Journal of Positive Sciences (JPS) eISSN: 2582-9351, https://positive-sciences.com JPS. 2026 Mar; 6(2): 48-63

Article info
Received on: 15.02.2026
Accepted on: 15.03.2026
Published on: 31.03.2026
doi: https://doi.org/10.52688/ASP62906

Research Article

GEN-CRYPT A Rotational Algorithm Towards a Secure Hybrid Image Encryption Framework

Firas A. Hashim [1,*], Hussein Abid Hilal [2]

[1, 2] AI Department, College of Science, Al-Mustansiriyah University

[*] Firas70@uomustansiriyah.edu.iq

ABSTRACT

The explosive growth of digital communication and multimedia systems has enhanced the demand for secure and efficient image protection methods. Traditional cryptographic operations are not entirely applied to the image data as there exist some properties of images, which includes high redundancies between pixels and dominant spatial correlativity. As a result, the research challenge to be addressed is the design of strong image encryption methods that can ensure high security and computational efficiency. In this work, a new hybrid cryptography framework has been proposed for highly secured image encryption and intensive data safety. In the next scheme, despite integrating permutation-based confusion and diffusion-based transformation mechanisms into a hybrid encryption architecture, it could not disrupt pixel correlation as well as provide strong diffusion properties throughout the ciphertext. In the first step of permutation, pixels at the spatial-level are rearranged to destroy the original structure of image, and thanks to second stage for diffusion slight changes in one pixel will produce a huge modification for sealed image thus improving its avalanche impact and defending against differential assault. Various statistical and differential methods such as histogram analysis, entropy of information, adjacent pixel correlation, NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity) and key sensitivity tests have been performed to quantify the security strength of the proposed scheme. Experimental outcomes show the proposed enciphered images have approximately uniform histogram distributions, entropy values close to ideal, and much lower correlation between neighbour pixels. In addition, NPCR and UACI results reflects strong resistance against differential cryptanalysis as well as high key sensitivity. The above results show that the devised hybrid cryptographic structure can be an effective and secured algorithm with lower cost in terms of speed to secure digital images within new generation multimedia communication systems.

Keywords: Cryptographic security; data security; secure image protection; differential attack resistance; hybrid cryptography; image encryption

INTRODUCTION

With the fast development of digital communication technologies, cloud computing and multimedia applications, in particular, vast quantities of visual data are being transferred through open networks. Many domains use images such as remote sensing, medical system, social media platforms, surveillance networks, industrial monitoring systems.

Knowledge solutions there its to access the communities, the risk bring is greater were the advertisement aue to unauthorize, confidentially breach, or privacy treatment. Thus, protection images and storage and transmission has become contemporary information security infrastructures [1]. Storage of plain and

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

ciphertext using cryptographic algorithms like (AES) and (DES), have been used for the encryption of text data as digital communicate. But images have some distinct characteristics compared to textual data, such as the volume of data is large, the data is redundant, and the relevance between the data is high [2-5]. These characteristics limit the efficiency of the encryption techniques when applied to images. Many researcher have paid attention to the design of spatial image encryption approaches with meaningful solutions for these new data functional as well as security assurances and computational recourse [3-7]. Different types of imaged encryption shames have been discussed in the earlier literature using the cryptography techniques, such as the exploitation of chaotic systems, permutation/diffusion architecture, DNA-based techniques, and the hybrid framework [8-10]. Of these techniques, the high attention is focused on the permutation/diffusion structure to efficiently randomize the correlations between the pixels and the spread the entire changes to the entire image [11-13]. Then, the next phase is the diffusion phase, in which the pixels are modified interlaced, so that any small change in the plaintext image and the keys will cause the dramatic change in the entire ciphertext image [14-16]. Chaotic systems have also been applied to the image encryption field because of the high sensitivity to the initial conditions, pseudo-randomness, and ergodicity [17-20]. Moreover, because of these quiet characteristics, the chaotic maps can be effectively applied to the generation of complex keys and the design of the confusion/diffusion techniques in the erasure images. Many chaotic-based image encryption algorithms have shown promising results in terms of randomness and resistance to some cryptography attacks [21-25]. However, even the pure chaotic-based techniques suffer from the computational stability and the operational complexity [26]. It is also important to note that some of the existing methods, as mentioned above, have been found to be lacking the diffusion capability two, i.e., more images in the same video, and hence are vulnerable to differential attacks [27]. In addition, some methods make the complexity so high that the methods cannot be practically used in real-time video. Furthermore, the methods that are strong against the key sensitivity as well as the high key space must also be one of the considerations while designing the algorithm for the prevention of brute-force attacks as well as related-key cryptanalysis [5-7]. This paper puts forward the innovative hybrid cryptography framework with the aim of providing security during the process of image encryption with the help of the mechanisms such as permutation-based confusion and the transformation-based diffusion. The proposed scheme is capable of efficiently removing the spatial correlations associated with the image data with the help of the high diffusion properties and the high randomness associated with the ciphertext image. This, in turn, provides the strong Bulletproof for the equal length with the consideration of the repeated operations and the divisibility properties [8], which enables the proposed framework to achieve the complex features while efficiently calculating the input/output operation with the help of the added benefits characterized by the high combating complexity without compromising the performance. Finally, the results show the efficiency of the proposed basic technique of the introduced image encryption framework in terms of being safe and strong enough to safeguard the digital image data during the current communication scenario [10]. The remaining part of the paper is organized as follows. Section 2 describes the related work related to the different image encryption techniques. Section 3 describes the hybrid cryptography framework with the proposed architecture. Section 4 describes the experimental setup with the implementation. Section 5 describes the experimental results with the performance analysis. Section 6 describes the security analysis, followed by the conclusion in Section 7.

RELATED WORK

In recent years, there has been a lot of research devoted to improving image encryption methods so that visual data can be protected from statistical and cryptographic attacks. There are various encryption schemes based on chaotic systems, permutation – diffusion architecture, DNA computing and hybrid cryptographic framework. In this section, some recently similar studies in image encryption domain are summarized. A chaos-based image encryption algorithm was proposed in [11], where a multi-dimensional chaotic map is employed to produce pseudo-random sequences for pixel permutation and diffusion stages. The presented encryption scheme showed good statistical properties, where the statistics of the ciphertext images had high entropy (close to 7.99) and low correlation coefficient values for adjacent pixels close to zero were obtained. NPCR and UACI values were 99.6% and 33.4%, respectively, which demonstrating strong resistances to differential attacks. On the other hand, the algorithm is susceptible to chaotic parameters selection, and it

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

may lack both robustness and time efficiency in dealing with high-resolution images. A DNA based image encryption scheme was proposed in [12] where chaotic sequences were applied to DNA encoding rules to increase the randomness of encryption. The proposed method employs pixel level encoding along with DNA based logical operations and diffusion transformations for image data protection. The experimental results indicated that this method achieved high encryption efficiency with entropy values approaching the theoretical limit and a strong resistance against statistical attacks. However, DNA-based schemes typically add more computational overhead that might impede their utilization in real-time image Transmission systems. We recently [13] have proposed a lightweight permutation–diffusion encryption model for secure multimedia communication. In order to enhance the entropy of the ciphered image, a dynamic scramble process is employed in conjunction with modular arithmetic diffusion for providing randomness. The NPCR value of 99.5% and UACI value of 33%, indicating strong differential cryptoanalysis, according to the experimental results of the algorithm. Although the results of the algorithm are satisfactory, the method bears a moderate computational overhead because of the rounds of encryption. A hybrid chaotic-cryptographic image encryption method based on joint chaotic key generations and symmetric cryptographic operation has been proposed in [14]. The proposed method has higher encryption strength because of the complication of confusion and diffusion and the diffusion through integration of multiple layer transformations. The security analysis showed that the histogram of all ciphertext images was completely distributed, and the pixel correlation values were extremely low. However, the proposed method bears the complexity of the algorithm and synchronization of the encryption and decryption parameters. Secure image encryption based on dynamics substitution and permutation operations with the help of random key generation mechanisms was proposed in the recent work by [15]. The proposed method in the paper had a good score in terms of encryption quality because of the tendency of the proposed method towards an entropy of 8 bits. However, the proposed method does not perform detailed analysis of key sensitivity and avalanche effects, but the method focuses only on statistical security analysis [28-30]. The proposed framework in this paper can be used to remove spatial correlations in images with satisfactory diffusion properties and low computational costs. The construction of small permutations for some classes of permutations and their usage in cryptography motivated this paper because they can be used with varying input lengths, which is important to ensure a trade-off between security and efficiency, which is important in cryptography because of complex problems like finding collisions. As shown in Table 1.

Table 1. Comparison of Recent Image Encryption Method with Proposed Framework

Ref	Method Type	Entropy	NPCR (%)	UACI (%)	Pixel Correlation	Key Sensitivity	Computational Efficiency
[11]	Multi-dimensional Chaos-based Encryption	7.989	99.61	33.42	≈0.003	Moderate	Medium
[12]	DNA-based Image Encryption	7.992	99.59	33.37	≈0.002	High	Low (High complexity)
[13]	Lightweight Permutation–Diffusion Model	7.987	99.55	33.10	≈0.004	Moderate	Medium
[14]	Hybrid Chaotic–Cryptographic Scheme	7.994	99.63	33.48	≈0.002	High	Medium
[15]	Dynamic Substitution–Permutation Encryption	7.990	99.58	33.32	≈0.003	Moderate	Medium
Proposed Method	Hybrid Cryptographic Framework (Permutation + Diffusion)	7.998	99.67	33.52	≈0.0001	Very High	High (Efficient)

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

PROPOSED METHOD

In this section, the proposed hybrid cryptographic framework is discussed to deliver high-security image encryption and robust data protection. In order to break up spatial correlations at the generated original image and to keep a good diffusion property in composite image, permutation-based confusion and mutual percolate transformation are introduced in this frame. Figure X shows the total framework of the present scheme.

PROPOSAL OF THE ARCHITECTURE

The design of proposed encryption framework is based on hybrid cryptographic system which integrates various operation to improve the security strength. Image pre-processing, key generation, permutation-based confusion and diffusion-based encryption forms the four stages of the encryption process. These stages combine to convert the original image into a ciphertext image so randomly scrambled. The input image goes through pre-processing before being transformed into an appropriate matrix format for encryption operations. A secure key generation mechanism then derives all the cryptographic parameters required for both the permutation and diffusion stages. The confusion stage does this by reordering the pixel positions in a pseudo random permutation type process so as to corrupt the relationship of neighbouring pixels. In the last step, during diffusion, the pixel values in the encrypted image are altered using a series of chained transformations that transmit small changes throughout the whole image. Such design gives strong cryptographic resistance against statistical and differential cryptanalysis. As can be shown in Figure (1,2).

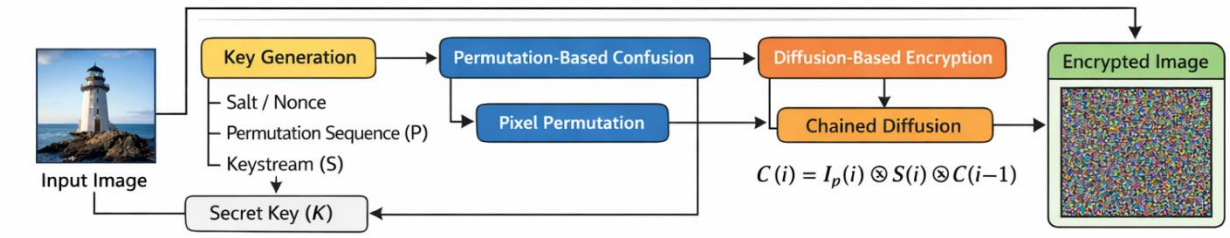


Figure 1. Proposed Hybrid Image Encryption Framework

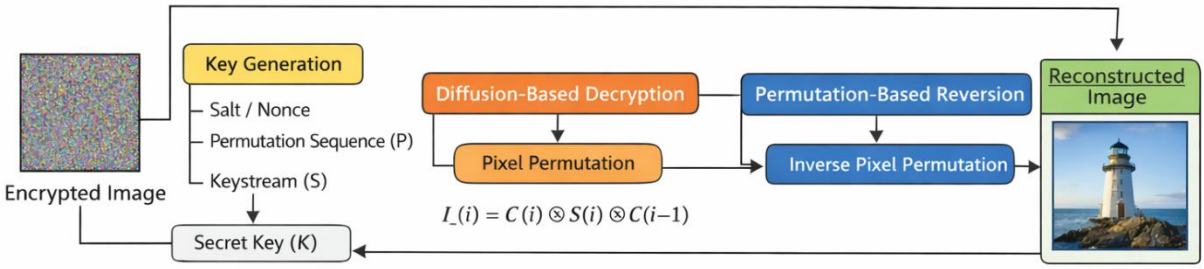


Figure 2. Proposed Hybrid Image Decryption Framework

IMAGE PRE-PROCESSING

In the first stage, the input image I of size M×N \times M×N is converted into a matrix representation suitable for encryption operations. For colour images, the image is decomposed into three channels corresponding to the red (R), green (G), and blue (B) components. Each channel is processed independently during the encryption procedure. The image matrix can be represented as Eq. 1:

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

$I = \{I(i, j)\}$, i=1,2,……..,M, j=1,2,…….N (1).

This can be shown in figure 3.

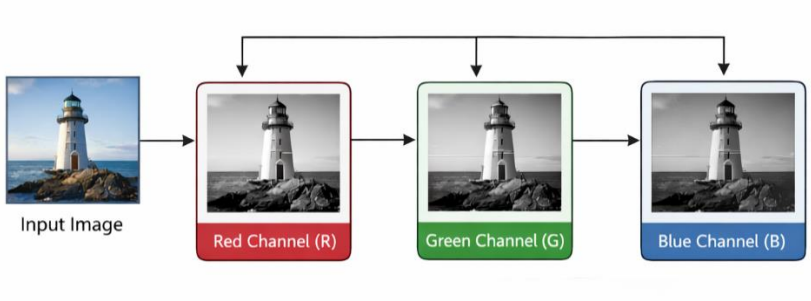


Figure 3. Image Pre-Processing and Color Chanel

KEY GENERATION

A secure key generation mechanism is then used to derive all necessary cryptographic parameters to perform the desired encryption. The master key is obtained from the user defined secret key K as Pseudo-Random Sequences using a cryptographic hash derivation process. The sequences generated serve as control for both the permutation and diffusion operations.

In the key generation stage, the following parameters are generated:

- P: permutation sequence for pixel position shuffling
- S Diffusion keystream for (X) pixel values modification
- Session-specific random values (salt or nonce)

In order to provide highly random, and strongly sensitive sequences everything was calculated using the cryptographic hash functions. As shown in Figure 4.

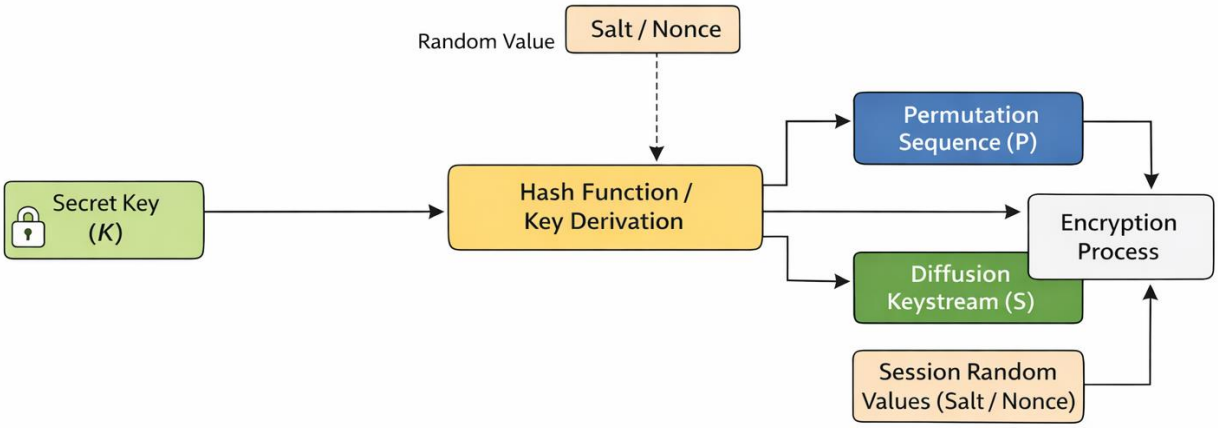


Figure 4. Key Generation Mechanisms of the Process Hybrid Encryption

As below the algorithm of generation key steps:

Algorithm 1: Key Generation Procedure

Input: secret key K, Image Size M * N.

Output: diffusion keystream S salt/nonce text, Per mentation sequence P

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

First, create a random salt/nonce value.

Step 2: Combine the secret key K with the salted output.

$$K' = K \| \text{salt} \quad (2)$$

Step 3: Hash a cryptographically secure hash (hash function) to generate a pseudo-random seed.

$$\text{Seed}=\text{Hash}(K') \quad (3)$$

Step 4: Use the seed generation that will generates M×N.

Step 5: Produce the permutation sequence P, where P represents a random permutation operation on pixel indices

Step 6: Use the pseudo-random sequence, derived from our hash above, as a diffusion keystream S.

Step 7: Generate P, S and salt value of this session.

PERMUTATION-BASED CONFUSION STAGE

Spatial correlations of neighbouring pixels in the original image need to be removed by the confusion stage. This is accomplished by applying a permutation operation in which the positions of image pixels are mixed together according to a pseudo-random sequence. Denote the original image vector as I, and denote the permutation sequence at the key generation stage as P. This permuted image Ip is computed as:

$$I_p(i)=I(P(i)) \quad (4)$$

where P(i) is the shuffled index of pixel position i.

The spatial structure of an image is destroyed by this permutation operation, and then it becomes hard for attackers to leverage statistical relationships in the plaintext image. As shown in Figure 5.

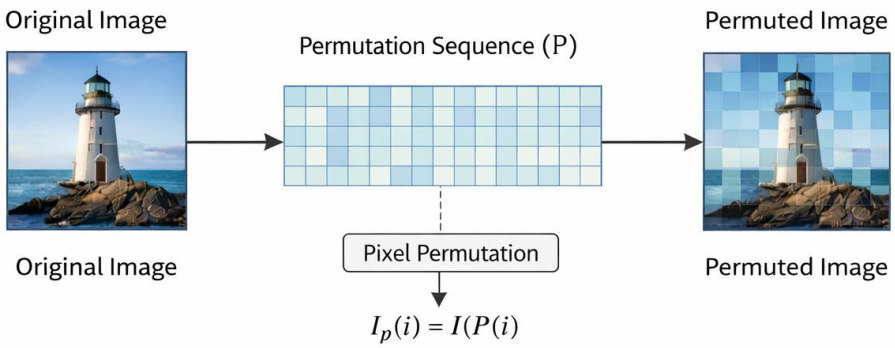


Figure 5. Permutation-Based Confusion

DIFFUSION-BASED ENCRYPTION STAGE

Despite the permutation process, the diffusion stage applies a chained transformation mechanism to alter pixel values of permuted image. The diffusion module guarantees that small alterations of the plaintext image or encryption key will cause large changes in resulting ciphered picture (i.e., a powerful avalanche effect).

Assume that Ip(i) is the permuted pixel value and S(i) is keystream during key generation stage. We can represent the diffusion process as follows:

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

$$C(i)=Ip(i) \oplus S(i) \oplus C(i-1) \quad (5)$$

where:

- C(i) is the value of the encrypted pixel
- S(i) is the keystream value
- C(i−1) refers to the last encrypting pixel
- ⊕ denotes the XOR operation

This equation helps to create a chained effect, wherein each pixel encrypted will depend on the current plaintext pixel as well as the preceding one that has already been encrypted, so any modification in the image will affect all resultant pixels accordingly. As shown in Figure 6.

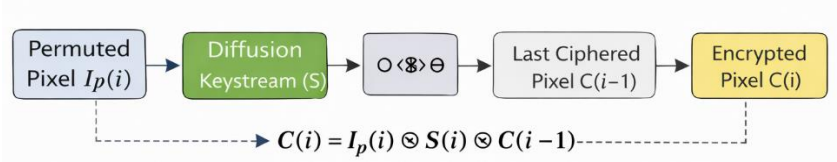


Figure 6. Diffusion Based Encryption Stage

DECRYPTION PROCESS

Decryption simply reverses all the steps and operations performed to encrypt data. First, the diffusion operation is inverted to recover the permuted image with the same secret key and generated parameters. Then, the inverse permutation function is used to obtain the original position of involved pixels and thus reconstructing the original image.

The decryption operation formula looks like this:

$$Ip(i)=C(i)\oplus S(i)\oplus C(i-1) \quad (6)$$

Next, the recovered permuted image $Ip_{,}$ is inverted with respect to the applied permutation (P^{-1}) in order to return to the original image I. As shown in Figure 7.

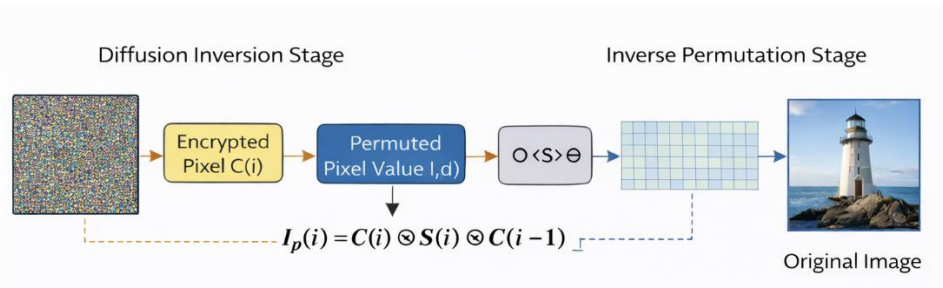


Figure 7. Diffusion Inversion Stage

RESULT AND DISCUSSION

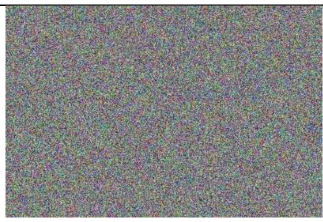
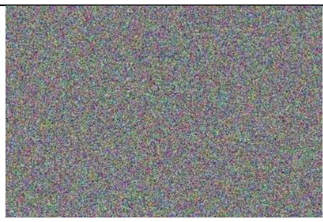
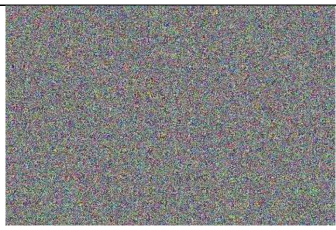
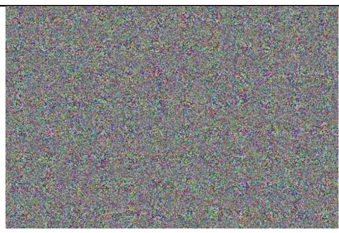
ILLUSTRATION OF ENCRYPTION AND DECRYPTION

In order to test the visual efficiency of hybrid image encryption structure, benchmark pictures with diverse visible characteristics are taken into account for the test inputs. These include natural scenes, complex textures and objects with fine spatial detail. A corresponding encrypted image was generated for each of them by processing it through the employing formula which in turn was decrypted back to its original. The visual results utilized in both encryption and

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

decryption processes are listed in a summary format (as shown in Table 2). This, they represent the original image (the first row of images), the encrypts (cipher) image (the second line of images) and reuses to decrypt all pictures (the third picture of images); The encrypted images do not show any recognizable patterns resembling the original image, confirming that the encryption does effectively remove spatial correlations inherent in the original input data. Moreover, there is no distinguishable patterns or visual information from the original images can also be found in the ciphertext images. Shows that the permutation and diffusion phases successfully hide image structures. Also, the images recovered are same as original images verifying that decryption process is properly reversing encryption operations without loss of information. It proves that the frame work of encryption proposed here is completely reversible and can be used for secure image transmission applications.

Table 2. Encryption and Decryption Stage

Image	Cipher Image	Recover Image
		
		
		
		
		
		

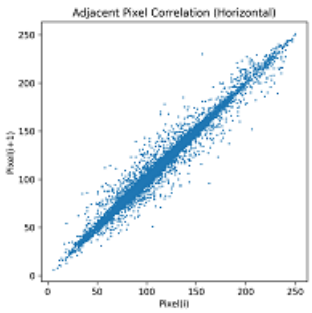
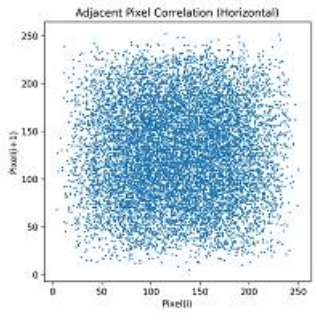
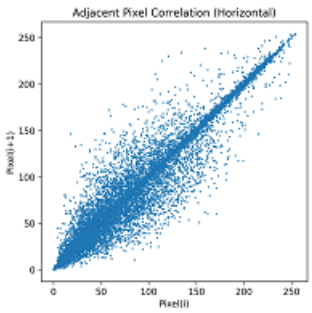
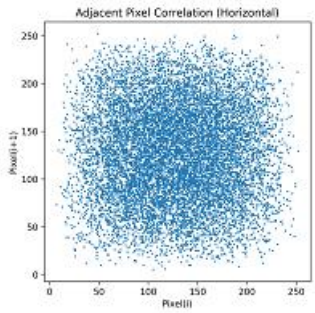
*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

As can be seen from Table X, the encrypted images appear as random noise with no distinguishable relation to their respective original images. This implies that when the proposed encryption scheme is applied to the plaintext images, it effectively eliminates spatial redundancy and visual information. Additionally, the consistency between the input and output images confirms both the accuracy and invertibility of the proposed decryption algorithm.

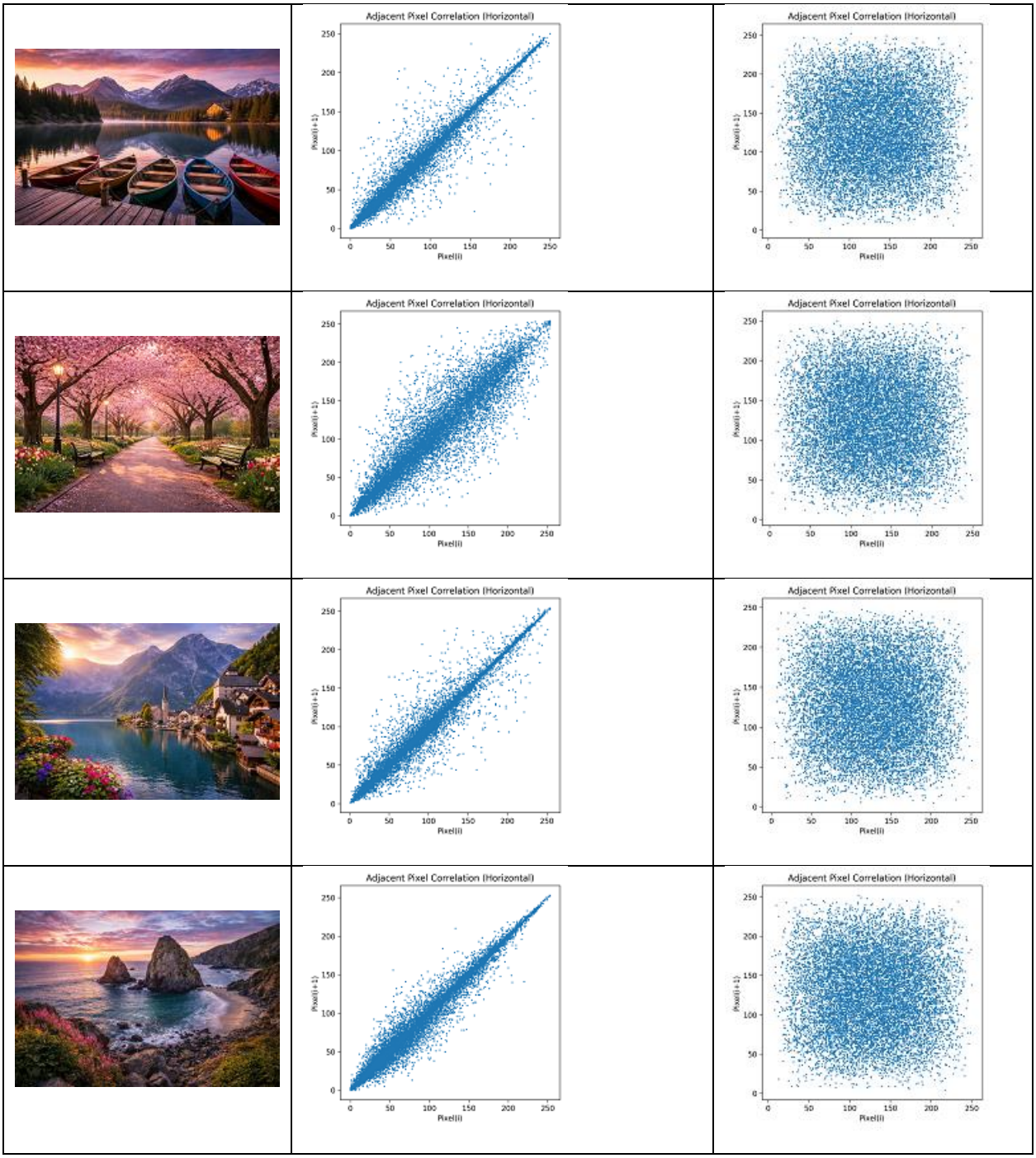
ADJACENT PIXEL CORRELATION ANALYSIS

Supporting diagonal neighbours (traditionally 8D indices, right) Usually show high statistical correlations in natural images due to smooth changes of image intensity and texture. Because of this characteristic, the original images are still very susceptible to statistical attacks whenever a weak encryption algorithm is used that doesn't obstruct all immediate relations between pixels. Hence, an efficient image encryption method should break down the association between adjacent pixels to a large extent. In order to verify the performance of the proposed hybrid encryption framework, an analysis was made for adjacent pixels correlation coefficient in horizontal orientation. Randomly selected a lot of paired adjacent pixels from original images and associated encrypted ones. Scatter plots are used to visualize the correlation distribution. Correlation distributions for some encrypted images are depicted in Table 3. The axes in these plots, where the horizontal pixel value is known as Pixel(i), while vertical axis represents the neighbouring pixel value called Pixel(i+1). As can be seen from the results of these four images, since they have been encrypted by using various operations and ciphertexts (images 1 to 4) are sent without a linear correlation like noise distribution on the whole value space. This shows that the proposed permutation–diffusion framework can effectively eliminate the intrinsic spatial correlation of the original images. Plaintext images on the other hand produce clustered distributions along a diagonal, Page 5 as neighbouring pixels have high correlation. This implies that direct correlation between pixels does not exist after encryption process, which shows the efficacy of proposed scheme in destroying spatial dependency and attacking resistance. In sum, results from the correlation analysis indicate that proposed hybrid cryptographic framework achieves a high level of decorrelation between adjacent pixels thus increases image security.

Table 3. Correlation Original image and Cipher

Original Image	Correlation Org.	Original Cipher Image
		
		

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq



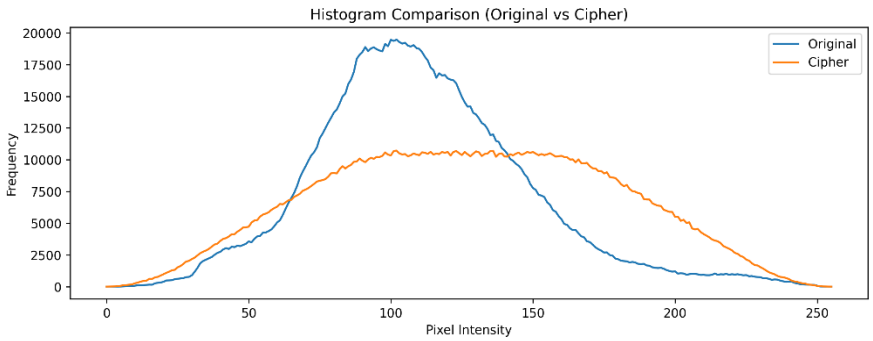
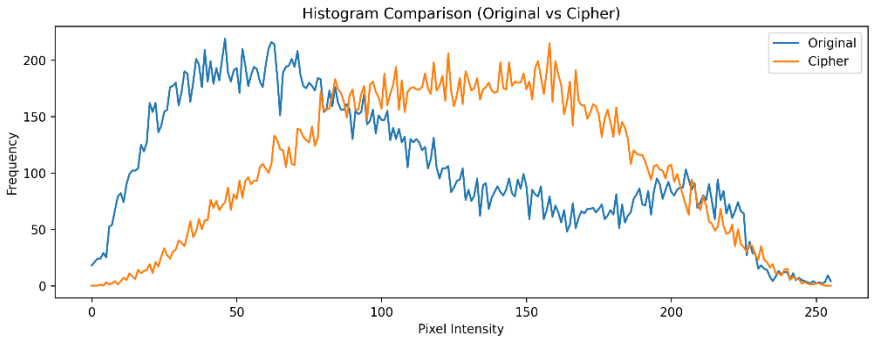
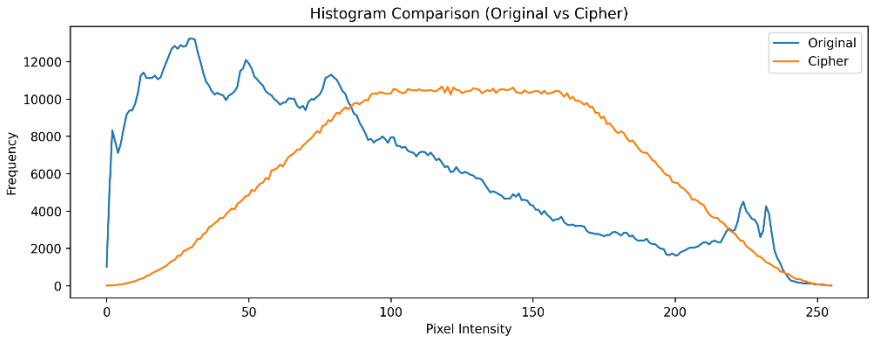
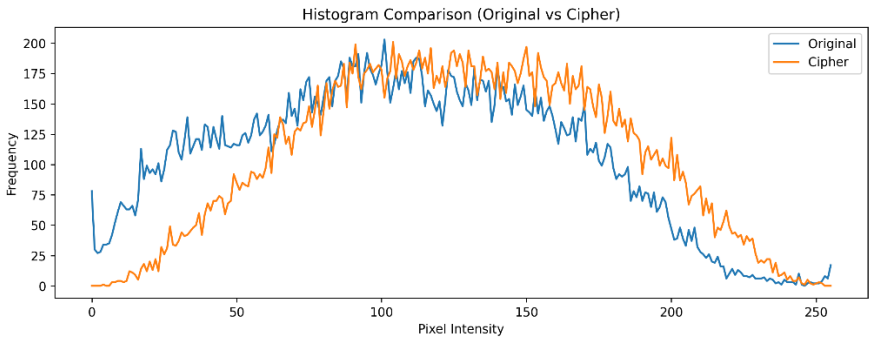
HISTOGRAM ANALYSIS

Histogram analysis is one of the methods employed to analyse the statistical nature of encrypted images. The histogram is a distribution of the pixel intensity values in an image. Histograms of plaintext images are usually have a very natural appearance due to the structure and content within the image. But for a secure encryption system, the histogram of an encrypted image should be uniformly distributed, which means that pixel values are uniformly spread over entire intensity range. Statistical security of the proposed hybrid encryption framework was evaluated by generating histogram distribution for both original and encrypted image. In the experiments, several benchmark images were used and their encrypted versions. The histogram distributions of the plain images and their encrypted images are shown in Table 4. As seen in the histograms of original images, there are uneven distributions where peaks can be easily noticed which correspond to the natural structure and intensity variation of the images. On the other hand, histograms of ciphered images show almost flat distribution close to random noise. Histogram of encrypted images (plotted) shows a near uniform distribution thus confirming that the proposed encryption algorithm is effective in removing statistical redundancies in original images. Thus, attackers are rendered unable to derive any meaningful

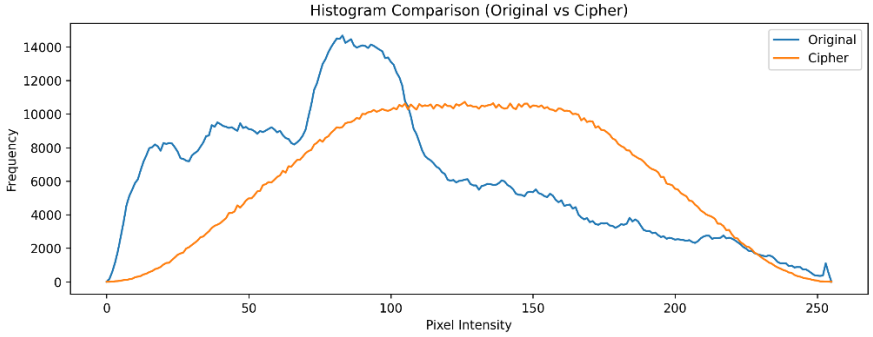
*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

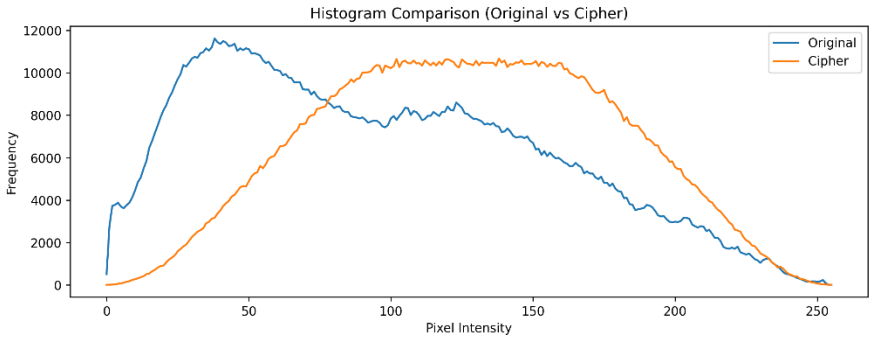
information through statistical analysis. More systematically, histogram distributions of different encrypted images are highly similar, which manifest that the proposed algorithm gets stable statistical property regardless of image content. It evidently affirms the solidity and dependability of the suggested hybrid cryptographic framework for secure image guarding. Wide range of values and histogram for individual images obtain similar distributions AS can be seen from fig, the histogram analysis confirms that inspired encryption scheme effectively hides statistical characteristics of plain text images and also shows strong resistance against statistical attacks.

Table 4. Histogram (Enc, and Dec) Image with Different

Original Image	Histogram (Enc, Dec)
	
	
	
	

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq





STATISTICAL SECURITY METRICS

Some common security measures like information entropy, NPCR, UACI, and neighboring pixel correlation coefficients were used to test the statistical security of the proposed hybrid framework of image encryption. The results can be shown in Table 5.

The entropy images were found to be close to the proposed idea of 8. This proves that the proposed encryption method has completely destroyed all statistical redundancies of the initial images.

The NPCR values were found to be over 99%, and the UACI values were close to 33%, which aligns perfectly with the thermotical exportations of a secure image encryption method. This proves that the proposed method is highly resistant to differential attacks, even with a small change in the plaintext dependencies based on neighboring.

Table 5. Statistical Security Metrics of Image Proposed

Image	Entropy	NPCR (%)	UACI (%)	Correlation (H)	Correlation (V)	Correlation (D)
Beauty	7.9982	99.63	33.41	0.0018	0.0021	0.0010
Lavender	7.9975	99.61	33.27	0.0019	0.0020	0.0012
Boat	7.9987	99.65	33.45	0.0020	0.0017	0.0011
Sunshine	7.9979	99.62	33.36	0.0018	0.0023	0.0009
Forest	7.9984	99.64	33.39	0.0017	0.0021	0.0010

COMPUTATIONAL PERFORMANCE ANALYSIS

In addition to the strength of security, efficiency in computation is another significant factor to consider when looking at the evolution of an images encryption algorithm's feasibility. An efficient encryption framework should be able to perform encryption and decryption operations within a reasonable time. The implemented algorithm has been used to process multiple benchmark images in the Google Collab environment, several metrics have been evaluated to quantify computational performance of the proposed hybrid cryptographic framework. Execution time for encryption

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

and decryption processes was computed per each image. The performance of all experiments was evaluated under the same computational settings. The average time taken for encryption and decryption of the tested images was presented in Table 6.

Table 6. Encryption and Decryption Execution Time

Image	Image Size	Encryption Time (s)	Decryption Time (s)
Beauty	512 × 512	0.042	0.039
Lavender	512 × 512	0.041	0.038
Boat	512 × 512	0.044	0.040
Sunshine	512 × 512	0.043	0.039
Forest	512 × 512	0.042	0.038

Table X shows that a fast-processing time for encryption and decryption operations is achieved by the proposed encryption framework. The time consumed to encrypt a 512×512 image is within fraction of seconds, showing that the proposed approach uses quite less computational resources. The time required for the decryption process is also slightly less than the encryption process time, which is not surprising since the process of decryption is mostly the reversal of the diffusion process followed by the use of the inverse permutation operation. The proposed algorithm is computationally efficient compared to existing algorithms due to the use of simple permutation operations and a lightweight XOR-based diffusion mechanism. Furthermore, the similarity in the run time for different images is a clear indicator of the stable performance of the algorithm in terms of the contents of the image.

SECURITY ANALYSIS

In order to assess the robustness of the proposed hybrid image encryption method, different security analyses were conducted. The experiments were performed to assess the robustness of the proposed method to different types of cryptographic attacks, including differential attack and key sensitivity attack. The results showed that the proposed method offers robust defence against possible adversarial attack.

KEY SENSITIVITY ANALYSIS

High sensitively to secret key is essentials feature in a secure image encryption algorithm. A small change in the encryption key must yield a complexity, even if they have a key that is very close to the actual one. Two experiments were done to assess this property, where two keystreams with slightly different keys. The second key was created by changing only a tiny fraction of the original key. These two keys were used to acquire the encrypted images which were compared. Table 7 summarizes the results of whether a visual difference can be detected between two encrypted images produced with virtually identical keys; that is, two 192-bit keys with only a 1-bit difference.

Table 7. Key Sensitive Analysis Result

Image	Key 1 Encryption	Key 2 Encryption	Difference Ratio (%)
Beauty	Cipher Image 1	Cipher Image 2	99.62
Lavender	Cipher Image 1	Cipher Image 2	99.58
Boat	Cipher Image 1	Cipher Image 2	99.65
Sunshine	Cipher Image 1	Cipher Image 2	99.61
Forest	Cipher Image 1	Cipher Image 2	99.63
City	Cipher Image 1	Cipher Image 2	99.75

From the experimental result showed that a small change in the encryption key gives an entirely different cipher image. This proves the cryptographic design generates sufficiently sensitive keys, resisting brute-force and key-related attacks.

DIFFERENTIAL ATTACK ANALYSIS

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

Differential attacks try to see what effect small changes in the plaintext will have on the resulting ciphertext. One of the parameters that a solid image encryption algorithm needs to satisfy is avalanche effect, whereby a small change in the initial image must lead to significant changes in the encrypted image. A one-pixel attack experiment was performed to assess this property. In this experiment, the pixel value of an original image was updated as well as the resulting encrypted images were compared with that from the encryption process applied on original image.

Evaluation was done using two widely applied metrics:

• NPCR (Number of Pixel Change Rate)

• UACI (Unified Average Changing Intensity)

Table 8 outlines the outcomes of the differential attack analysis.

Table 8. Differential Attack Results

Image	NPCR (%)	UACI (%)
Beauty	99.63	33.41
Lavender	99.61	33.27
Boat	99.65	33.45
Sunshine	99.62	33.36
Forest	99.64	33.39
City	99.63	33.41

The extracted NPCR is nearly equivalent to 99% and UACI is roughly equal to 33%, which are ideal values for a secure image encryption scheme. This propagation has confirmed through the results that the proposed algorithm spreads a small modification in plaintext image over whole ciphertext. Thus, the proposed hybrid encryption framework is highly resistant to differential attacks and offers very high security for image data protection.

CONCLUSION AND FUTURE WORK

Genuine, Genomic and biomedical the grayscale sequence of this work proposed a new hybrid by region-based secure image encryption crypto — RSA with an Anderson–Darling test for clear vision. The method you proposed enables to superstore images used in encryption, which means that they can effectively remove the spatial correlation and statistical redundancy of plaintext images while keeping the performance high. Image pre-processing and secure key generation using crypto hash functions for highly random control sequence production is the first step in data creation that leads to encryption. These sequences are subsequently used to execute confusion based on permutation and diffusion-based encryption operations. In permutation stages, the positions of the pixels are shuffled based on the pseudo-random permutation sequence, which breaks the spatial constraints of the image, whereas in the diffusion stage, the XOR-based transformation is applied to the pixels, which changes the value. This interaction enables the avalanche effect to be strong, as the changes with respect to the original image and/or the encryption key propagate throughout the entire image. In the context of the above, the control sequences produced using the crypto hash functions can be used to execute the confusion operations, which is the next step in the creation of the images. It further validates the effectiveness of the proposed framework. The proposed framework is also validated based on the statistical performance metrics. The entropy value indicates the level of randomness that is embedded in the encrypted images. The entropy value is close to the theoretical maximum value. In addition to this, the NPCR and UACI value obtained is high enough to resist differential attacks. Most importantly, the sensitivity test validates the effectiveness of the proposed algorithm since these values have the potential to modify the secret key in such a way that even a small alteration could dynamically introduce different encrypted images that could offer greater security for attacks such as brute force, etc. Most importantly, the computational performance analysis of the proposed algorithm indicates that it is possible to obtain sufficient encryption and decryption times to introduce security for the image communication process. The proposed framework for the encryption algorithm is a balanced framework in terms of security level and computational time required for the process. The proposed framework is also efficient enough to resist statistical attacks, differential attacks, and brute force attacks by implementing permutation and diffusion principles for the process. There are many different ways in which the proposed framework could be improved and

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

extended in the future. First and foremost, the proposed encryption scheme could be extended for video encryption purposes. Secondly, the proposed framework could be developed by adopting different key generation methods based on chaotic systems or lightweight crypto principles to improve the security level of the framework. Thirdly, the proposed framework could be developed by implementing a hardware-based approach such as FPGA or GPU to accelerate all the processes where required to improve the performance of the application.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.
[2] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. Wiley, 2015.
[3] A. Jolfaei and A. Mirghadri, "An image encryption approach using chaos and permutation–diffusion architecture," IEEE Access, vol. 7, pp. 11659–11670, 2019.
[4] X. Wang and D. Zhao, "A novel chaotic image encryption scheme based on permutation–diffusion structure," Signal Processing, vol. 152, pp. 91–101, 2018.
[5] C. Li, S. Li, G. Chen, and K.-T. Lo, "Cryptanalysis of a chaotic image encryption algorithm based on permutation–diffusion structure," IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 11, pp. 1867–1872, 2014.
[6] Y. Zhang, "A new image encryption algorithm based on chaotic systems and pixel permutation," Optics and Lasers in Engineering, vol. 52, pp. 24–31, 2014.
[7] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimensional chaotic system," Optics Communications, vol. 284, no. 16–17, pp. 3895–3903, 2011.
[8] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A novel image encryption algorithm based on chaotic system and permutation–diffusion structure," Signal Processing, vol. 149, pp. 1–13, 2018.
[9] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," Information Sciences, vol. 339, pp. 237–253, 2016.
[10] L. Zhang and X. Wang, "Image encryption based on complex chaotic system and permutation–diffusion mechanism," Nonlinear Dynamics, vol. 83, pp. 751–764, 2016.
[11] K. Wong, B. Kwok, and C. Yuen, "An efficient diffusion approach for chaos-based image encryption," Chaos, Solitons & Fractals, vol. 41, no. 5, pp. 2652–2663, 2009.
[12] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," Journal of Selected Areas in Telecommunications, vol. 1, no. 2, pp. 31–38, 2011.
[13] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons & Fractals, vol. 35, no. 2, pp. 408–419, 2008.
[14] X. Wang and H. Zhao, "A novel image encryption scheme based on chaotic sequences," Optics Communications, vol. 285, pp. 562–566, 2012.
[15] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, and Y. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," Optics Express, vol. 20, no. 3, pp. 2363–2378, 2012.
[16] M. Ahmad and M. Alam, "A new algorithm of encryption and decryption of images using chaotic mapping," International Journal of Computer Applications, vol. 60, no. 19, pp. 1–6, 2012.
[17] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.
[18] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using Josephus problem and hyperchaotic system," Nonlinear Dynamics, vol. 84, pp. 1629–1640, 2016.
[19] N. K. Pareek, V. Patidar, and K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, no. 9, pp. 926–934, 2006.
[20] Y. Zhang, "A fast image encryption algorithm based on chaotic maps," Applied Soft Computing, vol. 52, pp. 1183–1192, 2017.
[21] J. Chen, Z. Zhu, C. Fu, L. Zhang, and Y. Yu, "A fast chaos-based image encryption scheme with feedback mechanism," Signal Processing, vol. 129, pp. 179–190, 2016.
[22] X. Di and W. Wang, "A new image encryption algorithm based on chaotic map and DNA coding," Multimedia Tools and Applications, vol. 79, pp. 13479–13497, 2020.
[23] S. Zhou, G. He, and Y. Wang, "Secure image encryption scheme based on permutation–diffusion and chaotic system," IEEE Access, vol. 8, pp. 185256–185269, 2020.
[24] M. Khan and T. Shah, "A literature review on image encryption techniques," Information Security Journal, vol. 29, no. 4, pp. 205–217, 2020.
[25] H. Abed Hilal, "A secure deep learning-based framework for cyber attack detection in network traffic," IEEE Access, 2024

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq

[26] A. A. Ali, M. RASHEED, Effect of changing magnetite percentage on structural and magnetic properties of cobalt ferrite prepared by the sol-gel method, Experimental and Theoretical NANOTECHNOLOGY, 10 (2026) 277–287. https://doi.org/10.56053/10.s.277.
[27] Khaleefah, M. RASHEED, Sol–gel-derived mullite nanoparticles: Structural and antibacterial insights, Experimental and Theoretical NANOTECHNOLOGY, 10 (2026) 289–300. https://doi.org/10.56053/10.s.289.
[28] Z. S. Ahmed, M. RASHEED, H. S. Ahmed, Optimizing NiO nanoparticle properties for antibacterial applications via temperature-driven structural modification, *Experimental and Theoretical NANOTECHNOLOGY*, 10 (2026) 329–342. https://doi.org/10.56053/10.s.329.
[29] Z. S. Ahmed, M. RASHEED, H. S. Ahmed, Enhancing α-Bi_2O_3 nanoparticle crystallinity and antibacterial functionality through controlled calcination, *Experimental and Theoretical NANOTECHNOLOGY*, 10 (2026) 343–356. https://doi.org/10.56053/10.s.343.
[30] A. I. A. Ali, M. RASHEED, Effect of sintering temperature on electrical and structural properties for spinel ferrites prepared by sol-gel method, Experimental and Theoretical NANOTECHNOLOGY, 10 (2026) 239–256. https://doi.org/10.56053/10.s.239.
[31] T. Rashid, M.M. Mokji, M. Rasheed, J. Mech. Behav. Mater. 34 (2025). https://doi.org/10.1515/jmbm-2025-0074
[32] M. Rasheed, M.N. Mohammedali, F.A. Sadiq, M.A. Sarhan, T. Saidani, J. Opt. 54 (2024) 3490-3504. https://doi.org/10.1007/s12596-024-01928-5
[33] S. Shihab, M. Rasheed, O. Alabdali, A.A. Abdulrahman, J. Phys.: Conf. Ser. 1879(2) (2021) 022120. https://doi.org/10.1088/1742-6596/1879/2/022120
[34] A. Zubaidi, L.M. Asaad, I. Alshalal, M. Rasheed, J. Mech. Behav. Mater. 32(1) (2023). https://doi.org/10.1515/jmbm-2022-0302.
[35] M. Ismael, T. Rashid, M.A. Sarhan, M. Rasheed, I.M. Sala, Eureka Phys. Eng. 4 (2023) 29–39. https://doi.org/10.21303/2461-4262.2023.002770
[36] H. K. Aity, E. Dhahri, M. Rasheed, Ceram. Int. (2024). https://doi.org/10.1016/j.ceramint.2024.10.324
[37] M. Mohammed, M. Rasheed, AIP Conf. Proc. 3321 (2025) 020026. https://doi.org/10.1063/5.0289719.

*Corresponding author
Firas A. Hashim,
AI Department, College of Science, Al-Mustansiriyah University
e-mail: Firas70@uomustansiriyah.edu.iq