IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 24, 2021, accepted January 17, 2022, date of publication January 26, 2022, date of current version February 4, 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3146792*

# A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution

**JAMEEL ARIF[1], MUAZZAM A. KHAN[1,2], (Senior Member, IEEE), BARAQ GHALEB[3], (Student Member, IEEE), JAWAD AHMAD[3], (Senior Member, IEEE), ARSLAN MUNIR[4], (Senior Member, IEEE), UMER RASHID[1], AND AHMED Y. AL-DUBAI[3], (Senior Member, IEEE)**

[1]Department of Computer Sciences, Quaid-i-Azam University, Islamabad 45320, Pakistan
[2]Pakistan Academy of Sciences, Islamabad, Pakistan
[3]School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, U.K.
[4]Department of Computer Science, Kansas State University, Manhattan, KS 66506, USA

Corresponding author: Muazzam A. Khan (muazzam.khattak@qau.edu.pk)

**ABSTRACT** Privacy is a serious concern related to sharing videos or images among people over the Internet. As a method to preserve images' privacy, chaos-based image encryption algorithms have been used widely to fulfil such a requirement. However, these algorithms suffer from a low key-space, significant computational overhead, and a lag in resistance against differential attacks. This paper presents a novel chaos-based image encryption method based on permutation and substitution using a single Substitution Box (S-Box) to address issues in contemporary image encryption algorithms. The proposed encryption technique's efficiency is validated through extensive experiments as compared to the state-of-the-art encryption algorithms using different measures and benchmarks. Precisely, the collected results demonstrate that the proposed technique is more resilient against well-known statistical attacks and performs well under plaintext attacks. Indeed, the proposed scheme exhibits very high sensitivity concerning the plaintext attack. A minor change in the encryption key or the plain text would result in a completely different encrypted image.

**INDEX TERMS** Chaotic system, permutation, substitution, logistic map, image encryption.

## I. INTRODUCTION

In recent years, the privacy of users has become one of the major security concern that needs to be addressed carefully, especially when dealing with information shared over the Internet or other openly accessible communication outlets [1]. These privacy concerns are equally valid for digital images as in many cases the digital images carry sensitive information that requires protection from leakages, such as digital images relevant to military, medical, and online personal images [2]. Encryption plays an important role in the process of information security. Hence, several encryption algorithms have been proposed in the literature, mainly the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) [3].

The digital images are characterized by a high correlation among adjacent pixels. The digital images are also less sensitive to changes since a minor change in a pixel value would not translate to a drastic change in image quality as compared to textual data [4]. Consequently, conventional encryption methods such as AES and DES are not suitable for image encryption because they require high processing power and time. To address the aforementioned issue, several image encryption algorithms [5]–[7] have been proposed in recent years. The chaos-based encryption algorithms have been considered optimal practically in this context since they are characterized by fast encryption, low complexity, and high security, with reasonable computational power overhead.

According to Shannon [8], there are mainly two crucial steps of image encryption: confusion and diffusion. Diffusion refers to the relationship between plaintext and cipher images. An encryption method is considered more efficient if a slight change in the original image alters the cipher image completely. Alternatively, confusion refers to the relationship between the key and an encrypted image. Particularly in this context, an encryption method is considered more efficient if altering a bit in the key results in a different encrypted image [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

Many techniques are used in literature to achieve a significant level of confusion and diffusion. Chaotic maps have been recently used widely for image encryption due to their chaotic behavior and simplicity [9], [10]. For instance, Anees *et al.* [6] have proposed an encryption method based on chaotic map, where three S-Boxes are used for the chaotic substitution of image pixels. The results have demonstrated that chaotic map-based encryption has superior performance than encryption techniques utilizing one S-Box and has significantly faster processing time in comparison to the traditional algorithms. However, the method proposed by Anees *et al.* [6] does not perform efficiently in terms of diffusion.

Ahmad and Hwang [5] have proposed a novel chaos-based diffusion and a substitution encryption method in which auto-correlation in digital data is minimized for lower gray values. On the contrary, diffusion is achieved by dividing the substituted image into blocks of $Z \times Z$ elements where the random values of blocks are generated by exploiting the logistic map [5]. The resulting cipher is then further XORed with substituted image blocks resulting in a cipher image with reduced correlation [5]. Ahmad and Hwang method [5] has a lower impact on pixel values of the encrypted image when the corresponding plaintext image is taken with a changed pixel value and also has comparatively high correlation coefficient between the pixels of encrypted image.

He *et al.* [11] have proposed a cryptosystem by substituting sine map in sine iterative chaotic map with infinite collapse modulation map system utilizing a delayed sine map. Zeng and Wang [12] have utilized particle swarm optimization and cellular automata to design a hyper-chaotic image encryption method where cellular automata are used to diffuse each pixel value. In general, substitution-based algorithms employing a single S-Box have shown promising performance concerning image encryption. However, they do suffer from the problem of high correlation between the pixels of the encrypted image. Shafique and Ahmed [13] have proposed an image encryption algorithm based on the dynamic allocation of S-Box by using the chaotic map to reduce the correlation between the encrypted image pixels. Ahmad and Hwang [5] have used multiple S-Boxes for image encryption by chaotic allocation of S-Boxes to minimize the correlation between the encrypted image pixels but the results show that their techniques fail to achieve very low correlation coefficient between the pixels of encrypted image so better encryption algorithm can be designed to fill in this gap [5], [14].

The researchers have widely used permutations to encrypt the images. Indrakanti and Avadhani [15] have proposed a random permutation-based image encryption that uses a 64-bit symmetric key [15]. Anwar and Meghana [16] have presented a method of image encryption based on chaotic pixel permutation by using a variation of Arnold's cat map. These methods are not sensitive to the change in the plain-text images and the encrypted image provides sufficient information about the original image.

Masood *et al.* [17] have proposed a multi-stage image encryption scheme based on Henon chaotic map (Henon–Pomeau attractor map), Brownian motion, and Chen's chaotic system. In their approach, an image is divided into blocks and then the pixels of each block are shuffled [17]. Khan and Ahmad [7] have presented an encryption method based on skew tent map and tangent delay ellipse reflecting cavity map system (TD-ERCS map). The use of multiple chaotic maps in Khan and Ahmad method [7] causes it to take more computational time in encryption.

Agrawal has discussed an image encryption method based on a 2D sine tent composite map and superior fractal function in [18]. Chaotic sequences are generated by using the output of the superior fractal function as an initial value. Chaotic circular pixel shuffling is applied with the help of sequences generated by a 2D sine tent composite map, and then XOR operation is performed to generate cipher image. Their method hides the image features comparatively well, but it takes 7 seconds to encrypt a $512 \times 512$ image.

An improved version of the chaotic map with improved Markov properties [19] is used to introduce a new image encryption method by Ge and Ye [20]. An initial key is generated by adding all the image bits to make the cryptosystem secure against differential attacks. Reverse cat map is then applied to achieve confusion in the encrypted image. They have used a chaotic map for diffusion. The method has been further evaluated using different statistical and differential tests on the encrypted image, the results of which demonstrate that the method is comparatively less resistant against statistical attacks.

The previous studies have several limitations regarding resistance against differential attacks, computational overhead, and low key-space. This research tries to fill in the gap by introducing a novel chaotic permutation–substitution image encryption scheme based on logistic map and the AES S-Box. The results illustrate that the proposed encryption algorithm can produce a profoundly secured encrypted image with highly scrambled pixels, and as compared to the other cryptosystems, the proposed scheme is comparatively more efficient and resistant against attacks. Encrypted images using the proposed scheme are sensitive to a slight change in the pixel values of the plain text images or a slight change in the encryption key, which makes the proposed scheme more resistant against differential attacks.

The proposed scheme is evaluated and compared with several encryption techniques given in the literature. The evaluation is performed in terms of histogram analysis; the horizontal, vertical, and diagonal correlation coefficient between the plain-text image and the encrypted image; peak signal to noise ratio (PSNR); mean square error (MSE); the number of pixels changes rate (NPCR); unified average change intensity (UACI); maximum deviation; irregular deviation; deviation from the uniform histogram; entropy; and time complexity. Compared with the existing image encryption methods, this study has the following novel contributions:

- An efficient arrangement of substitution-permutation process is presented to design a lightweight image

encryption method and achieve a significant level of security.
- Key is generated from the plaintext image using SHA-2 to resist the chosen plaintext attacks. Tiny modification in the original image impacts the entire encryption process with the proposed image encryption algorithm approach.
- Instead of using multiple S-boxes, the proposed encryption scheme achieves a higher level of confusion by using a single AES S-box.
- The proposed encryption scheme achieves a significant level of resistance to differential and statistical attacks.
- The proposed scheme is compared with the state-of-the-art image encryption schemes. Results indicate the proposed encryption scheme outperforms other image encryption methods given in the literature and provides higher resistance against attacks, while requiring less computational power.

The rest of the paper is organized as follows. In Section II, a brief background of encryption and its main techniques is presented. The steps of our image encryption scheme are elaborated and discussed in Section III. We analyze the security of our proposed scheme in case of statistical attacks, and key and plaintext sensitivity in Section IV. Finally, we conclude the paper in Section V.

## II. BACKGROUND

In general, encryption algorithms are categorized into complete and selective. The former performs full encryption, while the latter performs encryption only on the part of data [21]. The complete encryption is more secure; however, it requires a higher processing power than the selective encryption. Hence, a complete encryption algorithm with faster compression time is considered more suitable for image encryption as it aims at hiding the maximum amount of information to deliver a sufficient level of security.

In addition to the substitution, hashing and permutation methods are well known in data encryption. The substitution process (a factorial boolean function) by employing a substitution box (S-Box) takes an $n$ bit input. The substitution process returns a substituted $m$ bit output with the main aim is to obscure the relationship between the key and the ciphertext (i.e., confusion). On the other hand, permutation is a technique that is used to replace the position of pixels of image in such a way that it can be recovered to the original state when needed. It plays an important role in image encryption [22]. Hashing is a process of converting any size of data into a fixed-size string known as the hash. Secure Hash Algorithm (SHA) is a standard cryptography hash function designed by the United State National Security Agency [23]. SHA is very sensitive to input such that a change in a single input bit would completely change the hash value. The different versions of SHA are SHA-1, SHA-2 and SHA-3 [24]. SHA-3 is the latest member of SHA family and is comparatively more secure but slower than the SHA-1 and SHA-2.

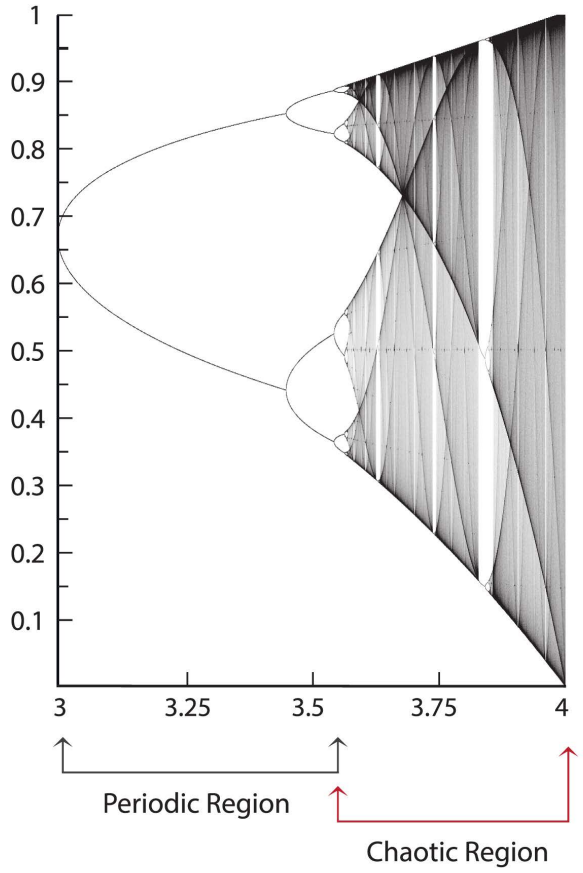



**FIGURE 1.** Bifurcation diagram of logistic map.

Many algorithms are discussed in the literature to create S-Boxes, with the main focus on ensuring the non-linearity of the created S-Box. If an S-Box is linear, we will always substitute the same m-bit output for the same n-bit input, suggesting a high correlation between the cipher and the plaintext data, a characteristic that makes breaking the encryption scheme easier. AES S-Box is comparatively better than other S-Boxes in cryptographic systems in terms of global avalanche criterion, non-linearity, and better resistance against external attacks [25], [26]. The AES S-Box provides most of the features and efficient functionalities that are required in cryptography [27].

The non-linearity of S-Boxes, chaotic maps, logistic maps, etc., have been proven efficient. The pseudo-random numbers generation ensures the chaotic behavior of non-linear S-Boxes. The mathematical equation for the logistic map is given below.

$$X_{i+1} = \mu X_i(1 - X_i)$$
$$\text{where } 0 \leq X_i \leq 1 \ \& \ 0 \leq \mu \leq 4 \quad (1)$$

where $\mu$ is the control parameter or growth rate, and $X_0$ is the starting population. According to a study, the random numbers generated by logistic maps are affected by the parameter $\mu$. The generated sequence repeats itself after a few cycles when the value of $\mu$ is between 0 and 3 [28]. The periodic sequence is found to be the generated numbers when

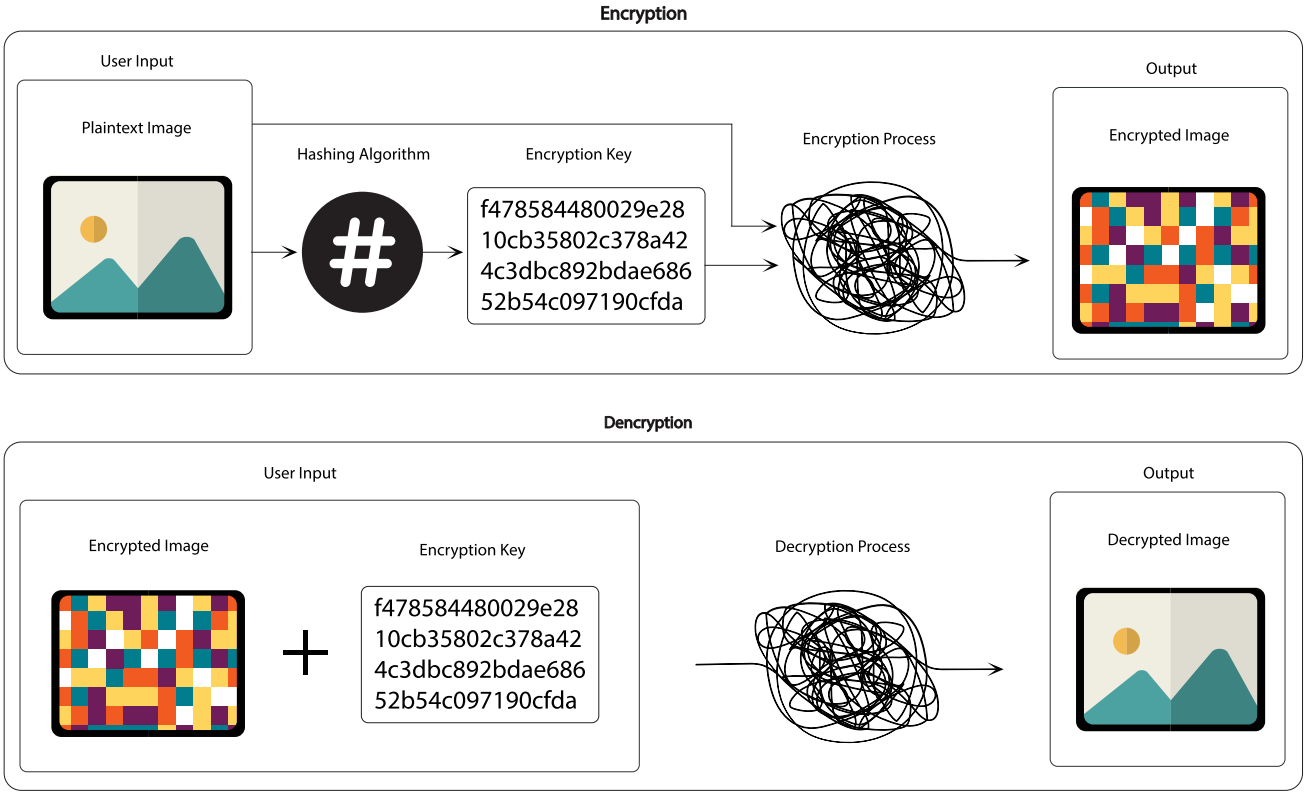



**FIGURE 2.** Overview of the proposed scheme: image encryption and decryption process.

the value of $\mu$ is between 3 to 3.569946 [28]. At 3.569946, Mosekilde *et al.* found the period of infinity, and the system behaves chaotically when the value of $\mu$ is between 3.569946 and 4 [28]. Bifurcation diagram of logistic map is shown in Figure 1. Uneven distribution, low security, and a small parameter space are all downsides of the logistic map, however, in the proposed work, we have utilised logistic map at one stage.

## III. PROPOSED SCHEME

This section provides an overview of the proposed scheme as well as its design and implementation.

### A. PROPOSED SCHEME OVERVIEW

Figure 2 provides an overview of the encryption and decryption process of the proposed scheme. The proposed scheme is designed to fill in the gaps in the previous methods of image encryption in the literature. To achieve the optimal level of security and efficiency, the proposed scheme is based on chaotic permutation, substitution, and XOR operation. The proposed scheme has a large keyspace and is very resistive against brute-force attack. The relation between the plaintext image and cipher image is obscured by using a key based on the plaintext image. AES S-Box is used to achieve the minimal level of correlation between the cipher image pixels. The proposed scheme is intended to provide an efficient method of image encryption that is more secure against attacks and consumes fewer resources.

Our proposed scheme performs encryption in two main stages. The first stage creates encryption keys by applying the SHA-2 256 hashing algorithm on the plaintext image. We have selected SHA-2 256, since SHA-1 was cracked in 2017 by Google [29]. We want to clarify that SHA-3 is more secure than SHA-2 256 but we have not selected SHA-3 due to its resource hungriness. The resulting hash is then divided into multiple parts, mapped between 0 and 1, suitable for logistic maps.

In the second stage, column and row permutation is performed on the image pixels employing pseudorandom numbers generated by a chaotic logistic map. The hash values produced in the first stage are used as the initial population for the logistic map. The value of $\mu$ (control parameter of the logistic map) is taken as 3.99123 to generate pseudorandom numbers since the logistic map system behaves chaotically for $\mu$ value between 3.569946 and 4 [28]. After permutation, the XOR operation is performed on the permuted image pixels and pseudorandom numbers generated by the logistic map. Then a substitution operation is applied to the resulting image.

This research employs AES and reverse S-Boxes to substitute a pixel value by considering logistic maps. The utilization of multiple less secure S-Boxes for image encryption effect the encryption quality. The state-of-the-art encryption methods suggests the employment of multiple secure S-Boxes [6].

### B. PROPOSED SCHEME DESIGN AND IMPLEMENTATION

Fig. 3 shows the flow chart of the proposed scheme. Steps of the proposed scheme to encrypt an image are presented below.

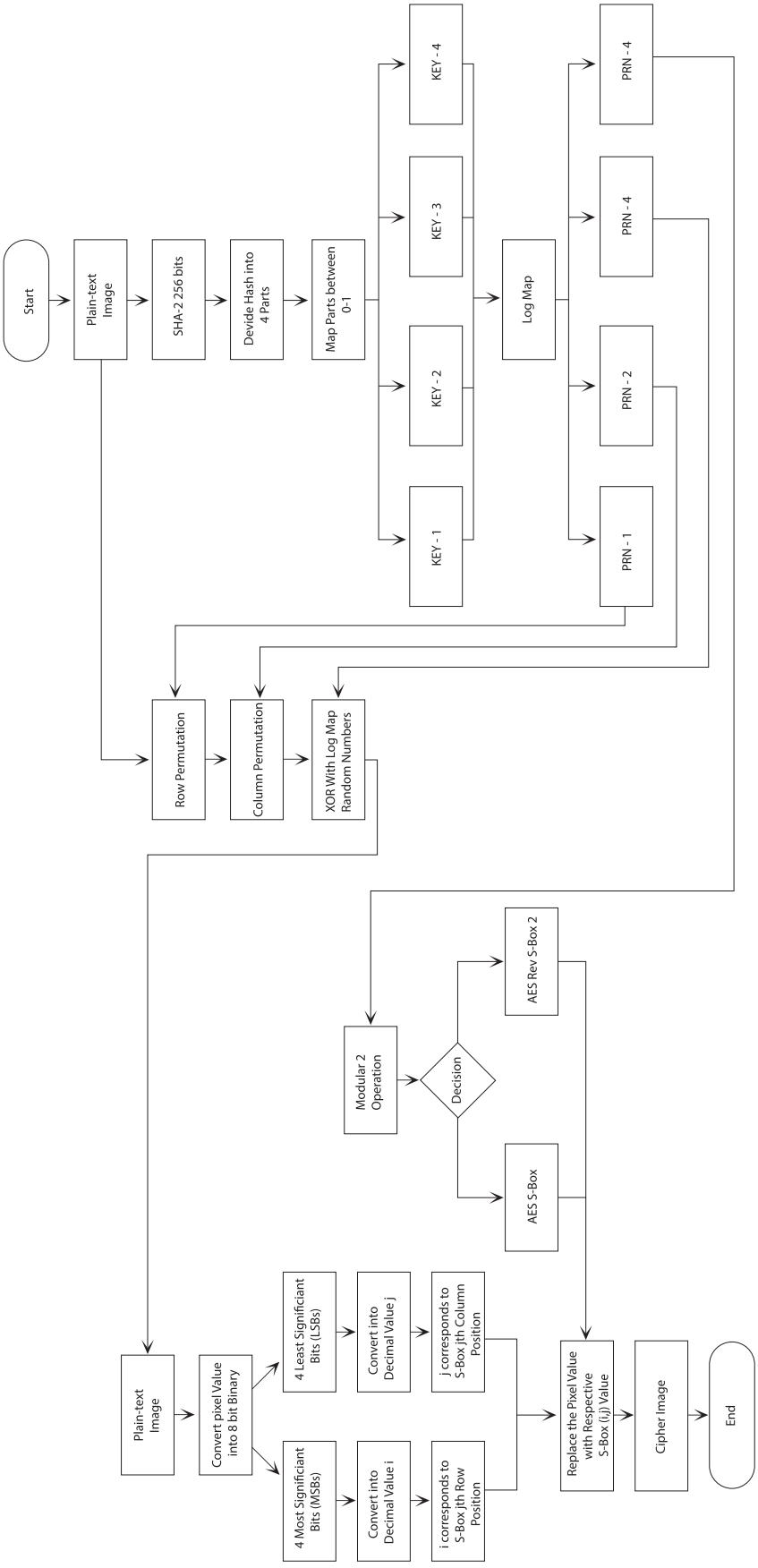



**FIGURE 3.** Flow diagram of the proposed scheme.

1) Apply SHA-2 256 on a plaintext image to generate a hash for the plaintext image.
2) Divide hash into 4 equal parts of 64 bits.
3) Mapping the hash parts from step-2 between 0-1 (by converting the hexadecimal hash part into integer and then taking modulus 0.9999) and save in Keys Key-1, Key-2, Key-3, and Key-4.
4) Use the Keys generated in step-3 as initial population parameter $\mu$ for the logistic map to produce pseudo-random numbers PRN-1, PRN-2, PRN-3, and PRN-4.
5) Perform chaotic row permutation on the image by using PRN-1.
6) Perform chaotic column permutation using PRN-2 on the resultant image generated by step-5.
7) XOR PRN-3 by the resultant image generated by step-6.
8) Convert the pixel values of the image generated in step-7 from decimal to binary.
9) Divide each 8-bit pixel value into 2 equal parts of 4 bits. Part-1 is the most significant 4 bits and part-2 contains the least significant 4 bits of the pixel.
10) Convert the parts of pixels from binary to decimal. Part-1 into Dpart-1 and Part-2 into Dpart-2.
11) Selection of AES S-Box or AES reverse S-Box (as discussed in section III-A), based on the value of PRN-4 for each pixel.
12) Use Dpart-1 from step-10 to corresponds to the row number Dpart-1 of the selected S-Box in step-11 and use Dpart-2 to corresponds to the row number Dpart-2 of the selected S-Box in step-11.
13) Generate the encrypted image by replacing the Pixel value with receptive S-Box value at position (Dpart-1, Dpart-2).

The decryption process of the proposed scheme is discussed in the steps below.

1) Read the encrypted image along with the encryption key.
2) Use the keys as initial population parameter $\mu$ for the logistic map to produce pseudo-random numbers PRN-1, PRN-2, PRN-3, and PRN-4.
3) Perform steps 8 to 12 of the encryption process and then substitute the encrypted image pixel values.
4) XOR PRN-3 by the resultant image generated by step-3.
5) Perform chaotic column permutation in reverse order using PRN-2 on the resultant image generated by step-4.
6) Perform chaotic row permutation in reverse order on the image from step-5 using PRN-1 to complete the decryption process.

## IV. RESULTS AND SECURITY ANALYSIS

We have used several images of 512 × 512 pixels, namely, the Cameramen.png, Baboon.png, Lena.png, Pepper.png, and Zelda.png to evaluate the proposed scheme. The selected images are widely used in literature to analyze image encryption methods (Fig. 4). A visual comparison of an encrypted Baboon 512 × 512 image by using the proposed scheme with Anees *et al.* [6] method is shown in Fig. 6. The encryption scheme proposed in this research is compared with state-of-the-art algorithms for resistance to differential attacks, encryption quality, entropy, PSNR, MSE, NPCR, UACI, and time complexity.

### A. CORRELATION COEFFICIENTS BETWEEN CONSECUTIVE PIXELS

The correlation coefficient is used to measure the association between two variables. In images, the pixels are highly correlated, and thus, image encryption algorithms mainly focus on reducing the association between the pixels of an encrypted image. The correlation coefficient is scaled between $+1$ and $-1$, where $+1$ indicates a maximum positive correlation, and $-1$ indicates a maximum negative correlation between two variables. Hence, if the correlation coefficient is equal to 0, it shows no association between the variables. However, a simple correlation coefficient only shows the overall association and generally might not be sufficient for highlighting local dependencies [4]. For assessing local association, Dikbaş [30] has introduced the horizontal correlation coefficient, and the vertical correlation coefficient as more efficient methods. Consequently, this paper opts to analyze the proposed scheme by calculating a horizontal correlation coefficient, vertical correlation coefficient, and diagonal correlation coefficient ($CC$) between consecutive pixels of the encrypted image. The method having a correlation coefficient value close to 0 is considered more secure. The mathematical representation of correlation coefficient is shown in Eq. 2.

$$\begin{aligned} S &= W \times H \\ M(p) &= \frac{1}{S}\sum_{i=1}^{S} p_i \\ D(p) &= \frac{1}{S}\sum_{i=1}^{S} (p_i - M(p)) \\ \mathrm{cov}(p_1, p_2) &= \frac{1}{S}\sum_{i=1}^{S} \left(p_{1_i} - M(p_1)\right)\left(p_{2_i} - M(p_2)\right) \\ CC_{p_1,p_2} &= \frac{\mathrm{cov}(p_1, p_2)}{\sqrt{D(p_1)D(p_2)}} \end{aligned} \tag{2}$$

where $W$ is the width of the image, $H$ is the height of the image, $S$ is the total number of pixels in the image, $p_{1_i}$ is the $i^{\text{th}}$ instance (pixel) of the plaintext image, and $p_{2_i}$ is the $i^{\text{th}}$ instance (pixel) of the encrypted image. $M(p)$ is the mean of the pixels values, $M(p_1)$ is the mean of the pixels values of plaintext image and $M(p_2)$ is the mean of the pixels values of encrypted image. $D(p)$ is the variance of image, and $D(p_1)$ and $D(p_2)$ are the variance of the plaintext image and the cipher image, respectively; $p_1$ and $p_2$ are the neighboring pixels of the image and $cov(p_1, p_2)$ is the co-variance of adjacent pixels. The horizontal correlation coefficient is the correlation between the horizontal pixels of the image as illustrated in


**FIGURE 4.** Plaintext images. a. Cameraman, b. Baboon, c. Lena, d. Pepper and e. Zelda.

Fig. 5 (c), and similarly the vertical correlation coefficient is the correlation between the vertical pixels of the image as illustrated in 5 (b), while diagonal correlation coefficient is the correlation between the diagonal pixels of the image, as shown in Fig. 5 (a). The evaluation results of the proposed encryption method and Anees *et al.*'s algorithm [6] in terms of the vertical correlation coefficient, horizontal correlation coefficient, and the diagonal correlation coefficient are shown in Table 1, 2, and 3, respectively, under several images. We have also compared our proposed scheme to several other algorithms; however, under only the 512 × 512 encrypted Peppers image as shown in Table 4. Results show that the proposed scheme has a lesser vertical correlation coefficient, horizontal correlation coefficient, and diagonal correlation coefficient than the other.

**TABLE 1.** Vertical correlation coefficient of proposed scheme and Anees *et al.* [6] method.

| | proposed scheme | Anees et al. [6] |
|---|---|---|
| Baboon | -0.00356 | 0.00585 |
| Cameraman | -0.00337 | 0.10554 |
| Lena | -0.00335 | 0.17218 |
| Peppers | 0.00061 | 0.03447 |
| Zelda | -0.00075 | 0.03785 |

**TABLE 2.** Horizontal correlation coefficient for proposed scheme and Anees *et al.* [6] method.

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | -0.00193 | 0.00547 |
| Cameraman | -0.01041 | 0.13523 |
| Lena | -0.00275 | 0.15164 |
| Peppers | 0.00081 | 0.03406 |
| Zelda | -0.00415 | 0.03031 |

### *B. CORRELATION COEFFICIENTS BETWEEN PLAINTEXT IMAGE AND CIPHER IMAGE*

A critical measure to demonstrate the efficiency of the encryption algorithms is the correlation coefficient between the plaintext and encrypted images, as it shows the level of association between the plaintext and encrypted images. As a simple correlation is unable to provide as much information about the ability of encryption methods to resist attacks, we have carried out our analysis, which is vertical, horizontal, and diagonal correlations comparison of our proposed scheme with other schemes discussed in literature [6], [11].

We carry out the following steps to calculate the vertical correlation coefficient between the plain and cipher images. The column-wise variance is calculated for plaintext and cipher images in a couple of steps. The mean of each column is calculated. After that, the standard deviation of the pixels

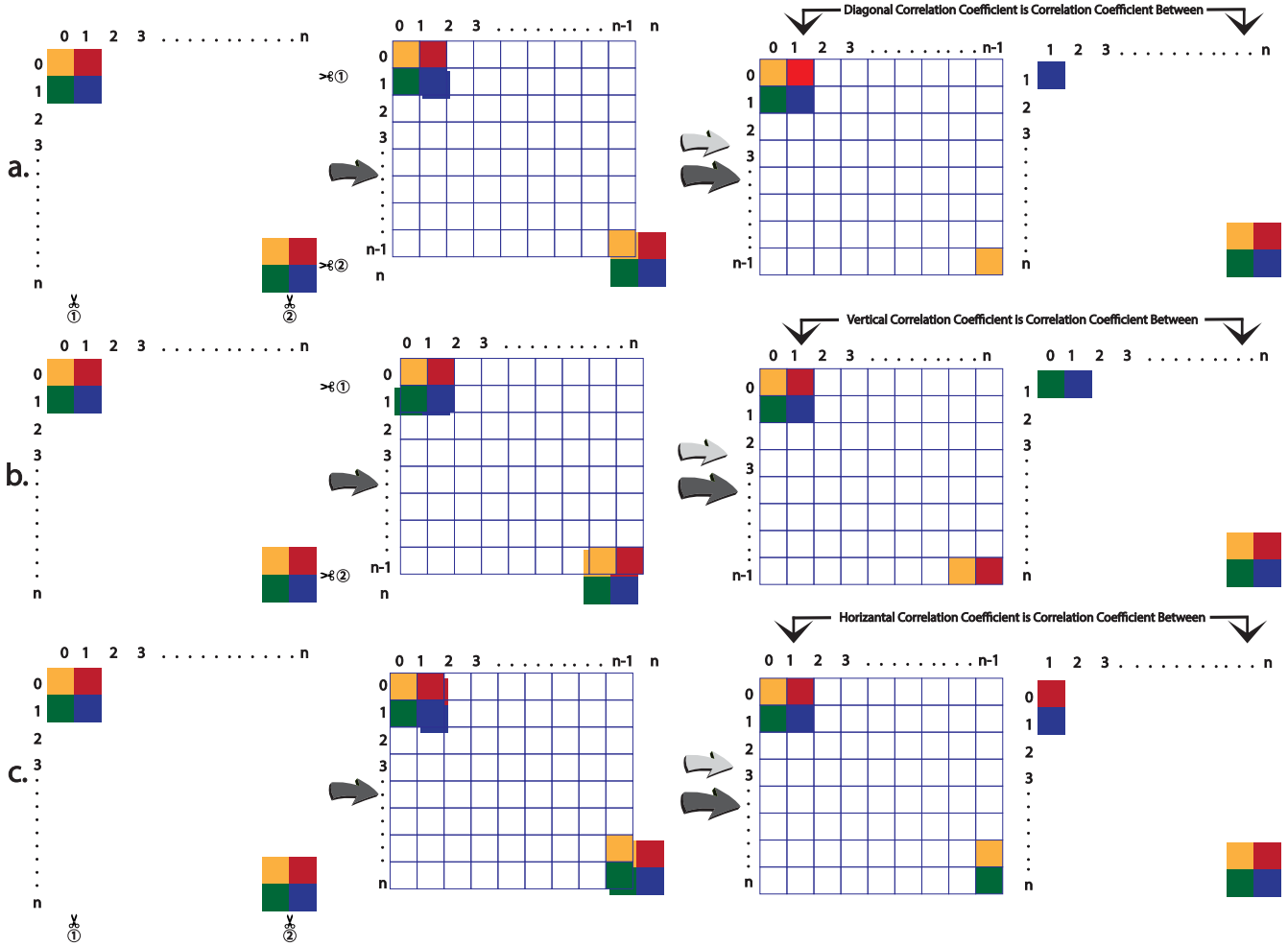



**FIGURE 5.** a. Diagonal correlation coefficient b. Vertical correlation coefficient c. Horizontal correlation coefficient.

from the mean is computed for every pixel in the column. All the standard deviations are squared and summed. Finally, the sum is divided by the total number of pixels in the image. The variance is mathematically representated in Eq. 3.

$$V_v(P) = \frac{\sum_{i=0}^{W}\{\sum_{j=0}^{H}(P_j - \bar{P}_i)^2\}}{W \times H} \tag{3}$$

where $P$ is the image, $W$ is the width of the image and $H$ is the height of the image, $\bar{P}_i$ is the mean of the column number $i$ and $P_j$ represents a pixel at a position $j$ in column $\bar{P}_i$. The mean of each column is calculated along with the standard deviation of the pixels from the mean for every pixel in that column. The resulting deviations are then squared, added up, and the final sum is divided by the total number of pixels in the image.

The vertical co-variance of the plaintext image and its cipher is then calculated as shown in Eq. 4.

$$C_v(P, C) = \frac{\sum_{i=0}^{W}\{\sum_{j=0}^{H}(P_j - \bar{P}_i) \times (C_j - \bar{C}_i)\}}{W \times H} \tag{4}$$

**TABLE 3.** Diagonal correlation coefficient for proposed scheme and Anees *et al.* [6] method.

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | -0.00329 | 0.00531 |
| Cameraman | -0.00011 | 0.12206 |
| Lena | 0.00025 | 0.14592 |
| Peppers | 0.00332 | 0.03615 |
| Zelda | -0.00123 | 0.03339 |

**TABLE 4.** Correlation coefficients of the encrypted Peppers image with different methods.

| Test | Plaintext image | [11] | [6] | Proposed |
|---|---|---|---|---|
| Vertical | 0.9709 | 0.00094 | 0.03447 | 0.00061 |
| Horizontal | 0.9639 | 0.00213 | 0.03406 | 0.00081 |
| Diagonal | 0.9414 | -0.00246 | 0.03615 | 0.00332 |

where $P$ is the plaintext image, $C$ is the cipher image, $W$ is the width of the images, and $H$ is the height of images, $\bar{P}_i$ is mean of the column number $i$ of plaintext image, and $P_j$ represent a pixel at a position $j$ in the column $\bar{P}_i$ of plaintext image. $\bar{C}_i$ is a column number $i$ of cipher image, and $C_j$ represents a

pixel at a position $j$ in column $\bar{C}_i$ of cipher image. Finally, the vertical correlation coefficient is obtained by the division of the co-variance of the plaintext image and its cipher image by the square root of the product of the variance of the plaintext image and its cipher as demonstrated in Eq. 5.

$$CC = \frac{V_{cov}}{\sqrt{V(P) \times V(C)}} \tag{5}$$

where $V_{cov}$ is co-variance of the plaintext image and the corresponding encrypted image, and $V(P)$ and $V(C)$ are the variances of plaintext image and encrypted image, respectively. We have also carried out the exact steps mentioned previously to calculate the correlation between the rows of the plaintext image and its cipher image (i.e., horizontal correlation coefficient) and the diagonal correlation coefficient. The correlation coefficient value close to zero shows little correlation between the plaintext and encrypted images, and the encryption algorithm has a better resistance against attacks.

As mentioned earlier, tests are performed on Baboon, Cameraman, Lena, Peppers, and Zelda test images to compare our method with Anees *et al.* [6] method. Hence, Table 5, Table 6, and Table 7 present the results of the vertical correlation, the horizontal correlation and the diagonal correlation coefficients between the plaintext and cipher images, respectively. The proposed scheme has a smaller vertical correlation coefficient, horizontal correlation coefficient, and diagonal correlation coefficient and is more resistant to attacks as compared to Anees *et al.* [6] method.

**TABLE 5. Vertical correlation coefficient for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 0.00190 | 0.02967 |
| Cameraman | 0.00830 | -0.05623 |
| Lena | 0.00193 | 0.03311 |
| Peppers | -0.00341 | -0.03876 |
| Zelda | -0.00143 | -0.03436 |

**TABLE 6. Horizontal correlation coefficient for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 0.00275 | 0.03216 |
| Cameraman | 0.00578 | -0.13308 |
| Lena | 0.00182 | 0.05508 |
| Peppers | -0.00395 | -0.03735 |
| Zelda | -0.00098 | -0.02464 |

**TABLE 7. Diagonal correlation coefficient for proposed scheme and Anees *et al.* [6] method.**

| | proposed scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 0.00142 | 0.03334 |
| Cameraman | 0.00709 | -0.11107 |
| Lena | 0.00230 | 0.04605 |
| Peppers | -0.00392 | -0.04031 |
| Zelda | 0.00075 | -0.03320 |

### C. VISUAL ANALYSIS

The sample Baboon, Cameraman, Lena, Peppers and Zelda images, using the proposed scheme and their comparison with Anees *et al.* [6] method, for visual examination are shown in Figure. 6, 7, 8, 9, and 10.

As it emerges from the experimental results that encrypted images using the proposed scheme hide more information and are more secure against visual attacks as compared to prior methods in literature.

### D. HISTOGRAM ANALYSIS

Histogram analysis is a widely used statistical measure which is used to calculate the distribution of grayscale pixels in an image. An image is considered to be more secure against statistical attacks if it has a uniform histogram. The histogram of a cipher image can capture information about the original image if it is not uniform enough [4], [31].

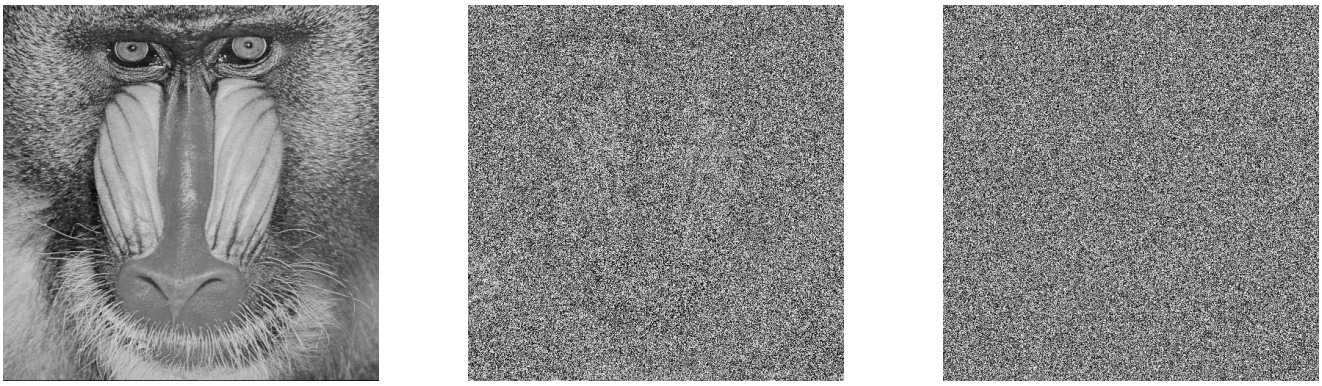
The results of histogram analysis of our proposed scheme in comparison with Anees *et al.* [6] encryption technique for the Baboon, Cameraman, Lena, Pepper, and Zelda images are presented in Fig. 11, Fig. 12, Fig. 13, Fig. 14, and Fig. 15, respectively. The histogram for the proposed scheme is more uniform than the histogram of the encrypted image using the Anees *et al.* [6] method, which shows that encrypted images using the proposed scheme hides more information and provides more resistance against attacks.

### E. ENTROPY

Information entropy is another statistical measure of uncertainty in communication theory [32] and can be used to capture the randomness and unpredictable behavior of a system [33]. In this context, an encrypted image with higher entropy conceals more information as compared to an encrypted image with lower entropy, and vice versa. The mathematical representation for entropy is presented in Eq. 6.

$$H(X) = -\sum_{i=0}^{255} P(X_i) log(P(X_i)) \tag{6}$$

where $X$ is a random variable and $P(X_i)$ is the probability of occurrence of instance $X_i$. If we generate 256 instances with the same probability and every instance is 8 bits, then $H(X) = 8$. Generally, the entropy is always less than the ideal value because the real data does not have the ideal random distribution. In a system, the less the entropy value is, the more the system is crackable. Thus, it is desirable to have the entropy closer to the ideal entropy for a secure system [34], [35]. The entropy analysis results of the proposed technique compared to the encryption schemes in the literature are shown in Table 8. The entropy of the image encrypted by the proposed scheme is very close to the ideal entropy, that is, 8 or higher than other methods, which shows the proposed scheme's better resistance than other methods.



(a) (b) (c)

**FIGURE 6.** a. Plaintext Baboon image b. Encrypted Baboon image using Anees *et al.* [6] encryption technique c. Encrypted Baboon image using the proposed encryption scheme.

(a) (b) (c)

**FIGURE 7.** a. Plaintext Cameraman image b. Encrypted Cameraman image using Anees *et al.* [6] encryption technique c. Encrypted Cameraman image using the proposed encryption scheme.

(a) (b) (c)

**FIGURE 8.** a. Plaintext Lena image b. Encrypted Lena image using Anees *et al.* [6] encryption technique c. Encrypted Lena image using the proposed encryption scheme.

### *F. ENCRYPTION QUALITY*

The encryption quality is an essential tool to check the effectiveness and efficiency of the cryptosystems. The resulting image is measured for deviation and correlation with several methods in the literature. The traditional subjective method of visual inspection, where a human assesses the quality of the image, used to be the norm in this context. However, it has been found recently that such a method cannot reveal the hidden flaws in encryption quality. Hence, several other methods were proposed in literature introducing the idea

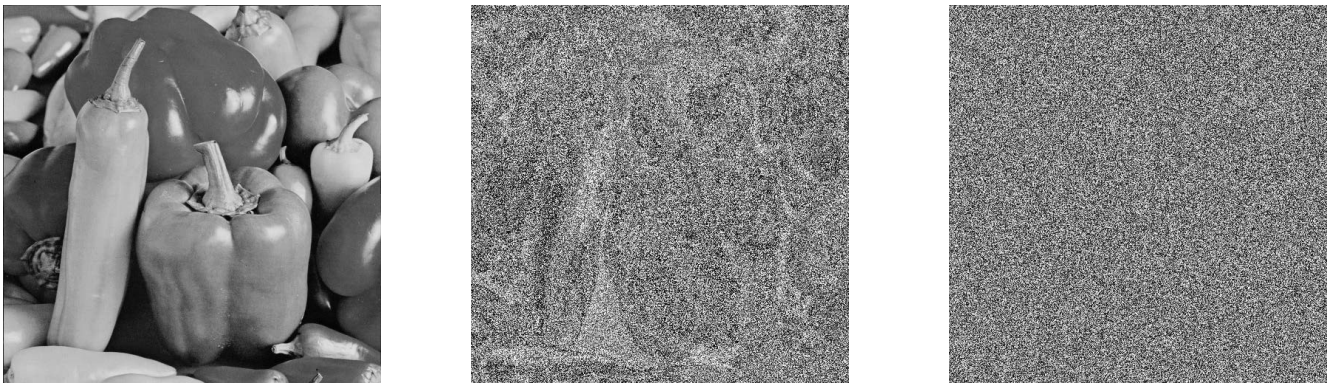



**FIGURE 9.** a. Plain text Peppers image b. Encrypted Peppers image using Anees *et al.* [6] encryption technique c. Encrypted Peppers image using the proposed encryption scheme.

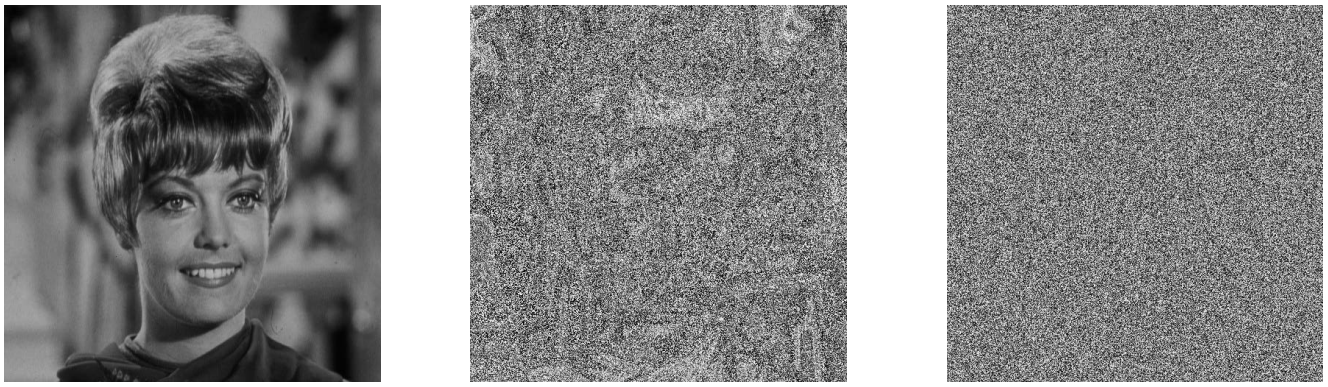



**FIGURE 10.** a. Plaintext Zelda image b. Encrypted Zelda image using Amir *et al.* encryption technique c. Encrypted Zelda image using the proposed encryption scheme.

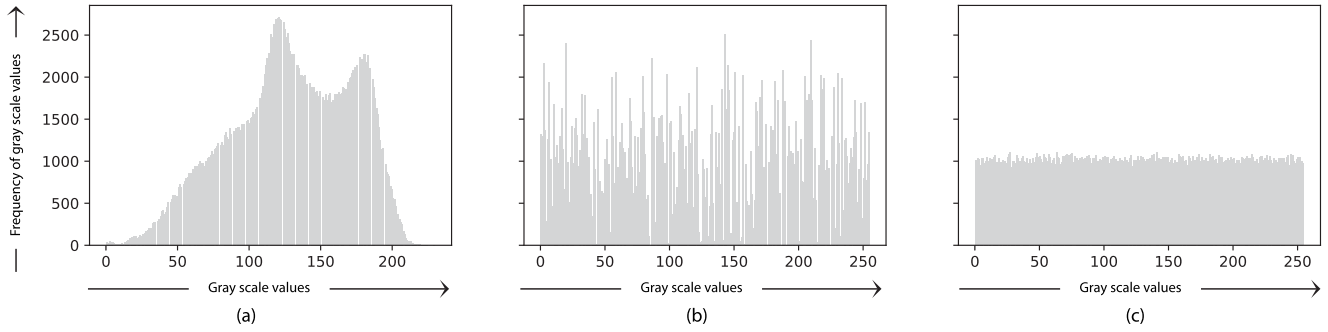



**FIGURE 11.** Histogram analysis for Baboon image. Y-axis is representing the levels of grayscales in the image. The X-axis is representing the frequency of grayscale values. a. is showing the histogram for the plaintext image, b. is showing the histogram for an encrypted image using Anees *et al.* [6] method, and c. is showing the histogram for an encrypted image by using the proposed scheme.

of quantitative measures of the encryption quality based on maximum deviation and correlation [4], [36].

The standard deviation of pixel values of the plaintext image computed via the pixel values of the corresponding cipher image is an excellent measure to measure encryption quality. Indeed, three different deviation measures are used in this research to examine the quality of the proposed scheme, namely, maximum deviation, irregular deviation, and deviation from the uniform histogram.

### 1) MAXIMUM DEVIATION

Maximum deviation is the sum of the difference between the histograms of the plaintext image and the cipher image. The mathematical representation of maximum deviation is represented in Eq. 7.

$$D_{max} = \frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i \tag{7}$$

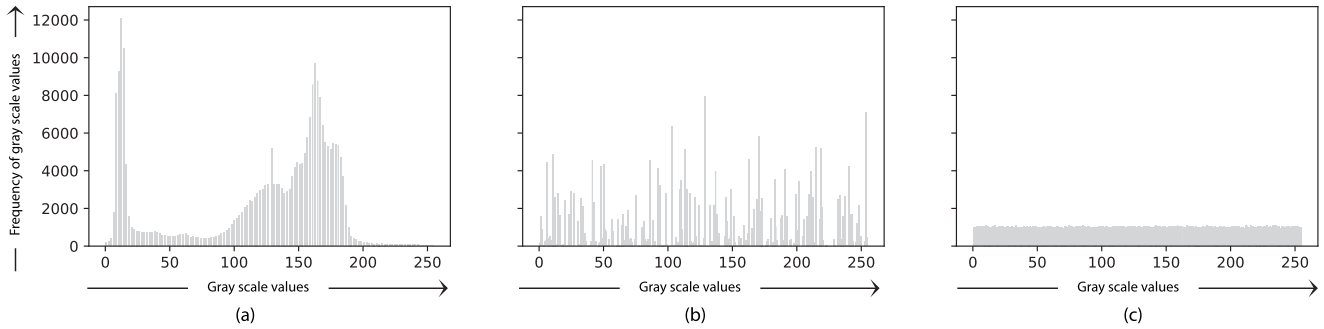



**FIGURE 12.** Histogram analysis for Cameraman image. Y-axis is representing the levels of grayscales in the image. The X-axis is representing the frequency of grayscale values. a. is showing the histogram for the plaintext image, b. is showing the histogram for an encrypted image using Anees *et al.* [6] method, and c. is showing the histogram for an encrypted image by using the proposed scheme.

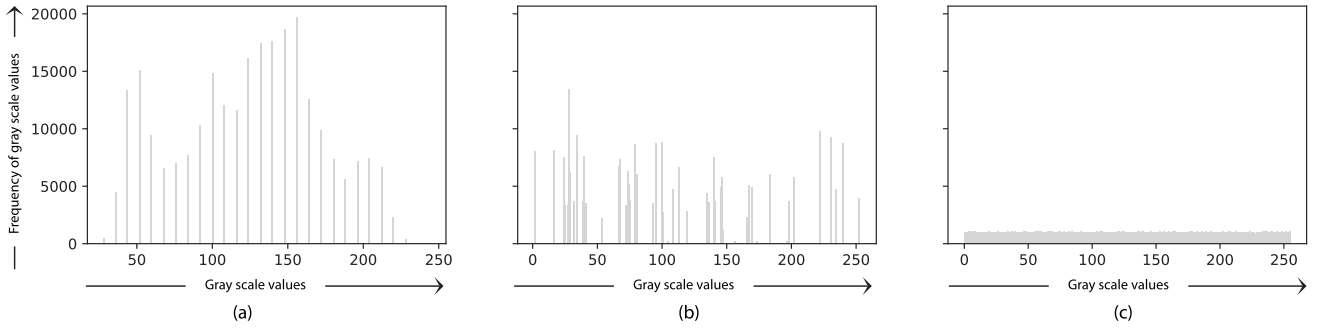



**FIGURE 13.** Histogram analysis for Lena image. Y-axis is representing the levels of grayscales in the image. The X-axis is representing the frequency of grayscale values. a. is showing the histogram for the plaintext image, b. is showing the histogram for an encrypted image using Anees *et al.* [6] method, and c. is showing the histogram for the encrypted image by using the proposed scheme.

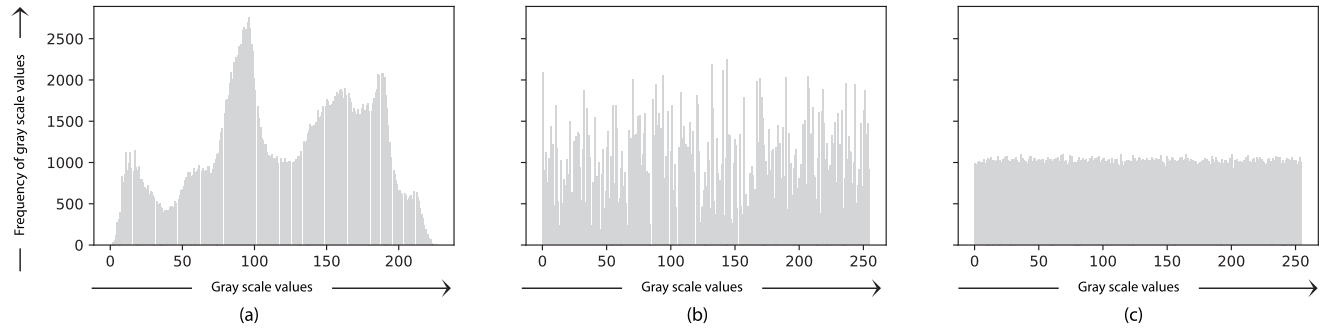



**FIGURE 14.** Histogram analysis for Pepper image. Y-axis is representing the levels of grayscales in image. The X-axis is representing the frequency of grayscale values. a. is showing the histogram for the plaintext image, b. is showing the histogram for an encrypted image using Anees *et al.* [6] method and c. is showing the histogram for an encrypted image by using the proposed scheme.

where $d_i$ is the instant of the $d$ at index $i$. $d$ is the difference between the histogram of plaintext image and the cipher image. $d_0$ is the difference at index 0 of $d$ and $d_{255}$ is the difference at index 255 of $d$. A higher value of maximum deviation shows that the encrypted image is more deviated from the plaintext image and the encryption method is more secure. The evaluation results of the proposed scheme's maximum deviation compared to that of Anees *et al.* [6] encryption technique for the Baboon, Cameraman, Lena, Pepper and Zelda images are presented in Table 9. The maximum deviation of encrypted image using the proposed scheme is largely deviated from the original image; however, the performance of Anees *et al.* [6] is better than the proposed scheme with respect to this metric.

### 2) IRREGULAR DEVIATION

One of the problems with the maximum deviation for measuring the quality of encryption is that it only provides the cumulative difference between the histograms of the plaintext image and the corresponding cipher image. Thus, it can not

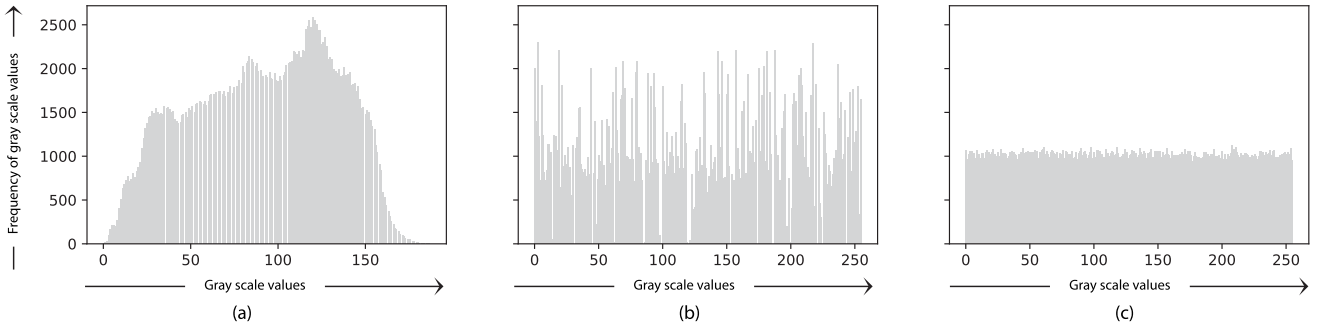



**FIGURE 15.** Histogram analysis for Zelda image. Y-axis is representing the levels of grayscales in image. The X-axis is representing the frequency of grayscale values. a. is showing the histogram for the plaintext image, b. is showing the histogram for an encrypted image using Anees *et al.* [6] method and c. is showing the histogram for an encrypted image by using the proposed scheme.

**TABLE 8.** Entropy for proposed scheme and Anees *et al.* [6] method.

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 7.99923 | 7.70033 |
| Cameraman | 7.99696 | 7.43966 |
| Lena | 7.99931 | 5.40750 |
| Peppers | 7.99938 | 7.80263 |
| Zelda | 7.99923 | 7.70117 |

**TABLE 9.** Maximum deviation results for proposed scheme and Anees *et al.* [6] method.

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 199158 | 232790 |
| Cameraman | 64998 | 77074 |
| Lena | 474797 | 77074 |
| Peppers | 146408 | 179377 |
| Zelda | 213345 | 240416 |

capture the deviation on the level of individual pixels as the difference between the histograms is greater at some pixels but lesser at some other pixels. Hence, Irregular Deviation could be used to capture this behavior. The lower the Irregular Deviation value, the higher the encryption quality. The mathematical representation of the irregular deviation is represented in Eq.8 below:

$$D_{irr} = \sum_{i=0}^{255} \left[ \left| d_i - \left[ \frac{1}{256} \sum_{j=0}^{255} d_j \right] \right| \right] \tag{8}$$

where $d_i$ is the instance of $D$ and $D$ is the histogram of the absolute difference between the plaintext image and the cipher image. $D$ is defined in Eq. 9. Table 10 presents the results of irregular deviation for the 512 × 512 images of Baboon, Cameraman, Lena, Pepper and Zelda for the proposed scheme in comparison to the Anees *et al.* [6] method. Results show that the proposed scheme has smaller irregular deviation values for all encrypted images which indicates that the proposed scheme has better encryption quality.

$$D = histogram(|P - C|) \tag{9}$$

where $P$ and $C$ are the plaintext image and cipher text image, respectively.

**TABLE 10.** Irregular deviation results for proposed scheme and Anees *et al.* [6] method.

| | Proposed Scheme | Amir et al. |
|---|---|---|
| Baboon | 80203 | 134569 |
| Cameraman | 32706 | 56384 |
| Lena | 385859 | 718779 |
| Peppers | 84465 | 108271 |
| Zelda | 63036 | 125206 |

### 3) DEVIATION FROM UNIFORM HISTOGRAM

A uniform histogram is a histogram with equal distribution of pixel values. A uniform histogram is taken as a benchmark to evaluate the quality of encryption where the lesser the image deviates from the uniform histogram, the better the encryption is. A histogram of a perfectly encrypted image is very close to the uniform histogram. Uniform histogram is represented mathematically in Eq.10.

$$D_{uni} = \frac{\sum_{i=1}^{255} |H_{c_i} - H_{u_i}|}{W \times H}$$
$$H_{u_i} = \begin{cases} \dfrac{H \times W}{256} & \text{if } 0 \leq i \leq 255 \\ 0 & \text{if } 0 > i > 255 \end{cases} \tag{10}$$

where $H_{u_i}$ is the histogram value of $i^{th}$ pixel of the uniform histogram, values of $H_{u_i}$ are considered if pixel value lies between 0 to 255 otherwise $H_{u_i}$ values are considered zero for all $0 > i > 255$. $H_{c_i}$ is the $i^{th}$ pixel value of the histogram of cipher image. The lower the value of $D_{uni}$, the better is the encryption quality. Table 11 shows the results of the deviation from uniform histogram of the proposed technique compared to that of Anees *et al.* [6] encryption method. The value of deviation from the uniform histogram should be lower so that the encrypted image will be less deviated from the uniform histogram. For all results for encrypted images using proposed scheme and Amir *et al.* method in Table 11 the deviation from uniform histogram for proposed scheme is lower than Anees *et al.* [6] method which indicates that the encryption quality of the proposed scheme is better than Anees *et al.* [6] method.

**TABLE 11. Deviation from uniform histogram results for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 0.99902 | 0.99904 |
| Cameraman | 0.99609 | 0.99610 |
| Lena | 0.99902 | 0.99979 |
| Peppers | 0.99902 | 0.99904 |
| zelda | 0.99902 | 0.99908 |

### G. MEAN SQUARE ERROR

Mean square error (MSE) is a widely used statistical method to calculate the average squared difference between the pixel values of an encrypted image and its plaintext image. The mean square error for a good quality encryption algorithm is generally ≥30dB [37]. The mathematical representation of the MSE in relation to image encryption is defined in Eq. 11.

$$MSE = \frac{1}{W \times H} \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [P(i,j) - C(i,j)]^2 \qquad (11)$$

Note that $H$ and $W$ are the height and width of the plaintext image and cipher image. $P(i,j)$ is the pixel value of the plaintext image at position $(i,j)$ and $C(i,j)$ is the pixel value of the cipher image at position $(i,j)$. We compared the MSE of the proposed scheme to that of Anees *et al.* [6] encryption method under several images including Baboon, Cameraman, Lena, Peppers and Zelda as depicted in Table 12. Results show that the proposed scheme has greater MSE than Anees *et al.* [6] method which indicates that the security of the images encrypted by the proposed scheme is better than images encrypted by Anees *et al.* [6] method.

**TABLE 12. MSE results for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 39.67941 dB | 39.63439 dB |
| Cameraman | 32.53179 dB | 31.79649 dB |
| Lena | 39.37463 dB | 39.51088 dB |
| Peppers | 39.00139 dB | 38.79973 dB |
| Zelda | 39.02306 dB | 38.75836 dB |

### H. PEAK SIGNAL TO NOISE RATIO

Peak signal to noise ratio is an image quality metric. Used to measure noise between plaintext image and cipher image [38]. PSNR is defined as the ratio of peak signal power to noise power. Mathematical representation of PSNR is shown in Eq. 12.

$$PSNR = 20 \log_{10} \frac{MAX_f}{MSE} \qquad (12)$$

where $MAX_f$ is the maximum possible value of a pixel and MSE is the mean square error between the plaintext image and its cipher image as in Eq. 11. Greater value of PSNR shows that there is more closeness between the plaintext image and encrypted image. If an encryption image has a lower PSNR value then the encryption algorithm is considered better. Table 13 represents the PSNR values of proposed scheme compared to the PSNR values of Amir's encryption method, for the Baboon, Cameraman, Lena, Peppers and Zelda.

**TABLE 13. PSNR for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 9.54241 | 9.49739 |
| Cameraman | 8.41539 | 7.68011 |
| Lena | 9.23763 | 9.37388 |
| Peppers | 8.86441 | 8.66273 |
| Zelda | 8.88607 | 8.62137 |

### I. RESISTANCE TO DIFFERENTIAL ATTACKS

Differential cryptanalysis seeks to find the difference between the plaintext image and the corresponding encrypted image [39]. The attackers make a small change in plaintext image and analyze the impact on cipher image. The attacker then performs a statistical test to find non-randomness in cipher Image. An encryption algorithm is considered to be more secure against differential attacks if a single pixel change in the plaintext image makes a significant change in the corresponding cipher image. Avalanche effect, number of pixels change rate(NPCR) and unified average change intensity (UACI) are the tests usually used to analyze the performance of the encryption method against differential attacks.

#### 1) AVALANCHE EFFECT

In a cryptosystem, a small change in key or a small change in plaintext image should cause a big change or completely change the corresponding encrypted image. This effect is called the avalanche effect. Mean square error (MSE) is used to check the avalanche effect. MSE presents the cumulative error between two cipher images. Eq. 13 below is used to calculate the MSE.

$$MSE = \frac{\sum_{h,w}^{H-1,W-1} [C_1(h,w) - C_2(h,w)]^2}{W \times H} \qquad (13)$$

where $H$ and $W$ are the height and width of the image. $C_1(h,w)$ and $C_2(h,w)$ are the pixel values in the matrices of actual cipher image and the cipher image after a small change in key or a small change in plaintext image at position $(h,w)$. If a small change in input causes 50% or greater change in output then the cryptosystem satisfies strict avalanche criteria [40], [41].

#### 2) NUMBER OF PIXELS CHANGE RATE

NPCR is used to capture the change in cipher images by changing a bit in the corresponding plaintext image. It is an important measure to analyze the ability of an encryption algorithm to resist differential attacks. NPCR presents the variance rate between cipher images after changing a pixel in a plaintext image. Eq. 14 is the mathematical representation of NPCR.

$$NPCR = \frac{\sum_{i=1}^{W} \sum_{j=1}^{H} D(i,j)}{W \times H} 100\%$$

**TABLE 14. Results comparison with literature.**

| Methods in literature | Horizontal Correlation Coefficient | Vertical Correlation Coefficient | Diagonal Correlation Coefficient | Entropy | NPCR | UACI | Time Complexity |
|---|---|---|---|---|---|---|---|
| [6] | 0.1352 | 0.1055 | 0.1220 | 7.8026 | 0.0015 | 0.0010 | Very Low |
| [5] | 0.0732 | 0.0293 | 0.0280 | 7.9801 | 99.36 | 32.72 | High |
| [20] | 0.0220 | -0.0083 | -0.0029 | 7.9972 | 99.61 | 33.49 | Very High |
| [11] | 0.0021 | 0.0009 | 0.0024 | 7.9972 | 99.21 | 33.16 | Low |
| [17] | 0.0020 | 0.0050 | 0.0020 | 7.9986 | 99.59 | 33.27 | Moderate |
| [7] | 0.0068 | 0.033 | 0.0474 | 7.9969 | 99.15 | 33.21 | Low |
| [18] | 0.0019 | 0.0003 | 0.0033 | 7.9942 | 99.42 | 33.35 | Very High |
| Proposed Scheme | 0.0008 | 0.0006 | 0.0033 | 7.9994 | 99.62 | 33.49 | Low |

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \quad (14)$$

where $H$ and $W$ are the height and width of the cipher image. $C_1$ is cipher image and $C_2$ is the cipher image after changing a pixel value in plaintext image. $C_1(i,j)$ is the pixel of cipher image $C_1$ at position $i,j$ and $C_2(i,j)$ is the pixel of cipher image $C_2$ at position $i,j$. NPCR is calculated for the proposed scheme. Table 15 is showing the results of NPCR for the proposed scheme and Anees *et al.* [6] method. Results show that the proposed scheme has greater NPCR than Anees *et al.* [6] method, which indicates that the proposed scheme has more resistance against differential attacks than [6].

**TABLE 15. NPCR for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 99.60594 | 0.00038 |
| Cameraman | 99.60481 | 0.00152 |
| Lena | 99.61929 | 0.00038 |
| Peppers | 99.64142 | 0.00038 |
| Zelda | 99.61014 | 0.00038 |

### 3) UNIFIED AVERAGE CHANGE INTENSITY

UACI is used to measure the average intensity of change between the two cipher images, one for original plaintext image and one after changing a pixel in the plaintext image. Eq. 15 is the mathematical representation of UACI.

$$UACI = \frac{1}{W \times H}\left[\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}(C_1(i,j) - C_2(i,j))}{255}\right] 100\% \quad (15)$$

where $H$ and $W$ are the height and width of the cipher image. $C_1(i,j)$ is the pixel of cipher image $C_1$ at position $i,j$ and $C_2(i,j)$ is the pixel of cipher image $C_2$ at position $i,j$.

UACI is calculated by using Eq. 15 for Baboon, Cameraman, Lena, Peppers and Zelda images. Table 16 is showing the results for the proposed scheme and Anees *et al.* [6] method. The proposed scheme has higher UACI values for all encrypted images which indicates that the proposed scheme is better than previous work [6]. Comparison of the proposed scheme with other methods discussed in the literature is presented in Table 17. Results show that the proposed scheme has better resistance against differential attacks than other methods.

**TABLE 16. UACI for proposed scheme and Anees *et al.* [6] method.**

| | Proposed Scheme | Anees et al. [6] |
|---|---|---|
| Baboon | 33.43754 | 0.00025 |
| Cameraman | 33.48555 | 0.00105 |
| Lena | 33.48595 | 0.00011 |
| Peppers | 33.45324 | 0.00026 |
| Zelda | 33.54295 | 0.00013 |

**TABLE 17. Comparison of NPCR and UACI values for different methods.**

| Test | [38] | [11] | [6] | Proposed |
|---|---|---|---|---|
| NPCR | 99.60111% | 99.61211% | 0.00038% | 99.61929% |
| UACI | 33.56121% | 33.46132% | 0.00026% | 33.48595% |

**TABLE 18. Time taken by different methods to encrypt a 512 × 512 image.**

| Test | [38] | [11] | [6] | Proposed |
|---|---|---|---|---|
| time sec | 3.68 | 1.53 | 1.21 | 1.28 |

### 4) TIME COMPARISON

The machine used for the testing of the proposed scheme is a Core i5 with 8GB RAM. Spyder 3.3.6 is used with Python version 3.7.4. Table 18 demonstrating the results for the proposed scheme and comparison with other methods discussed in the literature. Results showing that the time taken by the proposed scheme is lower than the other methods, which is proving that the proposed scheme is comparatively more efficient.

The extensive experiments are performed to analyze the proposed scheme the results for the proposed scheme along with the results for the other image encryption methods in the literature or shown in Table 14. The results demonstrate that the proposed scheme is more efficient than other image encryption methods. The lowest correlation coefficient results for the proposed scheme make it more resistant to statistical attacks, also the proposed scheme is better in terms of entropy, it has the highest entropy value. In the differential attacks, the test results of the proposed scheme outperform all the methods in the literature by obtaining the highest NPCR and UACI. The proposed scheme comparatively takes shorter time in the encryption and decryption process that makes it more suitable for mobile devices. All these results clearly show that the proposed scheme is a more efficient method for image encryption.

## V. CONCLUSION

In this study, a new chaotic-based image encryption scheme has been proposed utilizing a single AES S-Box, a deviation from the state-of-the-art algorithms where multiple S-Boxes are utilized. While the chaotic-based permutation used in our method maximizes the algorithm's resistance against differential attack, the single S-Box substitution enables more optimal randomization of the values of the image pixels making the encryption more robust against statistical attacks. We have carried out extensive experiments to evaluate the proposed scheme with respect to the state-of-the-art encryption methods under various settings. The results demonstrate the superiority of our scheme and its ability to nullify the statistical attacks despite the fact that we utilize only a single S-Box. Indeed, our proposed scheme has shown promising results in addressing the chosen plaintext attack with very high sensitivity towards the change in the key or the plaintext. We have also provided a detailed comparison of the proposed scheme with other methods in literature (Table 14). As a future work, our proposed scheme can be implemented for color images as currently our scheme is designed for gray scale images. Furthermore, as a future work our proposed scheme can be extended for other media types, such as audio and video. We have implemented logistic map in the proposed scheme for simplicity; future works can explore other chaotic maps and integrate those maps with the proposed scheme. Moreover, it is also possible to design a better S-Box than AES S-Box for the proposed scheme.

## CONFLICT OF INTEREST

The authors declare no conflict of interest.

## REFERENCES


[1] K. M. Sadique and P. Johannesson, "Layered architecture for end-to-end security, trust, and privacy for the Internet of Things," in *Intelligent Computing and Innovation on Data Science*. Singapore: Springer, 2021, pp. 289–298.

[2] A. J. Ibada, P. Ehkan, R. Ngadiran, D. A. Hammood, and A. Alkhayyat, "RGB image encryption using Hill algorithm and chaos system," *J. Phys., Conf. Ser.*, vol. 1962, no. 1, Jul. 2021, Art. no. 012061.

[3] D. Buell, "Modern symmetric ciphers—DES and AES," in *Fundamentals of Cryptography*. Cham, Switzerland: Springer, 2021, pp. 123–147.

[4] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, p. 25, Jun. 2010.

[5] J. Ahmad and S. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1839–1850, Dec. 2015.

[6] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 9, pp. 3106–3118, 2014.

[7] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[9] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," in *Proc. 5th Int. Conf. Signal Image Process.*, Jan. 2014, pp. 102–107.

[10] S. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 51, no. 4, p. 3670, 1995.

[11] P. He, K. Sun, and C. Zhu, "A novel image encryption algorithm based on the delayed maps and permutation-confusion-diffusion architecture," *Secur. Commun. Netw.*, vol. 2021, Mar. 2021, Art. no. 6679288.

[12] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Feb. 2021.

[13] A. Shafique and F. Ahmed, "Image encryption using dynamic S-box substitution in the wavelet domain," *Wireless Pers. Commun.*, vol. 115, no. 3, pp. 2243–2268, 2020.

[14] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and S-box," in *Proc. 6th Int. Conf. Modeling, Simulation, Appl. Optim. (ICMSAO)*, May 2015, pp. 1–6.

[15] S. P. Indrakanti and P. S. Avadhani, "Permutation based image encryption technique," *Int. J. Comput. Appl.*, vol. 28, no. 8, pp. 45–47, Aug. 2011.

[16] S. Anwar and S. Meghana, "A pixel permutation based image encryption technique using chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27569–27590, Oct. 2019.

[17] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, and W. J. Buchanan, "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Pers. Commun.*, pp. 1–28, May 2021. [Online]. Available: https://link.springer.com/article/10.1007/s11277-021-08584-z#citeas

[18] S. Agarwal, "Secure image transmission using fractal and 2D-chaotic map," *J. Imag.*, vol. 4, no. 1, p. 17, Jan. 2018.

[19] L. Quan, L. Pei-Yue, Z. Ming-Chao, S. Yong-Xin, and Y. Huai-Jiang, "Construction of a class of chaos systems with Markov properties," *Acta Phys. Sinica*, vol. 62, no. 17, 2013, Art. no. 170505.

[20] M. Ge and R. Ye, "A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties," *Egyptian Inform. J.*, vol. 20, no. 1, pp. 45–54, 2019.

[21] A. Said, "Measuring the strength of partial encryption schemes," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2, Sep. 2005, p. II-1126.

[22] S. K. Abd-El-Hafiz, S. H. Abdelhaleem, and A. G. Radwan, "Novel permutation measures for image encryption algorithms," *Opt. Lasers Eng.*, vol. 85, pp. 72–83, Oct. 2016.

[23] D. Eastlake and P. Jones, *U.S. Secure Hash Algorithm 1 (SHA1)*, document RFC 3174, 2001.

[24] H. Handschuh, "SHA family (secure hash algorithm)," in *Encyclopedia of Cryptography and Security*. Boston, MA, USA: Springer, 2005.

[25] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, "Study of S-box properties in block cipher," in *Proc. Int. Conf. Comput., Commun., Control Technol. (ICT)*, Sep. 2014, pp. 362–366.

[26] T. Eisenbarth and S. Kumar, "A survey of lightweight-cryptography implementations," *IEEE Design Test Comput.*, vol. 24, vol. 6, pp. 522–533, Nov./Dec. 2007.

[27] N. J. Parmar and P. K. Verma, "A comparative evaluation of algorithms in the implementation of an ultra-secure router-to-router key exchange system," *Secur. Commun. Netw.*, vol. 2017, pp. 1–7, Jan. 2017.

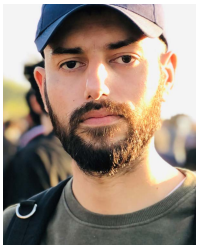
[28] E. Mosekilde, *Topics in Nonlinear Dynamics: Applications to Physics, Biology and Economic Systems*. Singapore: World Scientific, 2003.

[29] R. Brandom, "Google just cracked one of the building blocks of web encryption (but don't worry)," *Verge*, vol. 23, no. 2, pp. 1–6, Feb. 2017.

[30] F. Dikbaş, "A novel two-dimensional correlation coefficient for assessing associations in time series data," *Int. J. Climatol.*, vol. 37, no. 11, pp. 4065–4076, Sep. 2017.

[31] I. F. Elashry, O. S. F. Allah, A. M. Abbas, S. El-Rabaie, and F. E. A. El-Samie, "Homomorphic image encryption," *J. Electron. Imag.*, vol. 18, no. 3, Jul. 2009, Art. no. 033002.

[32] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.
[33] R. M. Gray, *Entropy and Information Theory*. New York, NY, USA: Springer, 2011.
[34] H. Ahmed, H. M. Kalash, and O. Allah, "Implementation of RC5 block cipher algorithm for image cryptosystems," *Int. J. Inf. Technol.*, vol. 3, no. 4, pp. 1–6, 2007.
[35] R. Enayatifar, "Image encryption via logistic map function and heap tree," *Int. J. Phys. Sci.*, vol. 6, no. 2, pp. 221–228, 2011.
[36] H. M. Elkamchouchi and M. A. Makar, "Measuring encryption quality for bitmap images encrypted with Rijndael and Kamkar block ciphers," in *Proc. 22nd Nat. Radio Sci. Conf. (NRSC)*, 2005, pp. 277–284.
[37] A. B. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of RC5 and RC6 block ciphers on digital images," in *Proc. 8th Int. Multi-Conf. Syst., Signals Devices*, Mar. 2011, pp. 1–6.
[38] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, 2016.
[39] E. Conrad, S. Misenar, and J. Feldman, "Domain 8: Software development security (understanding, applying, and enforcing software security)," in *CISSP Study Guide*, 3rd ed. Boston, MA, USA: Syngress, 2016, pp. 429–477.
[40] S. D. Sanap and V. More, "Performance analysis of encryption techniques based on avalanche effect and strict avalanche criterion," in *Proc. 3rd Int. Conf. Signal Process. Commun. (ICPSC)*, May 2021, pp. 676–679.
[41] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps," *IEEE Access*, vol. 9, pp. 52277–52291, 2021.



**JAMEEL ARIF** received the B.Sc. degree in mathematics and physics and the M.C.S. degree in computer science from The University of Azad Jammu and Kashmir, Muzaffarabad, Pakistan, in 2016 and 2019, respectively. He is currently pursuing the M.Phil. degree in computer science with Quaid-i-Azam University, Islamabad, Pakistan. His research interests include cybersecurity, cryptography, image encryption, data network security, and artificial intelligence.

**MUAZZAM A. KHAN** (Senior Member, IEEE) received the Ph.D. degree from IIUI, in 2011, and the postdoctoral degree from the University of Missouri, KC, USA, in 2016. He joined the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2013, and promoted to the Associate Dean, in 2017. He has been at the School of Computer Science, University of Ulm, Germany, and the Networking and Multimedia Laboratory, School of Computer and the Electrical Engineering, University of Missouri (UMKC), as a Research Fellow. He is currently working as an Associate Professor (Tenured) and the Head ICESCO Chair for data analytics and edge computing at Quaid-i-Azam University, Islamabad. He is also a member of the Pakistan Academy of Sciences. He has published more than 150 publications and book chapters. His research interests include the Internet of Things, next generation intelligent networks, blockchain, information and network security, vehicular *ad-hoc* networks, and acoustic networks.

**BARAQ GHALEB** (Student Member, IEEE) received the B.Sc. degree in computer science from The University of Jordan, Amman, Jordan, in 2009, the M.Sc. degree from the Jordan University of Science and Technology, Irbid, Jordan, in 2013, and the Ph.D. degree in applied computing from Edinburgh Napier University, Edinburgh, U.K. He holds one patent in the field of the IoT routing. His current research interests include routing protocols in low-power and lossy networks and the Internet of Things (IoTs), security of LLNs, and the IoT in addition to data mining.

**JAWAD AHMAD** (Senior Member, IEEE) is an experienced researcher with more than ten years of cutting-edge research and teaching experience in prestigious institutes, including Edinburgh Napier University (U.K.), Glasgow Caledonian University (U.K.), Hongik University (South Korea), and HITEC University Taxila (Pakistan). He has coauthored more than 100 research papers, in international journals and peer-reviewed international conference proceedings. He has taught various courses both at Undergraduate (UG) and Postgraduate (PG) levels during his career. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. He is an invited reviewer for numerous world-leading high-impact journals (reviewed more than 100 journal papers to date). His research interests include cybersecurity, multimedia encryption, and machine learning.

**ARSLAN MUNIR** (Senior Member, IEEE) received the M.A.Sc. degree in electrical and computer engineering (ECE) from the University of British Columbia, Vancouver, Canada, in 2007, and the Ph.D. degree in ECE from the University of Florida, Gainesville, FL, USA, in 2012.

From 2007 to 2008, he worked as a Software Development Engineer at the Embedded Systems Division, Mentor Graphics Corporation. He was a Postdoctoral Research Associate with the ECE Department, Rice University, Houston, TX, USA, from May 2012 to June 2014. He is currently an Associate Professor with the Department of Computer Science, Kansas State University. His current research interests include embedded and cyber-physical systems, secure and trustworthy systems, parallel computing, artificial intelligence, and computer vision. He has received many academic awards, including the Doctoral Fellowship from Natural Sciences and Engineering Research Council (NSERC) of Canada. He earned gold medals for best performance in electrical engineering and gold medals and academic roll of honor for securing rank one in pre-engineering provincial examinations (out of approximately 300,000 candidates).

**UMER RASHID** received the B.S. degree in computer science from The University of Lahore, Pakistan, in 2005, and the M.Phil. and Ph.D. degrees in computer science from Quaid-i-Azam University, Islamabad, Pakistan, in 2008 and 2017, respectively. He has teaching and research experience in international organizations. He is currently working as an Assistant Professor with Quaid-i-Azam University. His work is published in international journals and conferences. His research interests include user-centered computing, multimedia information retrieval, and multimedia technology.

**AHMED Y. AL-DUBAI** (Senior Member, IEEE) received the Ph.D. degree in computing from the University of Glasgow, Glasgow, U.K., in 2004. He is currently a Professor of networking and communication algorithms with the School of Computing, Edinburgh Napier University, Edinburgh. His research interests include communication algorithms, mobile communication, the Internet of Things, and future internet. He has received several international awards.