.9994	7.9992	7.9994	7.9994	7.9993	7.9993
Green Color	7.9993	7.9992	7.9993	7.9993	7.9994	7.9993
Blue Color	7.9995	7.9993	7.9995	7.9993	7.9993	7.9993
Cipher Image	7.9994	7.9992	7.9994	7.9993	7.9993	7.9993

Table 3: The entropy among state-of-the-art encryption techniques using image (a).

Channels\ Refs.	Ref. [25]	Ref. [29]	Ref. [30]	Proposed Technique
Red Color	7.9991	7.9962	7.9971	**7.9994**
Green Color	7.9992	7.9950	7.9950	**7.9993**
Blue Color	7.9991	7.9971	7.9962	**7.9995**
Cipher Image	7.9991	7.9963	7.9961	**7.9994**

Analytical Pixel Correlation

Natural images, even simple ones, exhibit strong dependencies between adjacent pixels. Neighboring pixels often share similar color or intensity values, creating smooth transitions and forming recognizable features. This high correlation contributes to the image's coherence and meaning [31].
Ideally, the encrypted image should exhibit a significantly lower correlation between adjacent pixels, indicating successful randomization and increased resistance to analysis [42–45]. The following formula is used to get the coefficient:

$$r_{ij} = \frac{E[i - E(i)][j - E(j)]}{\sqrt{D(i)D(j)}} \qquad (11)$$

where E(.) and D(.) stand for the data i and j's expectation and variance, respectively. These can be expressed as follows:

$$E(i) = \frac{1}{N}\sum_{x=1}^{N} i_x \qquad (12)$$

$$D(i) = \frac{1}{N}\sum_{x=1}^{N} [i_x - E(i)]^2 \qquad (13)$$

When the correlation coefficient is close to one, there is typically a strong pixel relationship in the initial image. To find the picture correlation, several pairs of nearby pixels from the original and encrypted photos are selected. On the other hand, when the correlation coefficient is close to zero, the cipher image has a low pixel correlation.

As displayed in Table 4, the results of the proposed technique in three directions (H, V, and D) provided a very low correlation between adjacent pixels of both original and cipher images. So, it achieves successful randomization and increases resistance to statistical analysis.

In Figures 9, 10, we randomly selected 5000 adjacent pixels in three directions: horizontal, vertical, and diagonal, before and after encryption for six images. It illustrates that even if the cipher pictures have been cracked and have a random distribution, the original images exhibit a high pixel relationship. As a result, the proposed technique has a superior encryption effect against various statistical attacks.

As mentioned earlier, natural images typically exhibit strong correlations between neighboring pixels due to spatial patterns and color gradients. Our proposed technique, the 9-D Lorenz chaotic map with RGB bit substitutions, aims to disrupt these patterns. Moreover, reducing correlations makes the encrypted image more randomized and less predictable, hindering attackers' ability to glean meaningful information from visual inspection or statistical analysis.

As described in Table 5, a comparison between the correlation coefficients of the proposed scrambled system and the state-of-the-art strategies using test image (a). As compared to references [25, 29, 30], it is clear that our cryptosystem encrypts the image and considerably reduces the correlation coefficient between adjacent pixels.

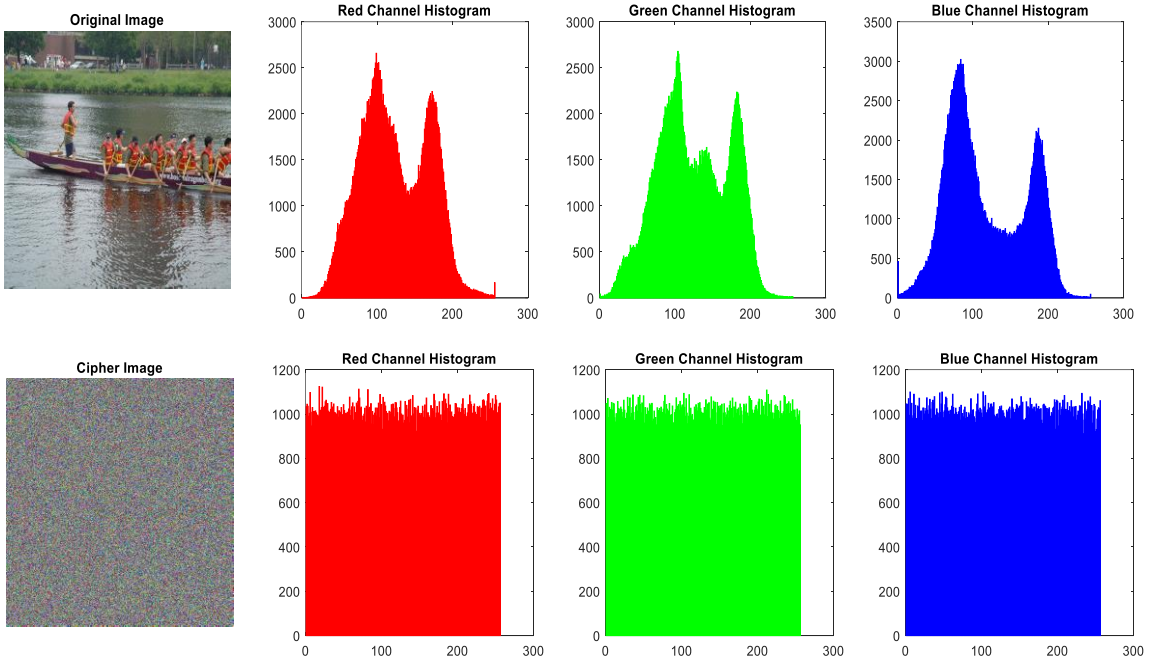
Table 4: The correlation coefficients between the original and ciphered images in three directions- horizontal, vertical, and diagonal.

Images	Channel	Original			Cipher		
		H	V	D	H	V	D
Image (a)	R	0.9699	0.9793	0.9585	-0.0014	-0.0028	-0.0051
	G	0.9757	0.9691	0.8909	-0.0012	0.0083	-0.0125
	B	0.9506	0.9456	0.8515	-0.0017	-0.0043	-0.0045
Image (b)	R	0.9784	0.9635	0.9545	-0.0150	-0.0017	-0.0053
	G	0.9556	0.9374	0.9124	0.0034	-0.0080	0.0061
	B	0.9420	0.9243	0.8813	0.0177	-0.0088	0.0056
Image (c)	R	0.9123	0.9252	0.8810	0.0070	-0.0124	-0.0136
	G	0.9079	0.9116	0.8806	0.0149	-0.0150	0.0068
	B	0.9071	0.9287	0.8914	0.0068	0.0093	-0.0126
Image (d)	R	0.9608	0.9620	0.9536	0.0185	-0.0041	0.0030
	G	0.9596	0.9657	0.9510	-0.0044	0.0006	-0.0110
	B	0.9667	0.9642	0.9492	0.0342	-0.0020	0.0118
Image (e)	R	0.9322	0.9298	0.8924	-0.0086	0.0196	0.0082
	G	0.9220	0.9262	0.8829	0.0080	-0.0058	-0.0076
	B	0.9185	0.9283	0.8920	0.0146	0.0039	0.0095
Image (f)	R	0.9295	0.9384	0.8987	0.0034	0.0049	-0.0170
	G	0.9095	0.9141	0.8602	-0.0102	-0.0244	0.0250
	B	0.8692	0.8858	0.8167	-0.0010	0.0304	0.0018

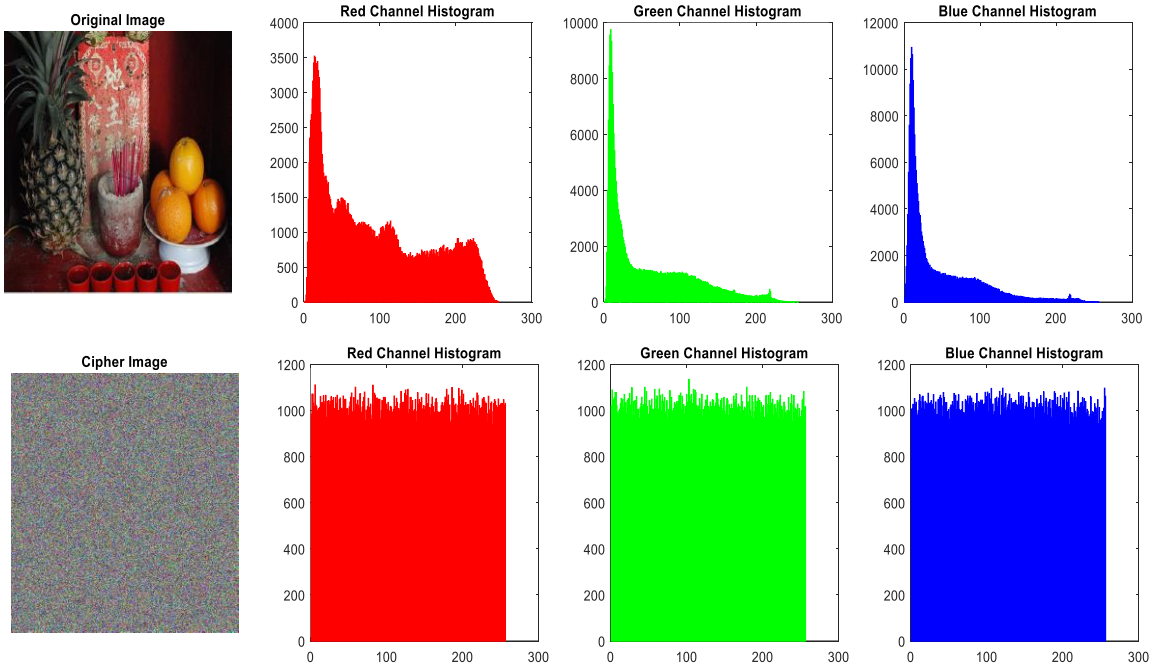
Table 5: Pixel correlation analysis among state-of-the-art encryption techniques using image (a).

Refs.	Original			Cipher		
	H	V	D	H	V	D
Ref. [25]	0.9308	0.8620	0.9536	0.0165	0.0282	-0.0151
Ref. [29]	0.9557	0.9291	0.8909	0.0126	0.0583	-0.0125
Ref. [30]	0.9004	0.9251	0.8725	0.0173	0.0243	-0.0245
Proposed Technique	**0.9654**	**0.9647**	**0.9603**	**-0.0014**	**0.0004**	**-0.0074**

Furthermore, the correlation coefficients are lower than the references [25, 29, 30] in the three directions (H,V,D) for the original and cipher images, respectively. This indicates that our technique is more efficient and effective than alternatives.

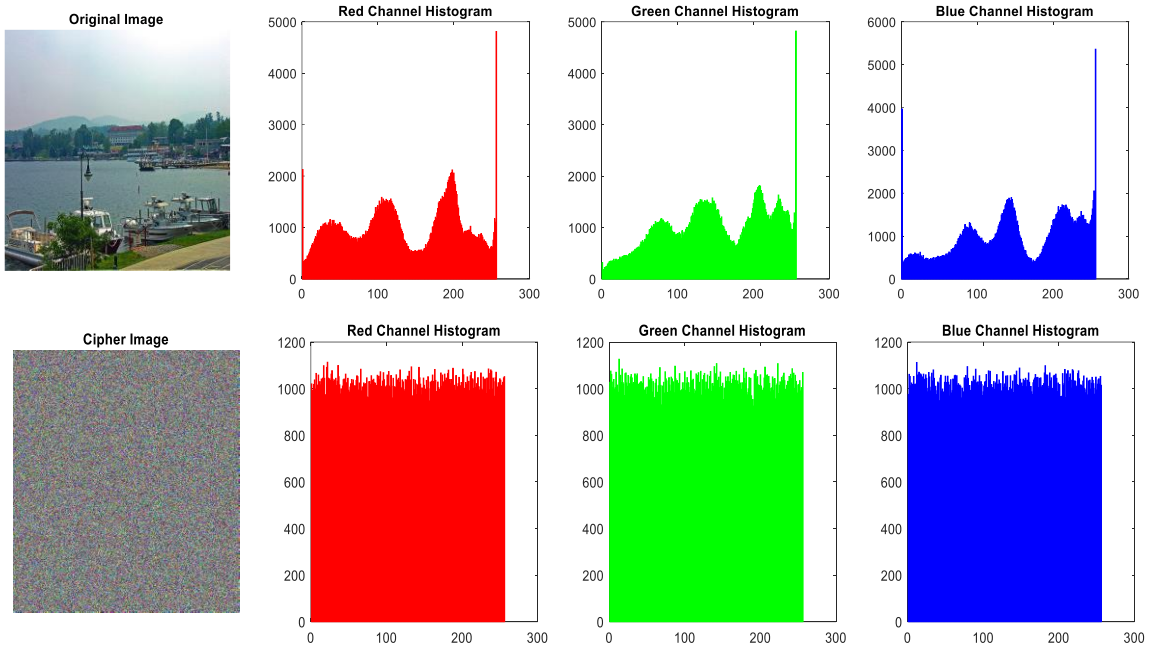


(a)

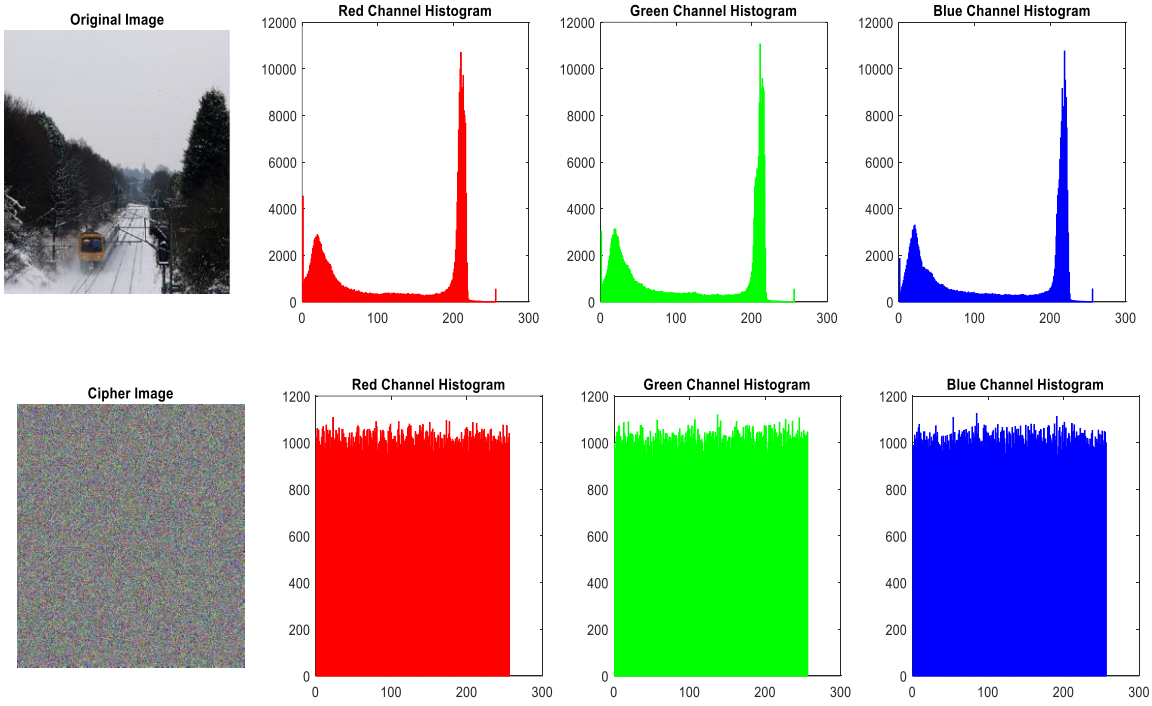


(b)

Figure 6: Histogram analysis of original images (a) and (b) with their cipher images according to R, G, B color.

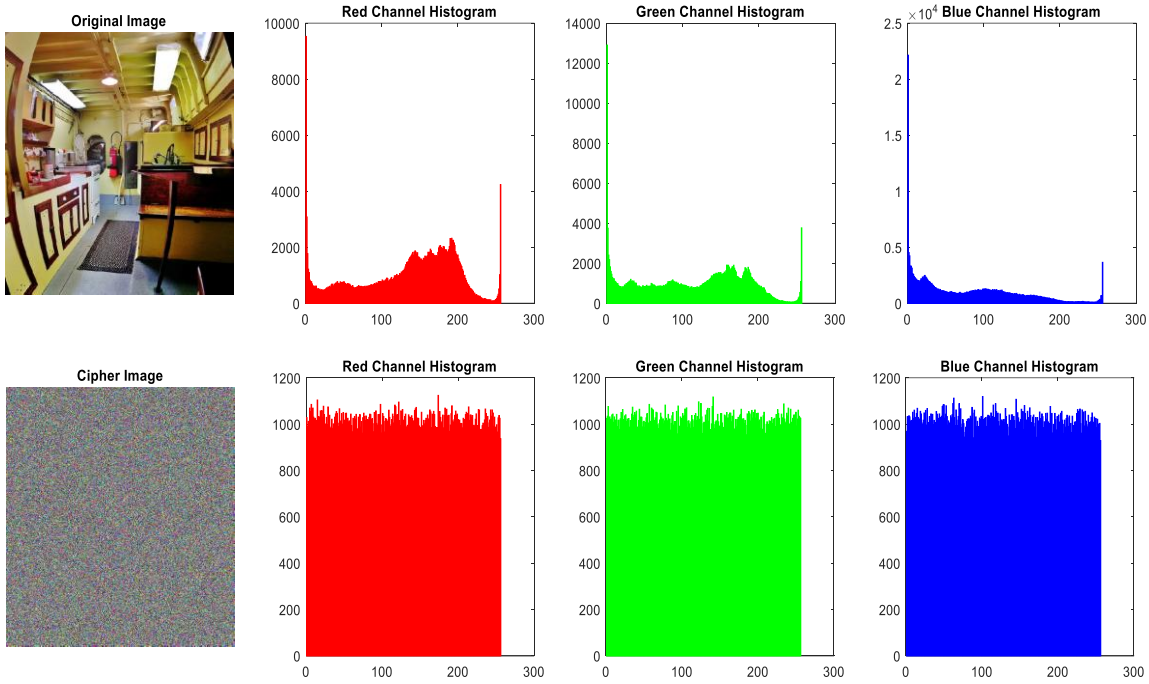


(c)

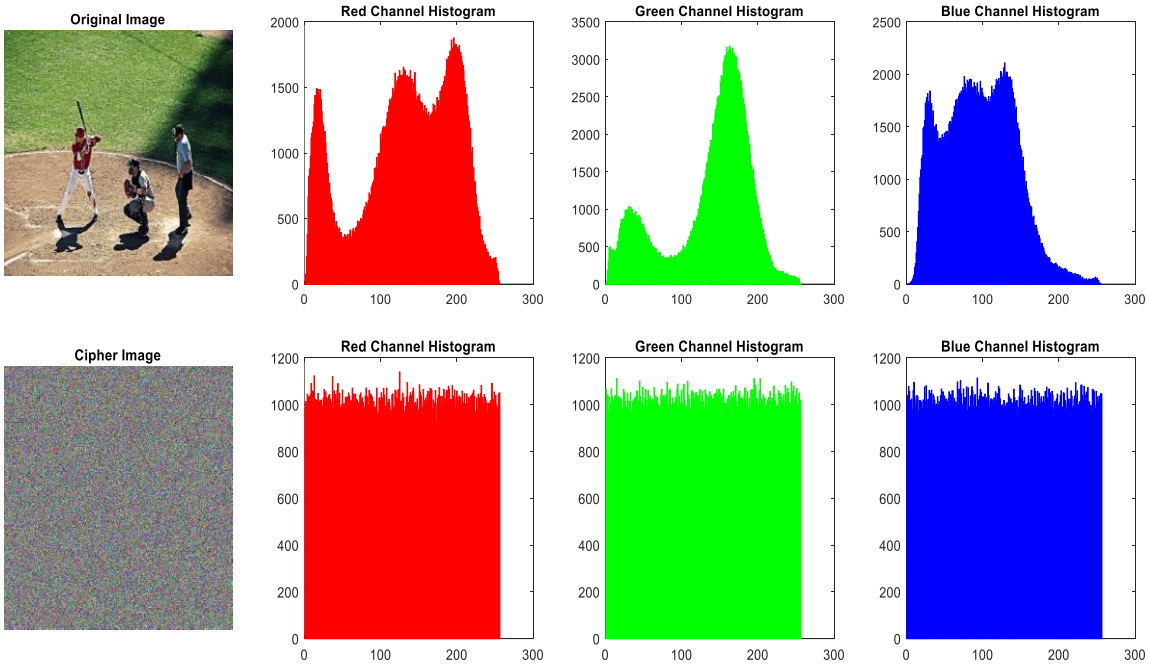


(d)

Figure 7: Histogram analysis of original images (c) and (d) with their cipher images according to R, G, B color.



(e)



(f)

Figure 8: Histogram analysis of original images (e) and (f) with their cipher images according to R, G, B color.

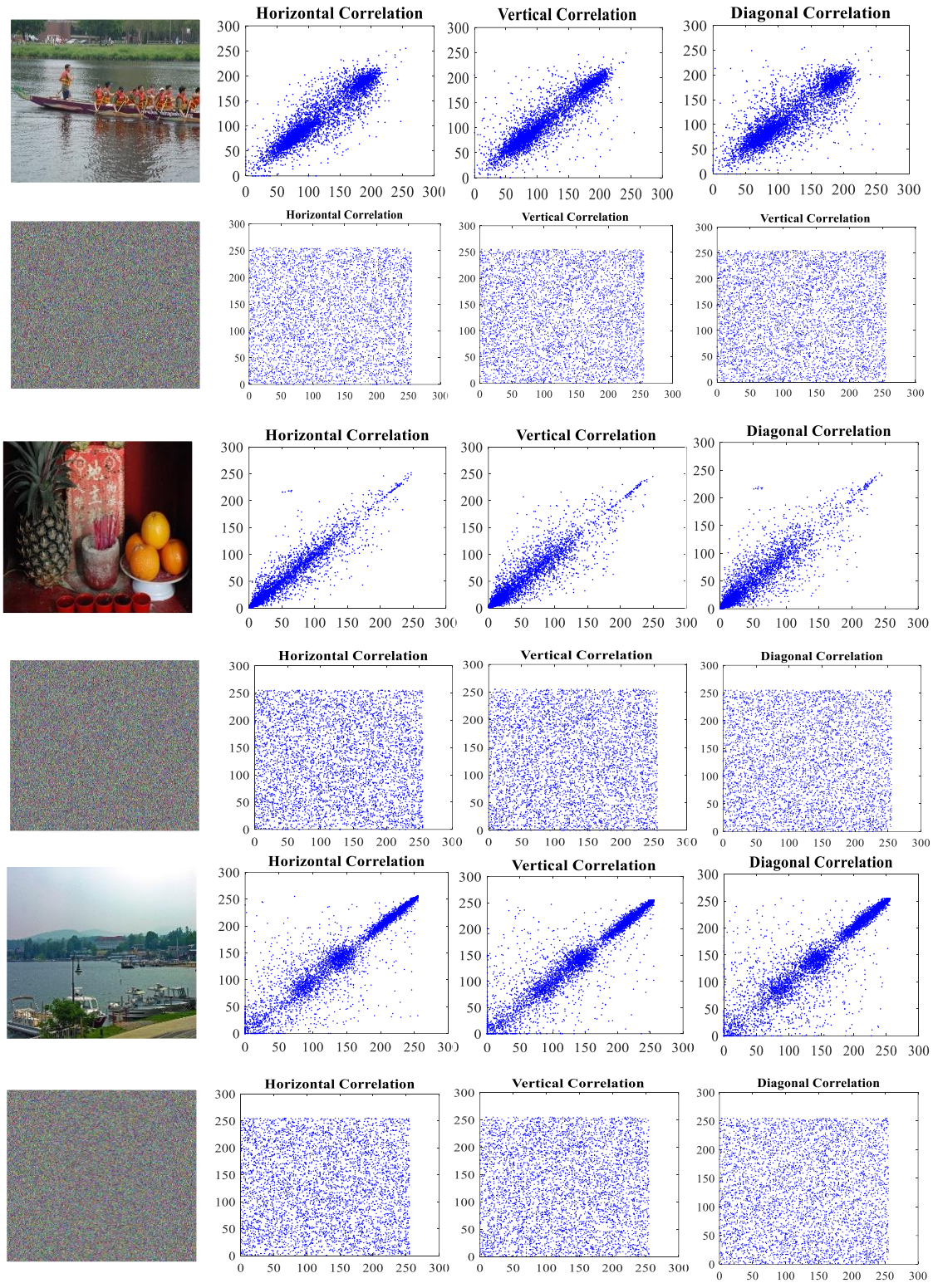


Figure 9: Pixel correlation analysis of original images (a), (b), (c) and their cipher images.

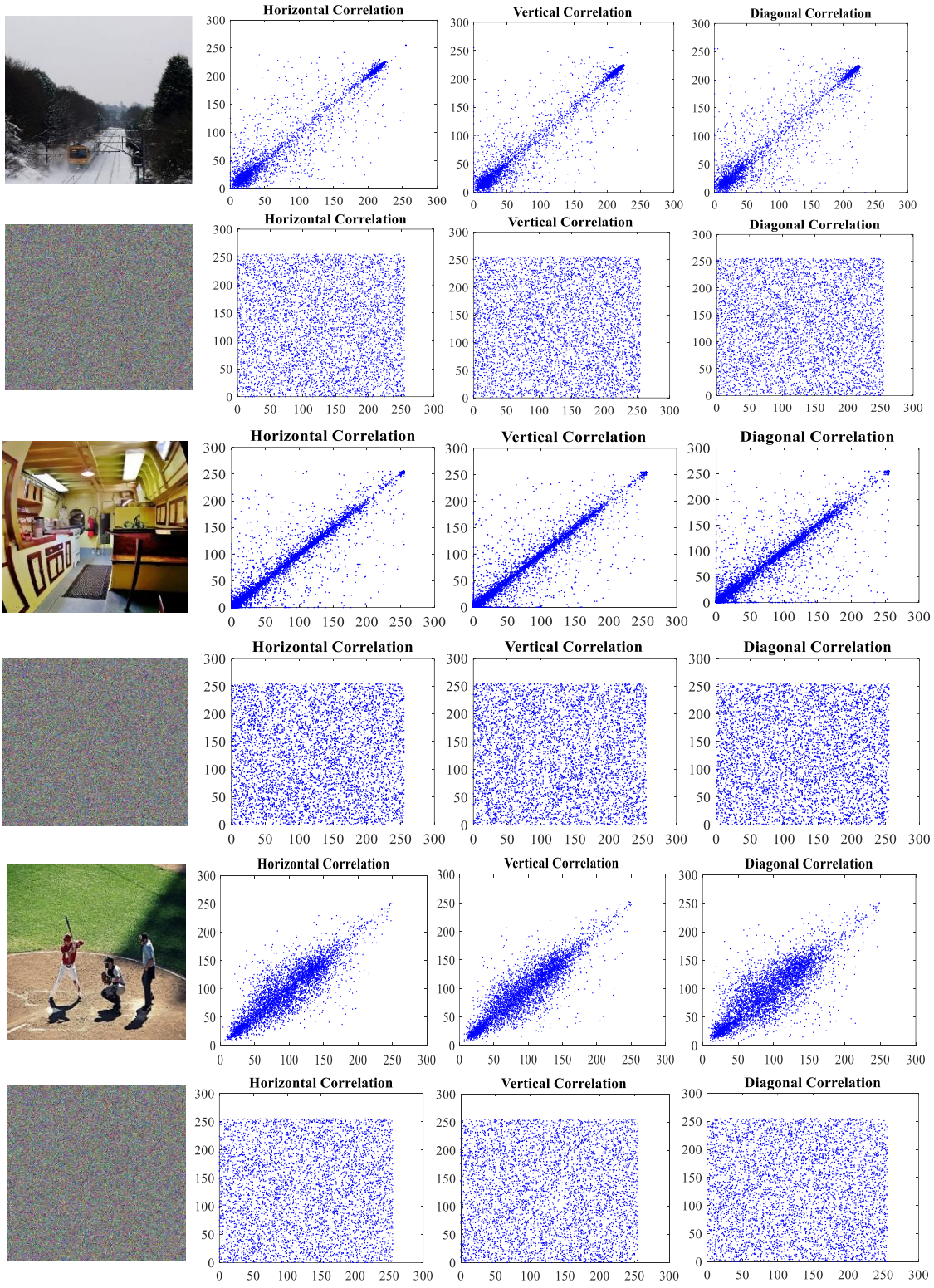


Figure 10: Pixel correlation analysis of original images (d), (e), (f) and their cipher images.

5. CONCLUSION

This research presents the use of 9-dimensional chaotic systems and 3-dimensional bit-level substitutions for secure color image encryption. The original color image is divided into 8 distinct bits for each color channel (R, G, B). Our proposed system generates specific sequences that determine the order in which bits will be substituted, creating an initial scrambling effect. The selected sequences are applied to the 3-bit levels (red, green, and blue) independently, further scrambling the bits within each color channel. Three distinct key matrices are generated using a multilayer differentiation technique applied to the same 9-D chaotic system. These matrices are used to diffuse the scrambled bits, spreading their influence across the entire image and enhancing security. The diffusion process involves interactions between scrambled components and key matrices, creating a complex, interwoven cipher image. The simulation results conclude that a large key space makes brute-force attacks impractical, which leads to high resistance to statistical procedures such as histograms, entropy, and correlation analysis. Furthermore, it performs more efficiently and securely than current methods. Also, it acts as a unique source of complexity and randomness, ensuring the high confidentiality of transmitted data. Finally, we conclude that the decrypted images maintain high visual quality and minimize distortions. As a result, the proposed scrambled encryption technique achieves highly secure transmission of sensitive image data over networks, employing integrity and privacy.

REFERENCES

1. Rizi MH, Seno SA. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things. 2022 Nov 1; 20:100584.
2. Saini R, Joshi K, Punyani K, Yadav R, Nandal R, Kumari D. Interpolated Implicit Pixel-based Novel Hybrid Approach Towards Image Steganography. Recent Advances in Electrical & Electronic Engineering. 2023 Dec 1;16(8):851-71.
3. Li H, Deng L, Gu Z. A robust image encryption algorithm based on a 32-bit chaotic system. IEEE Access. 2020 Feb 7; 8:30127-51.
4. Zhang Q, Xue X, Wei X. A novel image encryption algorithm based on DNA subsequence operation. The Scientific World Journal. 2012 Jan 1;2012.
5. Huang CK, Nien HH. Multi chaotic systems based pixel shuffle for image encryption. Optics communications. 2009 Jun 1;282(11):2123-7.
6. Vaishnavi A, Pillai S. Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods. In Journal of Physics: Conference Series 2021 Jul 1 (Vol. 1964, No. 4, p. 042002). IOP Publishing.
7. Hameed MA, Abdel-Aleem OA, Hassaballah M. A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. Journal of Ambient Intelligence and Humanized Computing. 2023 May;14(5):4639-57.
8. Hameed MA, Hassaballah M, Aly S, Awad AI. An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques. IEEE Access. 2019 Dec 17; 7:185189-204.
9. Hassaballah M, Hameed MA, Awad AI, Muhammad K. A novel image steganography method for industrial internet of things security. IEEE Transactions on Industrial Informatics. 2021 Jan 22;17(11):7743-51.
10. Abdel Hameed M, Aly S, Hassaballah M. An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). Multimedia Tools and Applications. 2018 Jun; 77:14705-23.

11. Hassaballah M, Hameed MA, Aly S, AbdelRady AS. A color image steganography method based on ADPVD and HOG techniques. In Digital Media Steganography 2020 Jan 1 (pp. 17-40). Academic Press.
12. Tiwari A, Srivastava VK. Image watermarking techniques based on Schur decomposition and various image invariant moments: A review. Multimedia Tools and Applications. 2023 Jul 15:1-37.
13. Yoo K, Ahn W, Jang J, Kwak N. Robust multi-bit natural language watermarking through invariant features. In Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers) 2023 Jul (pp. 2092-2115).
14. Gong LH, Luo HX. Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR. Optics & Laser Technology. 2023 Dec 1; 167:109665.
15. Babaei M. A novel text and image encryption method based on chaos theory and DNA computing. Natural computing. 2013 Mar;12(1):101-107.
16. Hazra A, Ghosh S, Jash S. A Review on DNA Based Cryptographic Techniques. Int. J. Netw. Secur.. 2018 Nov 1;20(6):1093-104.
17. Geetha S, Punithavathi P, Infanteena AM, Sindhu SS. A literature review on image encryption techniques. International Journal of Information Security and Privacy (IJISP). 2018 Jul 1;12(3):42-83.
18. Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic baker maps. International Journal of Bifurcation and chaos. 2004 Oct;14(10):3613-24.
19. Corrochano EB, Mao Y, Chen G. Chaos-based image encryption. Handbook of Geometric Computing: Applications in Pattern Recognition, Computer Vision, Neural computing, and Robotics. 2005:231-65.
20. Murillo-Escobar MA, Meranza-Castillón MO, López-Gutiérrez RM, Cruz-Hernández C. Suggested integral analysis for chaos-based image cryptosystems. Entropy. 2019 Aug 20;21(8):815.
21. Jain A, Rajpal N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools and Applications. 2016 May; 75:5455-72.
22. Zhang Q, Liu L, Wei X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU-International Journal of Electronics and Communications. 2014 Mar 1;68(3):186-92.
23. Diaconu AV, Costea A, Costea MA. Color image scrambling technique based on transposition of pixels between RGB channels using Knight's moving rules and digital chaotic map. Mathematical Problems in Engineering. 2014 Jan 1;2014.
24. Gao X. A color image encryption algorithm based on an improved Hénon map. Physica Scripta. 2021 Mar 18;96(6):065203.
25. Li Q, Chen L. An image encryption algorithm based on 6-dimensional hyper chaotic system and DNA encoding. Multimedia Tools and Applications. 2023 Jun 1:1 8.
26. Zhang B, Liu L. Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics. 2023 Jun 5;11(11):2585.
27. Rakheja P, Vig R, Singh P. Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition. Optical and quantum electronics. 2020 Feb; 52:1-21.
28. Russakovsky O, Deng J, Su H, Krause J, Satheesh S, Ma S, Huang Z, Karpathy A, Khosla A, Bernstein M, Berg AC. ImageNet large scale visual recognition challenge. International journal of computer vision. 2015 Dec; 115:211-52.
29. Xu Q, Sun K, Cao C, Zhu C. A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Optics and Lasers in Engineering. 2019 Oct 1;121:203-14.
30. Wei D, Jiang M, Deng Y. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Systems with Applications. 2023 Mar 1;213:119074.

31. Zhang X, Wang X. Multiple-image encryption algorithm based on DNA encoding and chaotic system. Multimedia Tools and Applications. 2019 Mar;78:7841-69.
32. Zhang L, Zhang X. Multiple-image encryption algorithm based on bit planes and chaos. Multimedia Tools and Applications. 2020 Aug;79:20753-71.
33. Hemeida, A., Yahya, H., Al-Sanary, H. Image Segmentation Using Hybrid Optimization Algorithms: Review. Aswan University Journal of Sciences and Technology, 2022; 2(2): 86-104. doi: 10.21608/aujst.2023.183546.1012.
34. Hassan, A., Refaat, M., Hemeida, A. Image classification based deep learning: A Review. Aswan University Journal of Sciences and Technology, 2022; 2(1): 11-35. doi: 10.21608/aujst.2022.259887.
35. Mohamed, A., Mahmoud, M., Hemeida, A. Image segmentation-based optimization algorithms: A Review. Aswan University Journal of Sciences and Technology, 2022; 2(1): 53-72. doi: 10.21608/aujst.2022.261731.
36. Abbas, S., Hassan, T. Image Compression Using Different Optimization Algorithms: A Review. Aswan University Journal of Sciences and Technology, 2021; 1(2): 70-80. doi: 10.21608/aujst.2021.226490
37. Chai X, Gan Z, Chen Y, Zhang Y. A visually secure image encryption scheme based on compressive sensing. Signal Processing. 2017 May 1;134:35-51.
38. Chai X, Zheng X, Gan Z, Han D, Chen Y. An image encryption algorithm based on chaotic system and compressive sensing. Signal Processing. 2018 Jul 1;148:124-44.
39. Wang X, Li Y. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Optics and Lasers in Engineering. 2021 Feb 1;137:106393.
40. Xingyuan W, Junjian Z, Guanghui C. An image encryption algorithm based on ZigZag transform and LL compound chaotic system. Optics & Laser Technology. 2019 Nov 1;119:105581.
41. Munoz-Guillermo M. Image encryption using q-deformed logistic map. Information Sciences. 2021 Apr 1;552:352-64.
42. Hosny KM, Zaki MA, Lashin NA, Fouda MM, Hamza HM. Multimedia Security Using Encryption: A Survey. IEEE Access. 2023 Jun 20.
43. Gabr M, Elias R, Hosny K, Papakostas GA, Alexan W. Image encryption via base-n prngs and parallel base-n s-boxes. IEEE Access. 2023 Aug 2.
44. Mohamed HI, Alhammad SM, Khafaga DS, Hosny KM. A new image encryption scheme based on the hybridization of Lorenz Chaotic map and Fibonacci Q-matrix. IEEE Access. 2023 Dec 8.
45. Tahiri MA, Karmouni H, Bencherqui A, Daoui A, Sayyouri M, Qjidaa H, Hosny KM. New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations. The Visual Computer. 2023 Dec;39(12):6395-420.