IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 20, 2021, accepted November 2, 2021, date of publication November 8, 2021, date of current version November 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3125961

Integration of Spatial and Frequency Domain Encryption for Digital Images

ARSLAN SHAFIQUE[1], MOHAMMAD MAZYAD HAZZAZI[2], ADEL R. ALHARBI[3], AND IQTADAR HUSSAIN[4]

[1]Department of Electrical Engineering, Riphah International University, Islamabad 46000, Pakistan
[2]Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia
[3]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[4]Department of Mathematics, Statistics, Physics, Qatar University, Doha, Qatar

Corresponding author: Arslan Shafique (arslan.shafique@riphah.edu.pk)

This work was supported by the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant R. G. P. 2/150/42.

ABSTRACT Transmission of multimedia data such as images, videos, and audio over the Internet is risky due to cyberattacks. To overcome the security issues, several encryption schemes are proposed over the last few decades which also possess few vulnerabilities such as time inefficiency and weak security. In this research, to provide the highest level of security to the digital data, chaos is incorporated for the scrambling of rows and columns of the plaintext image. Further, a noisy image is generated based on the chaotic logistic map and the suitable initial conditions which are selected based on the analysis performed. For the reduction of the encryption computational time, a Discrete Wavelet Transform (DWT) is used in which only low-frequency bands are encrypted because most of the plaintext information lies in such frequency bands. To gauge the performance of the proposed encryption scheme, several security tests such as entropy, correlation, energy, peak signal to noise ratio, mean square error, keyspace, and key sensitivity analysis, noise-resistant, and cropping attack analyses are performed. From the cropping and noise attack analysis, we have found that the proposed encryption algorithm can decrypt the plaintext image with negligible loss of information but the content of the plaintext image can be visualized.

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

I. INTRODUCTION

The insecure channel (Internet) has been effectively used for the last few decades for the transmission of multimedia data. Internet is proved to be high speed and low-cost transmitting medium, but at the same time, it does not provide reliable security to the digital data [1]. In these circumstances, transmitting data can be risky and due to certain security issues, it has opened doors for the researchers for making the digital data safe and secure. To secure sensitive information, chaos theory, machine learning, and frequency transform methods such as DWT and Discrete Cosine Transform (DCT) based methods can be used in encryption techniques [2], [3]. In frequency domain encryption, it is always required to convert the pixel values into certain frequency components before further processing. While, for spatial domain encryption, any encryption technique may apply directly to the pixel values for the desired purpose. It can be achieved either by chaos theory, direct scrambling, or substitution process [4], [5].

Continuing the discussion, the lossless image technique is proposed by Tedmori et al in which before applying the spatial domain processing on the pixel values, DCT is used to convert them into frequency components [6]. In [7], et. al proposed a frequency domain encryption that consists of multiple rounds. To convert the pixel values into its frequency components, Fractional Fourier transform (FFT) is integrated with the spatial domain encryption. Due to the several encryption rounds, it takes more time to complete the encryption process which is not suitable for real-time applications. In [8], a color image encryption algorithm is presented in which Arnold transform and color-blend operation are incorporated with DCT. However, Liu *et al.* [8] used Fractional Fourier Transform (FFT) with multiple couped logistic maps to improve the encryption scheme proposed in [8].

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

For the direct manipulation of image pixels, spatial domain encryption is frequently is used by the researchers. To encrypt the digital in the spatial domain, substitution Boxes and Chaos-based techniques are mainly employed. In case of substitution, single and multiple S-boxes may use to substitute the image pixels. However, a single S-box is not suitable for the proper concealment of pixel values. The drawbacks of using a single S-box are highlighted in [9]. Moreover, the image sized 256×256 takes more than ten seconds for its substitution which is not considered ideal for practical systems. To resolve the problems of using the single S-box, Anees et. al. [9] used the multiple S-boxes which has proved more robust. However, the single S-box substitution problem is resolved to some extent, but still, it is failed to properly encrypt the images which consist of a low number of gray levels. Extending the idea proposed in [9], Jawad *et al.* [10] proposed a multiple S-boxes-based image encryption scheme which provides much better results than the encryption scheme proposed in [9].

In [11], *et al.* proposed a color image encryption scheme in which substitution and chaotic maps are integrated to provide the highest level of security to the digital images. In S-box based encryption scheme, it is crucial to use such an S-box which exhibits strong cryptographic properties. Therefore, to construct a robust S-box, a new technique to generate a strong S-box is proposed in [12] which is based on the chaotic cubic logistic map. In [13], the authors addressed few vulnerabilities that exist in the encryption scheme proposed in [14] and made necessary improvements to make it more robust and secure against cyberattacks. Further, an S-box is also generated using a 1D Chaotic map and applied in the said encryption scheme. It might be insecure because a single S-box is used instead of multiple S-boxes. In an encryption scheme, S-box is a source of creating diffusion in the plaintext image. The idea of confusion-diffusion is proposed by Claude Shannon [15]. According to his theory, an encryption scheme could be more secure if it consist of both confusion and diffusion properties. In [16], Pisarchick *et al.* proposed an idea of the chaotically coupled map which is used to create diffusion in the image pixels. Whereas Shatheesh *et al.* [17] proposed a Zigzag confusion and diffusion method which incorporates XOR operation as a result better results were achieved in terms of correlation, entropy, contrast, peak signal to noise ratio, and mean square error. In [18], a detailed comparison of security parameters for chaos and non-chaos-based image encryption is presented. While, in [19], a suitable level of security is achieved which is proved by analyzing the security parameters. The only vulnerability that can exist in the scheme proposed in [19] is the high encryption computational time because it uses the mechanism of confusion and diffusion stages one by one instead of applying them simultaneously.

To overcome the vulnerabilities discussed above, we propose a DWT and chaos-based encryption technique. The major contributions are as follows:

- A new algorithm is designed to secure the digital images in which DWT and chaos theory are incorporated.
- To reduce the encryption computational time, only the low-frequency sub-band is encrypted instead of encrypting the other sub-bands which consist of high frequencies. Apart from time efficiency, providing a high level of security a chaos theory is incorporated for generating random sequences and noisy images.
- Security attacks such as brute force attack, cropping attack, and noise attack are performed to prove the robustness of the proposed work against such attacks.
- Several experiments and security analyses such as entropy, correlation, energy, peak signal to noise ratio, key sensitivity and mean square error are also conducted to gauge the security level of the proposed work.

II. PRELIMINARIES

The proposed encryption algorithm is categorized into two parts:

- Chaos theory
- Discrete Wavelet Transform

Chaos is incorporated for two major purposes (a) to create random sequences for creating confusion in the plaintext image (b) a noisy is generated to create diffusion in the RGB components of the plaintext image.

A. CUBIC- LOGISTIC MAP (CLM)

The modified form of a chaotic map is known as CLM and it is a one-dimensional chaotic map [20]. The mathematical form for CLM is given in Equation 1:

$$\Omega_{i+1} = \omega * \Omega_i(1 - \Omega_i) * (2 + \Omega_i) \tag{1}$$

The region in which the CLM shows chaotic behaviour is given below:

$$\Omega_0 \in (01)$$
$$\omega \in [1.421.60)$$

CLM is non-periodic, key sensitive and able to generate random sequences which are difficult to predict. In case of reliability, it was claimed in [20] that CLM can perform better than the chaotic logistic map [21]. Chaotic ranges vary with the nature of chaotic systems. Therefore, it is necessary to analyze the chaotic behavior so that suitable initial values can be selected for the generation of truly random sequences [22]–[29].

In CLM, a control parameter ω plays a vital role in the generation of random values. By varying the value of ω, the chaotic system may show different behavior [30]–[34]. For instance, at ω=1.0 and $\omega = 1.3$, CLM can generate few values which are different from each other, which means, by selecting such values of ω, the CLM cannot generate random values. On the other hand, when ω increases from 1.0 to 1.55, the CLM generates random values till 200^{th} iteration as it is shown in Figure 1.

B. DISCRETE WAVELET TRANSFORM

A wavelet transform can be used to convert the signal into its wavelet components. Wavelets have the ability to separate the fine details in a signal [19]. For instance, in the case of digital images, a wavelet is used to split the edges (fine details) and the low-frequency details. For this purpose, very small and large wavelets are used. Small wavelets are for isolating the fine details. Whereas, large wavelets are for separating the coarse details. Wavelet transform can be a very powerful tool to analyze the local spectrum of dynamic signals such as seismic, radar, sonar, and for image processing and compression. In the proposed encryption methodology, the Haar wavelet is used to transform the plaintext into different frequencies. By decomposing the plaintext image using DWT, four frequency sub-bands such as *LL* sub-band, *LH* sub-band, *HL* sub-band, and *HH* sub-band can be produced.

The Haar wavelet transform can be represented as $Q' = HPH^T$ in which P is a plaintext image having equal number of pixel rows and columns i.e the size of image P is R(rows) $\times$ R(columns), H represents the Haar transform matrix having the size equal to the plaintext image and Q is the transform matrix which contain the Haar basis function $h_a(w)$. Where $w \in [0\ 1]$ and a is defined as $a|\ a \in N \wedge 0 \leq a \leq R-1\ \}$.It can be decompose uniquely as:

$$a = 2^b + t,$$

where b is the highest power of 2 and t is the reminder which is: $t = 2^b - a$. The basis function of haar can be defined by equation 2.

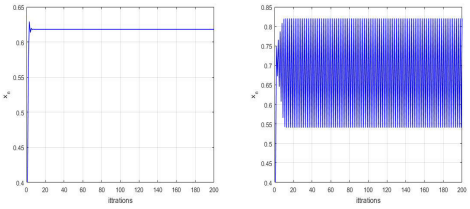
$$h_a(w) = \frac{1}{\sqrt{R}} \begin{cases} 1 & ifa = 0 \ \ \& \ \ 0 \leq w < 1 \\ 2^{b/2} & ifa > 0 \ \ \& \ \ t/2^b \leq w < \dfrac{t+0.5}{2^b} \\ -2^{b/2} & ifa > 0 \ \ \& \ \ (t+0.5)/2^b \leq w < \dfrac{t+1}{2^b} \\ 0 & \text{Elsewhere} \end{cases} \tag{2}$$

A 2D Discrete Haar Wavelet Transform (DHWT) is obtained by substituting the inverse version of the transformation kernel as given in Equation 3.

$$h'(w,a) = \frac{1}{\sqrt{R}} h_a(w/M) \qquad for\ \ w = 0, 1, 2, \ldots, R-1 \tag{3}$$

where, $h_a(w)$ is given as:

$$h_a(w) = H' = \begin{Bmatrix} h_0(\frac{0}{R}) & h_0(\frac{1}{R}) & \ldots . h_0(\frac{R-1}{R}) \\ h_1(\frac{0}{R}) & h_1(\frac{1}{R}) & \ldots . h_1(\frac{R-1}{R}) \\ h_2(\frac{0}{R}) & h_2(\frac{1}{R}) & \ldots . h_2(\frac{R-1}{R}) \\ \vdots & \vdots & \ddots \\ h_{R-1}(\frac{0}{R}) & h_{R-1}(\frac{1}{R}) & \ldots h_{R-1}(\frac{R-1}{R}) \end{Bmatrix} \tag{4}$$



(a) $\omega = 1.0$ (b) $\omega = 1.3$

(c) $\omega = 1.48$ (d) $\omega = 1.55$

FIGURE 1. (a-d) Four different values of ω are selected to generate different random signals.

(a) Plaintext image

(b) LL frequency sub-band (c) LH frequency sub-band

(d) HL frequency sub-band (e) HH frequency sub-band

FIGURE 2. Frequency bands extracted from the cameraman image using DWT.

The resulting transformation matrix for a = 0,1,2,…., R - 1 is given by equation 5.

$$H = \frac{1}{\sqrt{R}} H' \tag{5}$$

In the case of two-dimensional signals i.e. digital images I(R, C), each pixel row is analyzed in the horizontal direction by high pass filter $\alpha(R)$ and low pass filter $\beta(R)$ and the output of both the filter is obtained in the form of images L_r and H_r having the size of $\frac{R}{2^1} \times \frac{C}{2^1}$. After that, high pass filter $\alpha(C)$ and low pass filter $\beta(C)$ is applied to analyze columns of the

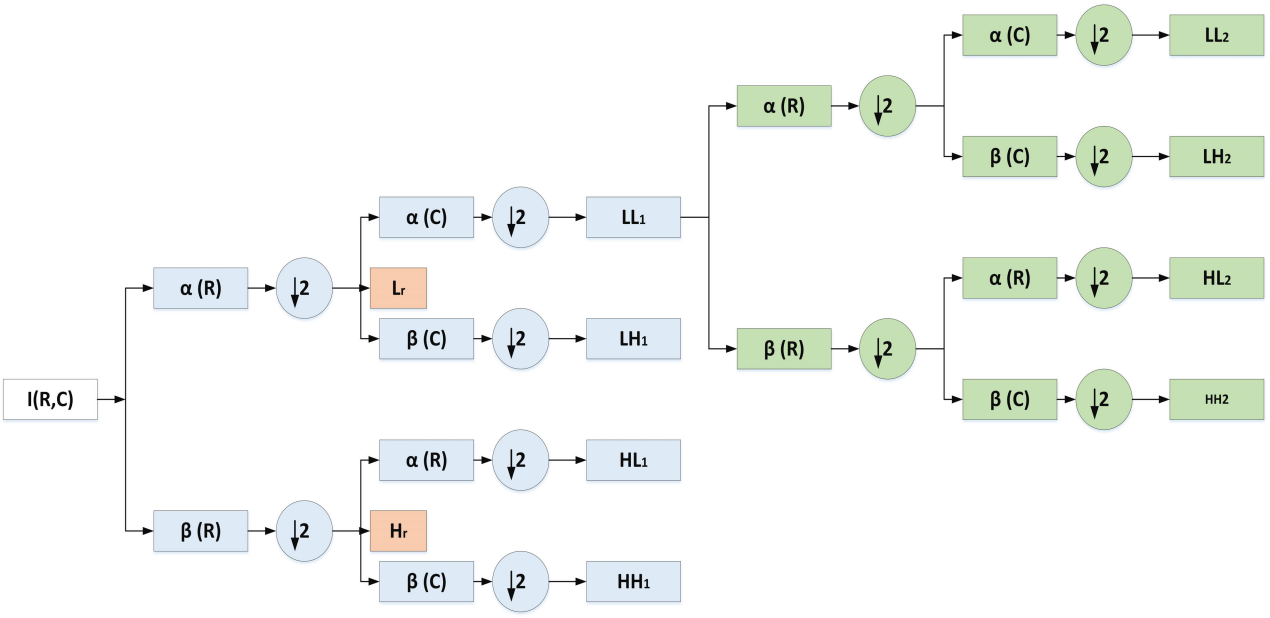


FIGURE 3. 2^{nd} level decomposition of digital image using 2D-DWT.

new image L_r and H_r. in the vertical direction. This produces the four frequency sub-bands LL_1,LH_1, HL_1 and HH_1. Such frequency sub-bands will be down sampled by the factor of 2 as shown in Figure 2.

For the 2^{nd} level wavelet decomposition, same procedure is applied on the LL_1 sub-band to produce further frequency sub-bands LL_2,LH_2, HL_2 and HH_2 having the size of each sub-band $\frac{R}{2^2} \times \frac{C}{2^2}$. The generalized form for the decomposition of wavelet frequency sub-bands is $\frac{R}{2^n} \times \frac{C}{2^n}$ in which the value of n may vary from [1 ∞-1] depending upon the decomposition level of wavelets. For the n level decomposition, the frequency sub-bands will be LL_n, LH_n, HL_n and HH_n. Figure 3 shows the decomposition of plaintext image upto 2^{nd} level using 2D-DWT.

III. PROPOSED ENCRYPTION SCHEME

Cubic logistic map and DWT are two main parts of the proposed algorithm that plays an important role in the concealment of plaintext information. The process of generation of security keys for the proposed encryption algorithm is given in the section III-A.

A. KEY GENERATION PROCESS

The permutation key is generated using the chaos by following steps:

1) Iterate Equation 1 $R \times C$ times using the initial conditions Ω_1, ω_1, Ω_2, ω_2, Ω_3 and ω_3 and generate random values. The number of values will be equal to the number of pixels present in one color component. These random values are known as a stream.
2) The generated value is multiplied by any large integer number N.
3) Convert the floating number into integer values by truncating all the numbers placed right after the decimal point.
4) To restrict the large values generated in step 3 in the interval [0 255], take modulo operation. Mathematically the generated sequences are given in Equations 6, 7 and 8:

$$X = uint8(mod(floor((stream_1) * N_1); \quad \text{Keys are:} \quad \Omega_1, \omega_1 \tag{6}$$

$$Y = uint8(mod(floor((stream_2) * N_2); \quad \text{Keys are:} \quad \Omega_2, \omega_2 \tag{7}$$

$$Z = uint8(mod(floor((stream_3) * N_3); \quad \text{Keys are:} \quad \Omega_3, \omega_3 \tag{8}$$

5) Now the sequences X, Y and Z will be used as a permutation keys to permute the rows and the columns of RGB components respectively.

B. ENCRYPTION PROCESS

The schematic diagram of the proposed encryption scheme is shown in 4. Steps used to encrypt the plaintext image using the proposed algorithm are as follows:

- **Step 1:** Input image of size $R \times C \times 3$ in which R and C represents the rows and columns of the plaintext image (P) respectively.
- **Step 2:** Red, green and blue (RGB) components of the input image are extracted from the image P.
- **Step 3:** For the rows and columns scrambling of the RGB components, the sequences X, Y and Z will be incorporated as key sequences.

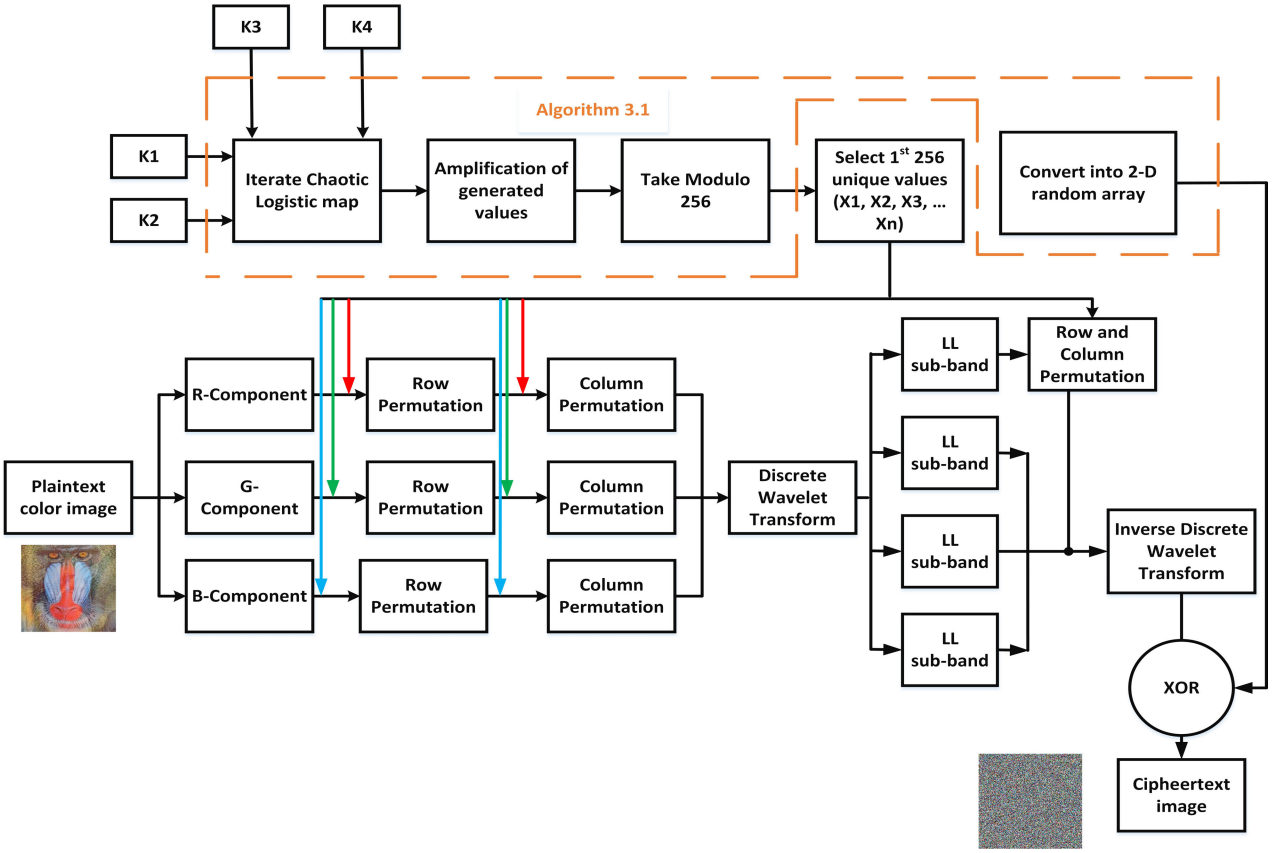


FIGURE 4. Proposed algorithm for color image encryption.

- **Step 4:** Apply DWT on the permuted components (per_{red}, per_{blue}, and per_{green}) to get the frequency sub-bands $\{LL_{1R}, LH_{1R}, HL_{1R}, HH_{1R}\}$, $\{LL_{1G}, LH_{1G}, HL_{1G}, HH_{1G}\}$ and $\{LL_{1B}, LH_{1B}, HL_{1B}, HH_{1B}\}$.
- **Step 5:** For the 2^{nd} level wavelet decomposition, apply DWT on LL_R, LL_G and LL_B. Mathematically, steps 5 and 6 can be written as:

$$\begin{aligned}
\text{DWT}(\text{per}_{red}) &\rightarrow [LL_{1R}, LH_{1R}, HL_{1R}, HH_{1R}],\\
\text{DWT}(\text{per}_{green}) &\rightarrow [LL_{1G}, LH_{1G}, HL_{1G}, HH_{1G}],\\
\text{DWT}(\text{per}_{Blue}) &\rightarrow [LL_{1B}, LH_{1B}, HL_{1B}, HH_{1B}],\\
\text{DWT}(LL_{1R}) &\rightarrow [LL_{2R}, LH_{2R}, HL_{2R}, HH_{2R}],\\
\text{DWT}(LL_{1G}) &\rightarrow [LL_{2G}, LH_{2G}, HL_{2G}, HH_{2G}],\\
\text{DWT}(LL_{1B}) &\rightarrow [LL_{2B}, LH_{2B}, HL_{2B}, HH_{2B}],
\end{aligned}$$

  The LL sub-bands have low-frequency components which mean most of the information lies in the LL sub-bands. Therefore, to reduce the encryption computational time, scramble the rows and columns of only LL sub-bands instead of all the frequency sub-bands using the sequences X, Y and Z.
- **Step 6:** The inverse wavelet transform is used to convert the manipulated frequency components of per_red, per_blue, and per_green components into real values and stored these images in $I_{per-red}$, $I_{per-green}$ and $I_{per-blue}$.
- **Step 7:** Generate random image using CLM by selecting the initial conditions (ω_4 and Ω_4).
  Algorithm 1 is given for the generation of the random image.
- **Step 8:** $I_{per-red}$, $I_{per-green}$ and $I_{per-blue}$ are than passed through XOR operation with the random image which is generated using algorithm 3.1. Finally, combine all the XORed images to generate the ciphertext image. The enciphered images and their corresponding histogram generated using the proposed encryption algorithm are shown in Figure 5.

IV. STATISTICAL SECURITY ANALYSIS

Statistical security analyses of the proposed technique and a comparison is made is in this section. Such analyses include; mean square error (MSE), entropy, peak signal to noise ratio (PSNR), energy, contrast, entropy, and correlation. Mathematically, such parameters can be calculated using Equations 9 [35]–[40].

$$MSE = \frac{1}{xw}\sum_{0}^{x-1}\sum_{0}^{w-1}(f(a,b) - g(a,b))^2 \tag{9}$$

where the size of the image is defined by xw. Whereas, $P(a,b)$ and $C(a,b)$ are the plaintext and ciphertext images

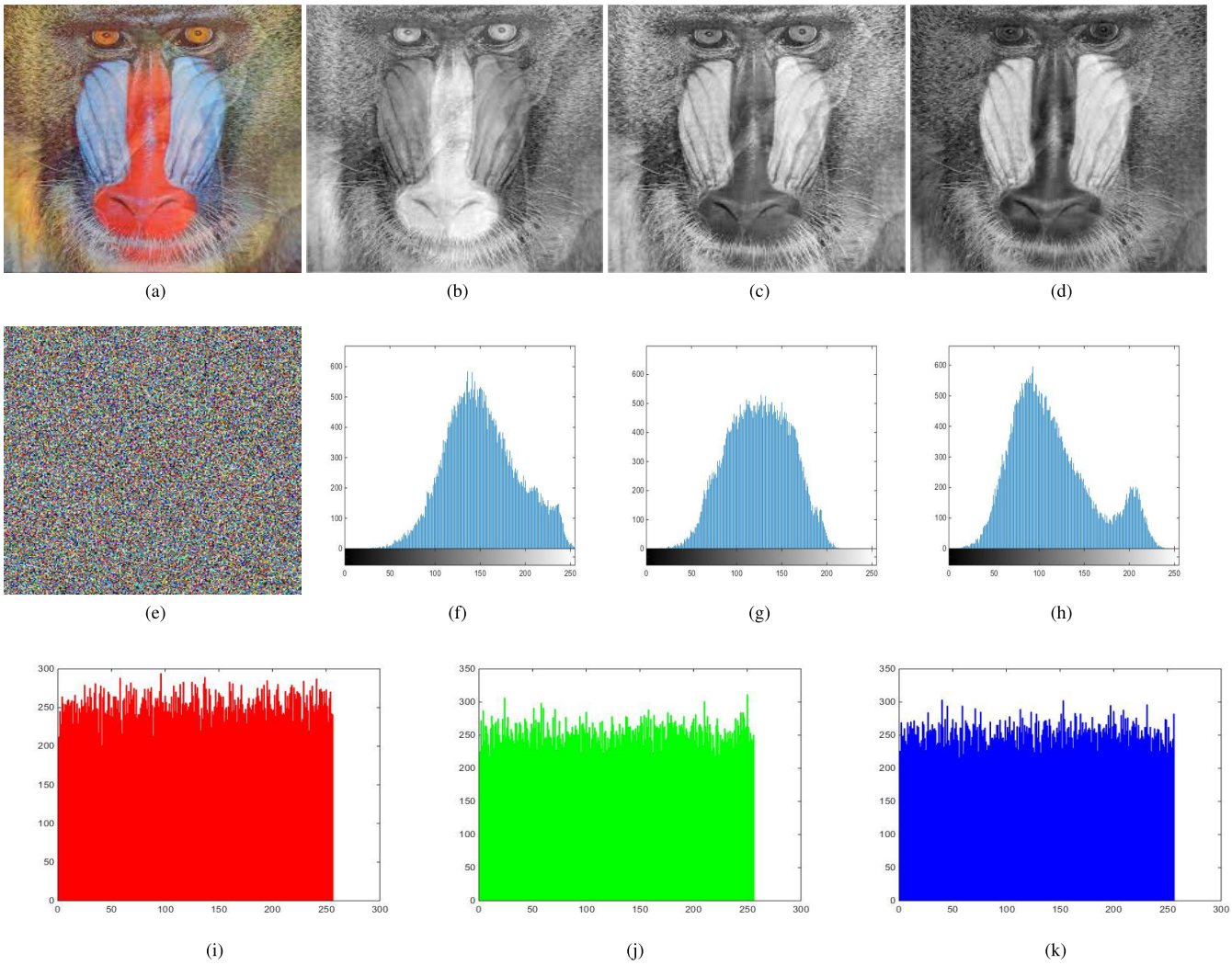


FIGURE 5. (a) Color image of Baboon (b-d) Red, Green and Blue components (e) Enciphered color image (f-h) Histogram of the corresponding Red, Blue and Green components (i-k) histogram of encrypted Red, Blue and Green components.

respectively.

$$PSNR = log_{10}(\frac{MAX_P}{\sqrt{MSE}}) \tag{10}$$

where the maximum pixel value of the plaintext image is represented by MAX_P.

$$Entropy = -\sum im(p_i) log_2 en(c_i) \tag{11}$$

where: $im(p_i)$ is the probability of occurrence of random variable p.

$$Corr - Coeff = \frac{\frac{1}{N}\sum_{j=1}^{N}(x_i - E(x))(y_i - E(y))}{\sigma_x \sigma_y} \tag{12}$$

$$\sigma_x = \sqrt{VARx}, \qquad \sigma_y = \sqrt{VARy} \tag{13}$$

$$VAR(x) = \frac{1}{N}\sum_{j=1}^{N}(x_i - E(x))^2 \tag{14}$$

$$Contrast = \sum |r - x|^2 im(r, x) \tag{15}$$

where the gray-level co-occurrence matrices is represented by im(r,x).

$$Energy = \sum im(x, y)^2 \tag{16}$$

where: $im(i, j)$ is the value of the pixel in an image at i^{th} row and j^{th} column.

Various statistical values of the security parameters which are deduced from the ciphertext images generated using the proposed encryption algorithm are displayed in Tables 1-3. It can be analyzed from Tables 1-3, the proposed algorithm offers better security when it compares to the existing encryption schemes.

A. HISTOGRAM ANALYSIS

Pixel distribution of any image can be observed by the histogram analyses [52]–[54]. For the strong encryption technique, the histogram of the ciphertext image should be flat, uniform, and completely different from the histogram of the

Algorithm 1

Inputs: Chaotic map equation, initial conditions (ω_4 and Ω_4)

→Using initial values and CLM equation, generate $M \times N$ random values by iterating CLM $M \times N$. →Create an array(P) to store the random values generated in step 1.

→ The array P is updated by using following mathematical equation:

$$\phi = P_i \times K_{num}$$

→ Floor operation is used to truncate all digits which are placed after decimal points. The resultant values are saved in an array β.

→ The modulo operation is incorporated to limit the values in the interval [0,255]

$$\alpha = \text{mod}\ (\beta, 256)$$

→Convert the 1-D array generated in step 4 into a 2-D array to create a random image.

End

TABLE 1. Statistical security analysis of the proposed and existing encryption schemes.

Red-Component						
Original color images	**MSE**	**PSNR**	**Entropy**	**Correlation**	**Energy**	**Contrast**
House	259	19	7.9991	0.0002	0.155	9.2412
Pepper	254	16	7.9993	-0.0055	0.0157	10.7894
Tree	25	15	7.9989	0.0011	0.0156	10.1586
Baboon	247	17	7.9994	0.0002	0.0154	10.7915
Forest	245	20	7.9992	-0.0036	0.0153	10.7343
Aeroplane	257	17	7.9998	0.0008	0.0153	10.7984
Lena	252	17	7.9993	-0.0016	0.0154	10.1356
Man	26	16	7.9991	0.0008	0.0152	10.7547
Sky	253	16	7.9993	-0.0005	0.0156	9.9892
Bottles	253	19	7.9989	0.0004	0.0151	9.9782
Bike	255	16	7.9991	0.0003	0.0154	9.9986
Goat	255	18	7.9991	0.0002	0.0151	10.6975
Butterfly	257	19	7.9995	-0.0065	0.0154	9.9984
Clothes	256	17	7.9994	-0.003	0.0158	10.6986
Cameraman	250	16	7.9992	0.0007	0.0156	9.9978
Boat	247	18	7.9989	0.0005	0.0154	9.9911
Girl	254	19	7.9992	-0.0041	0.0153	9.9986
Plant	256	17	7.9987	- 0.0007	0.0153	10.9743
Lion	254	15	7.9992	-0.0086	0.0158	10.6873
Sun	2433	18	7.9989	-0.0005	0.0155	10.9785
Bridge	252	18	7.9991	0.0003	0.0159	9.998
Existing schemes comparison						
[41]	254	18	7.9897	-0.0027	0.0155	9.6789
[42]	244	17	7.9977	-0.0066	0.0157	9.9916
[43]	248	19	7.9997	0.0008	0.0159	9.3796
[44]	246	20	7.9976	- 0.0023	0.0154	10.0032
[45]	218	20	7.9995	0.0007	0.0155	9.9893
[46]	257	16	7.9895	-0.0077	0.0157	9.8749
[47]	225	24	7.9936	0.0014	0.0155	10.0344
[48]	255	21	7.9982	0.0002	0.0157	9.9346
[49]	248	1	7.9997	-0.0026	0.0154	9.8725
[50]	241	22	7.9982	0.0008	0.0157	9.4612
[51]	243	16	7.982	0.0081	0.0153	9.644

plaintext image. Figure 5(f-h) and 5(i-k) show the histogram of the RGB components of plaintext and cyphertext image in which it can be seen that the histogram for the proposed

TABLE 2. Statistical security analysis of the proposed and existing encryption schemes.

Green-Component						
Plaintext images	**MSE**	**PSNR**	**Entropy**	**Correlation**	**Energy**	**Contrast**
Clothes	258	16	7.9998	-0.0036	0.0158	10.6986
Girl	252	17	7.9992	-0.0041	0.0152	9.9988
Tree	255	17	7.9985	0.0011	0.0158	10.1582
Goat	253	16	7.9991	0.0002	0.0156	10.6975
Butterfly	253	16	7.9992	-0.0065	0.0154	9.9981
Plant	255	16	7.9985	- 0.0004	0.0152	10.9744
Boat	247	16	7.9985	0.0008	0.0154	9.9912
Sky	255	15	7.9994	-0.0014	0.0158	9.9891
House	256	15	7.9994	0.0003	0.157	9.2412
Lion	254	17	7.9994	-0.0085	0.0156	10.6877
Man	262	14	7.9988	0.0007	0.0154	10.7547
Sun	245	16	7.9985	-0.0001	0.0154	10.9786
Aeroplane	254	18	7.9988	0.0005	0.0158	10.7986
Bike	254	16	7.9991	0.0002	0.0155	9.9984
Lena	254	17	7.9987	-0.0011	0.0154	10.1353
Bottles	256	17	7.9978	0.0004	0.0157	9.9782
Forest	246	18	7.9991	-0.0032	0.0155	10.7342
Bridge	259	18	7.9992	0.0004	0.0156	9.9988
Pepper	254	14	7.9991	-0.0056	0.0155	10.7892
Cameraman	254	16	7.9995	0.0004	0.0153	9.9972
Baboon	245	17	7.9992	0.0001	0.0157	10.7682
Existing schemes comparison						
[41]	254	18	7.9896	-0.0027	0.0152	9.6789
[46]	257	19	7.9893	-0.0071	0.0155	9.8746
[42]	252	19	7.9942	-0.0062	0.0161	9.9916
[45]	210	18	7.9991	0.0002	0.0156	9.9894
[44]	243	18	7.9979	- 0.0022	0.0157	10.0036
[48]	255	20	7.9989	0.0002	0.0156	9.9343
[43]	249	18	7.9992	0.0009	0.0158	9.3792
[47]	225	21	7.9932	0.0011	0.0158	10.0352
[49]	235	19	7.9998	-0.0023	0.0161	9.8727
[50]	240	21	7.9980	0.0003	0.0601	9.4616
[51]	2465	17	7.9828	0.0087	0.0156	9.6442

encryption technique satisfies the three aforementioned properties.

B. KEY SENSITIVITY ANALYSIS

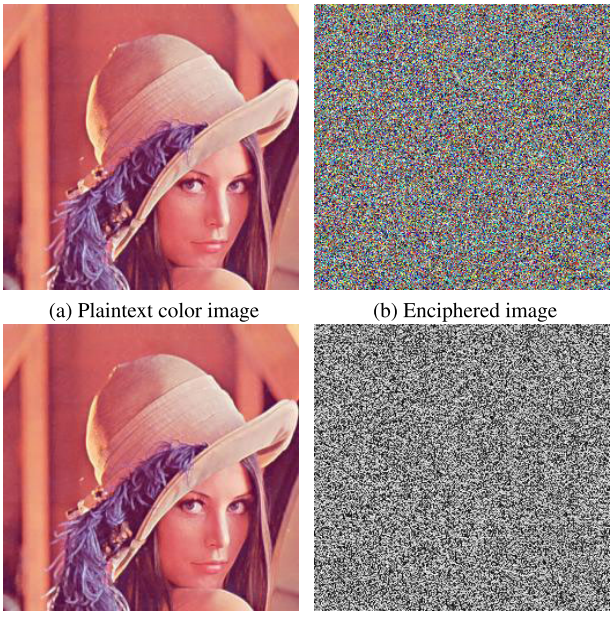
Key sensitivity shows that a minor change in the secrete keys result in the decryption failure [55]–[59]. There are four keys used in the proposed work and a little modification is made to evaluate sensitivity of such keys. The original keys used in the proposed algorithm are: $K_1 = 0.300000000000000$, K_2=0.400000000000000, K_3=3.7500000000000000 and $K_4 = 3.9000000000000000$), the modified keys are: K_1'=0.300000000000001, K_2' =0.400000000000001, K_3' = 3.7500000000000001 and K_4'=3.9000000000000001). Such modified keys are used in decryption and found that the decrypted image is completely different form the plaintext image as shown in Figure 6.

C. KEY-SPACE ANALYSIS

In brute force attack, the eavesdroppers try to use all the possible combinations of keys to decryp the plaintext image. To resist such attack, key-space must be large [60]–[69]. In [70], Alvarez presented a criteria that the key-space must be more than 2^{100} to hold out against the brute force attack. In the proposed encryption algorithm, the sensitivity of each key is 10^{-15}. Therefore the total key-space for all the keys used in the proposed work is 10^{15*4} which is approximately equal to 2^{250} which also satisfies Alvarez's criteria.

TABLE 3. Statistical security analysis of the proposed and existing encryption schemes.

Green-Component						
Plaintext images	**MSE**	**PSNR**	**Entropy**	**Correlation**	**Energy**	**Contrast**
Tree	258	15	7.9984	0.0013	0.0158	10.1588
Boat	251	13	7.9982	0.0.0002	0.0155	9.9879
Girl	255	16	7.9993	-0.0046	0.0158	9.9986
Sky	257	16	7.9999	-0.0013	0.0151	9.9891
Goat	255	17	7.9995	0.0003	0.015	10.6979
Butterfly	252	18	7.9994	-0.0065	0.0152	9.9985
Plant	257	18	7.9987	- 0.0005	0.0154	10.9749
House	256	15	7.9993	0.0002	0.155	9.2442
Clothes	258	16	7.9995	-0.0034	0.0158	10.6986
Lion	252	16	7.9997	-0.0086	0.0154	10.6872
Man	265	15	7.9982	0.0005	0.0151	10.7242
Sun	254	16	7.9985	-0.0002	0.0156	10.9783
Aeroplane	255	16	7.9992	0.0005	0.0152	10.7413
Bike	256	16	7.9990	0.0003	0.0154	9.9942
Lena	255	16	7.9992	-0.0013	0.0155	10.1346
Bottles	255	14	7.9982	0.0001	0.0155	9.9782
Forest	245	16	7.9992	-0.0034	0.0152	10.7343
Bridge	253	15	7.9990	0.0002	0.0156	9.9976
Pepper	256	16	7.9991	-0.0052	0.0156	10.7592
Cameraman	255	17	7.9996	0.00013	0.0155	9.9922
Baboon	2443	16	7.9991	0.0004	0.0154	10.7912
Existing schemes comparison						
[46]	247	19	7.9895	-0.0077	0.0153	9.8745
[44]	247	18	7.9972	- 0.0024	0.0159	10.0036
[43]	242	19	7.9994	0.0008	0.0154	9.3799
[42]	242	19	7.9941	-0.0064	0.0158	9.9912
[47]	228	19	7.9934	0.0015	0.0157	10.0356
[45]	233	20	7.9997	0.0007	0.0154	9.9896
[41]	245	18	7.9893	-0.00211	0.0158	9.6783
[49]	236	18	7.9992	-0.0022	0.0158	9.8721
[48]	249	21	7.9983	0.0002	0.0156	9.9342
[50]	244	22	7.9981	0.0008	0.0157	9.4612
[51]	244	19	7.9821	0.0082	0.0156	9.6461



(a) Plaintext color image (b) Enciphered image

(c) decryption without modified security keys (d) decryption with the modified security keys

FIGURE 6. Key sensitivity analysis.

D. COMPUTATIONAL TIME ANALYSIS

While designing the encryption scheme, two major factors must consider (a) strong security so it can resist cyberattacks and (b) it should be time-efficient for using real-time applications. The proposed work is implemented on MATLAB which is run on a computer having specifications 8GB RAM, Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz. The overall encryption time of the proposed work is calculated using a built-in MATLAB command known as tic toc. The encryption computational time of the proposed and the existing scheme are displayed in Table 4 in which it can be analyzed that the proposed work s slightly faster than the existing encryption schemes.

TABLE 4. Time analysis (sec).

Plaintext images	[71]	[72]	[73]	[74]	[75]	[76]	[77]	Proposed
Baboon	0.68132	0.0382	0.0345	0.0373	0.0631	0.0145	0.0317	0.0073
Camerman	0.0713	0.0374	0.0766	0.0988	0.0426	0.0542	0.0950	0.0064
Lenna	0.0215	0.3056	0.0735	0.0734	0.0734	0.0713	0.0716	0.0027

TABLE 5. Lossless analysis.

Plain images	**Proposed algorithm**		Ref [79]		Ref [78]	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Tree	0	∞	34.6350	23.8652	7.8551	69.7601
Cameraman	0	∞	6.2465	49.4701	6.8800	66.2168
Baboon	0	∞	21.6899	27.4986	5.2041	59.3236
Lena	0	∞	9.2486	49.0235	4.4034	61.0721
Building	0	∞	31.7312	24.7823	3.6999	71.9310

E. LOSSLESS ANALYSIS

Lossless analyses are frequently used to figure out the amount of information loss after decryption. For this purpose, MSE and PSNR can be under consideration. Such matrices can be calculated using Equations 9 and 10 respectively. The encryption schemes that cannot decrypt the exact pixel values of the original image are known as lossy encryption algorithms [78], [79]. However, the proposed encryption algorithm is lossless. To prove the proposed work is lossless, PSNR and MSE are calculated between the plaintext and decrypted image. In Table {loss, several PSNR and MSE values corresponding to different images are reported. Moreover, to show the superiority of the proposed wor over the existing encryption schemes, a comparison is also made. From the given values in Table 5, it can be seen that the proposed encryption scheme can decrypt the plaintext image without any loss of a single bit. While the compared schemes are lossy in nature because the values of PSNR and MSE are other than zero.

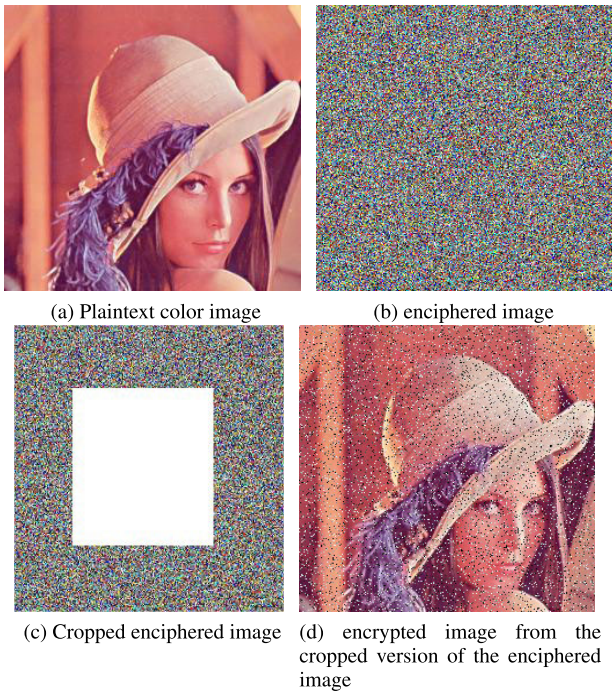
F. MEAN ABSOLUTE ERROR (MAE)

MAE is used to evaluate that whether the encryption algorithm can resist the differential attack or not. The MAE can be calculated between any two images. Whether two plaintext images, ciphertext images, or different images. In this case, MAE is calculated between the plaintext and ciphertext images (different images). Mathematically MAE can be written as:

$$MAE = \frac{1}{L \times K} \sum_{a=0}^{L-1} \sum_{b=0}^{K-1} |M_{a,b} - O_{a,b}| \qquad (17)$$

TABLE 6. MAE analysis.

Plaintext images	[81]	[82]	[83]	[84]	[85]	[86]	[87]	Proposed
Baboon	80	88	83	90	94	90	89	101
Camerman	84	83	89	79	91	90	87	99
Lenna	78	84	83	90	97	94	80	103
Tree	87	82	76	92	90	89	81	106
Building	88	79	91	94	86	89	77	99
House	87	81	91	93	94	97	88	100



(a) Plaintext color image (b) enciphered image

(c) Cropped enciphered image (d) encrypted image from the cropped version of the enciphered image

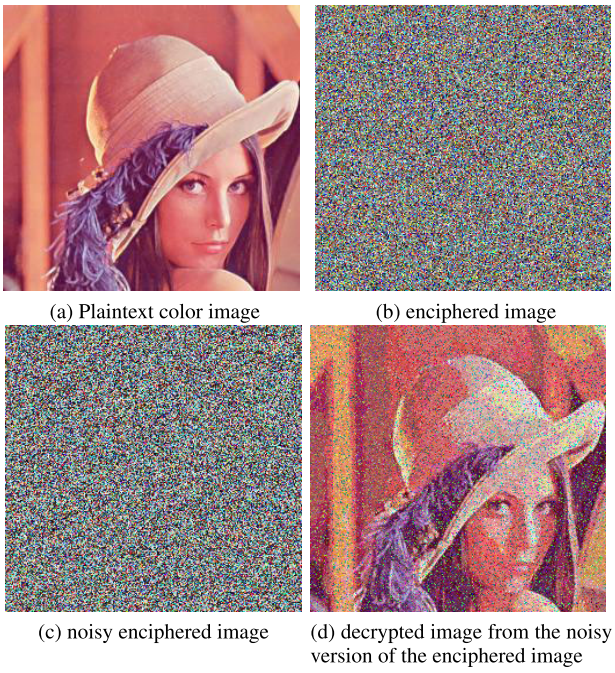
FIGURE 7. Cropping attack analysis.

where L and K are the rows and the columns of the plaintext or ciphertext image, M and O are the ciphertext and original image respectively.

The larger value of MAE refers to the strong security of the encryption algorithm. To resist the differential attack, the average value of MAE must be at least 75 [80]. Several values of MAE are displayed in Table 6 where it can be seen that the proposed encryption scheme shows the MAE value greater than 75 which satisfies the criteria of resisting the differential attack. Moreover, the compared schemes also show the MAE value greater than 75, but less than the proposed work. This means that the proposed encryption algorithm is more powerful than the existing schemes in terms of MAE analysis.

1) CROPPING ATTACK ANALYSIS

During the transmission of the data, the eavesdropper may fabricate the original information by cropping a certain portion. Therefore, to resist the cropping attack analysis, the encryption scheme must be able to decrypt the original image from the cropped version of the ciphertext image. In Figure 7(c), a cropped ciphertext image is displayed, while Figure 7(d) shows the decryption of the plaintext image which is recovered after cropping the ciphertext image. It can be seen from Figure 7(d) that the original image is recovered with little noise. Although there is some noise in the decrypted image, but the content of the plaintext and the decrypted image are the same.



(a) Plaintext color image (b) enciphered image

(c) noisy enciphered image (d) decrypted image from the noisy version of the enciphered image

FIGURE 8. Noise resistant analysis.

Moreover, the statistical analysis is also carried out in which the percentage of recovered information is calculated. Table 7 shows the several percentages of the recovered images from the corresponding cropped ciphertext images where it can be seen that the proposed encryption algorithm can recover more than 90% of the original information. Further, a comparison in Table 7 reveals that the proposed work is better than the existing ones in terms of recovering the information from the cropped ciphertext images.

G. NOISE RESISTANT ANALYSIS

The addition of noise is frequently used by the attackers to make the decryption failure. To resists the noise attack, the encryption scheme is designed in such a way that it can recover the original information from the fabricated ciphertext image. To gauge the performance of the proposed work in terms of noise resistance, random noise is added through the noisy image which is generated using algorithm 3.1. The noisy image is merged in the ciphertext image as follows:

$$\text{Noise}_{red} = \text{Enciphered image} \oplus \text{Noisy image}$$

The noise in the ciphertext image is controlled using the modulo operation which allows restricting the values in the range [0 30]. The recovered image from the noisy version of the ciphertext image is shown in Figure 8d in which the content of the plaintext image can be visualized. Moreover, the percentage loss of the information in the decrypted images

TABLE 7. Percentage of loss and recovered information from the attacked versions of ciphertext image.

Original images and the existing encryption schemes	Enciphered (Red, green and blue components)	Percentage of recovered information from the cropped enciphered image	Percentage loss of information after the addition of noise
Pepper	Enciphered red component	8.4973	98.3741
	Enciphered green component	7.9715	97.6983
	Enciphered bue component	9.9781	96.9365
Lenna	Enciphered red component	10.6978	96.9967
	Enciphered green component	9.8735	97.9866
	Enciphered blue component	6.8793	96.9977
Baboon	Enciphered red component	8.3671	97.6971
	Enciphered green component	9.8241	96.9982
	Enciphered red component	9.3791	97.6315
Ref [41]	Enciphered red component	9.7103	94.6980
	Enciphered green component	8.8036	95.6871
	Enciphered blue component	9.3708	96.4832
Ref [46]	Enciphered red component	9.3730	94.9961
	Enciphered green component	9.7013	94.6842
	Enciphered blue component	9.6301	98.6873
Ref [47]	Enciphered red component	9.7301	95.3121
	Enciphered green component	7.9324	94.3360
	Enciphered blue component	8.9350	95.6351

due to the addition of noise is reported in Table 7 in which it can be seen that a negligible part of the original information is lost.

V. CONCLUSION

In the proposed research, frequency and spatial domain encryption are incorporated using DWT and Chaotic map respectively. In the Spatial domain, random sequences are generated using the chaotic logistic map which is used to scramble the rows and the columns of the RGB components of the plaintext image. Whereas in the frequency domain, DWT is used to decompose the manipulated RGB components (scrambled components) into different frequency sub-bands. For the time reduction, only low-frequency sub-bands are considered, because a major portion of the original information lies in such frequency sub-bands. Moreover, for creating the diffusion in the original image, a noisy image is generated in which a chaotic map is integrated with the suitable initial conditions selected based on analysis of the chaotic logistic map. To evaluate the performance of the proposed work, several security analyses are performed which include entropy, contrast, correlation, noise-resistant and cropping attack. Further, a detailed comparison is also made which shows that the proposed research is better than the existing encryption algorithms.

CONFLICT OF INTEREST

- The authors declare no conflict of interest.

REFERENCES

[1] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 450–466, 2018.
[2] L. E. George, E. K. Hassan, S. G. Mohammed, and F. G. Mohammed, "Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key," *Iraqi J. Sci.*, pp. 920–935, Apr. 2020.
[3] L. Ding and Q. Ding, "A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyper-chaos," *Electronics*, vol. 9, no. 8, p. 1280, Aug. 2020.
[4] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," *IET Image Process.*, vol. 13, no. 9, pp. 1535–1539, 2019.
[5] H. Wang, J. Wang, Y.-C. Geng, Y. Song, and J.-Q. Liu, "Quantum image encryption based on iterative framework of frequency-spatial domain transforms," *Int. J. Theor. Phys.*, vol. 56, no. 10, pp. 3029–3049, 2017.
[6] S. Tedmori and N. Al-Najdawi, "Lossless image cryptography algorithm based on discrete cosine transform," *Int. Arab J. Inf. Technol.*, vol. 9, no. 5, pp. 471–478, 2012.
[7] Z. Liu, J. Dai, X. Sun, and S. Liu, "Triple image encryption scheme in fractional Fourier transform domains," *Opt. Commun.*, vol. 282, no. 4, pp. 518–522, Feb. 2009.
[8] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Opt. Commun.*, vol. 284, no. 1, pp. 123–128, 2011.
[9] 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.
[10] 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.
[11] H. Liu, A. Kadir, X. Sun, and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and S-boxes," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 1391–1407, Jan. 2018.
[12] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion," *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 4110–4127, 2011.
[13] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, 2018.
[14] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017.
[15] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[16] A. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Phys. D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638–2648, 2008.

[17] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "Chaos based image encryption scheme based on enhanced logistic map," in *Proc. Int. Conf. Distrib. Comput. Internet Technol.*, Springer, 2011, pp. 290–300.

[18] J. Ahmad, S. O. Hwang, and A. Ali, "An experimental comparison of chaotic and non-chaotic image encryption schemes," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 901–918, 2015.

[19] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010.

[20] N. F. Elabady, H. M. Abdalkader, M. I. Moussa, and S. F. Sabbeh, "Image encryption based on new one-dimensional chaotic map," in *Proc. Int. Conf. Eng. Technol. (ICET)*, Apr. 2014, pp. 1–6.

[21] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[22] S. Ansari, J. Ahmad, S. Aziz Shah, A. Kashif Bashir, T. Boutaleb, and S. Sinanovic, "Chaos-based privacy preserving vehicle safety protocol for 5G connected autonomous vehicle networks," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 5, 2020, Art. no. e03966.

[23] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic S-boxes based on Mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[24] A. Anees, "An image encryption scheme based on Lorenz system for low profile applications," *3D Res.*, vol. 6, no. 3, pp. 1–10, Sep. 2015.

[25] M. Safaei, A. S. Ismail, H. Chizari, M. Driss, W. Boulila, S. Asadi, and M. Safaei, "Standalone noise and anomaly detection in wireless sensor networks: A novel time-series and adaptive Bayesian-network-based approach," *Softw., Pract. Exper.*, vol. 50, no. 4, pp. 428–446, 2020.

[26] M. Safaei, S. Asadi, M. Driss, W. Boulila, A. Alsaeedi, H. Chizari, R. Abdullah, and M. Safaei, "A systematic literature review on outlier detection in wireless sensor networks," *Symmetry*, vol. 12, no. 3, p. 328, Feb. 2020.

[27] A.-U.-H. Qureshi, H. Larijani, J. Ahmad, and N. Mtetwa, "A novel random neural network based approach for intrusion detection systems," in *Proc. 10th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2018, pp. 50–55.

[28] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel substitution box for encryption based on Lorenz equations," in *Proc. Int. Conf. Circuits, Syst. Simul. (ICCSS)*, Jul. 2017, pp. 32–36.

[29] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, M. A. Khan, and S. O. Hwang, "A new technique for designing 8×8 substitution box for image encryption applications," in *Proc. 9th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2017, pp. 7–12.

[30] A. Anees and A. M. Siddiqui, "A technique for digital watermarking in combined spatial and transform domains using chaotic maps," in *Proc. 2nd Nat. Conf. Inf. Assurance (NCIA)*, Dec. 2013, pp. 119–124.

[31] A. Anees and Y.-P. P. Chen, "Discriminative binary feature learning and quantization in biometric key generation," *Pattern Recognit.*, vol. 77, pp. 289–305, May 2018.

[32] M. A. Gondal and A. Anees, "Analysis of optimized signal processing algorithms for smart antenna system," *Neural Comput. Appl.*, vol. 23, nos. 3–4, pp. 1083–1087, Sep. 2013.

[33] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, Jan. 2019.

[34] A. Anees and Y.-P. P. Chen, "Designing secure substitution boxes based on permutation of symmetric group," *Neural Comput. Appl.*, vol. 32, no. 11, pp. 7045–7056, 2020.

[35] I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, Mar. 2019.

[36] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, pp. 1–16, Aug. 2018.

[37] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, "Image encryption based on Chebyshev chaotic map and S8 S-boxes," *Optica Applicata*, vol. 49, no. 2, 2019.

[38] J. Ahmad, A. Tahir, J. S. Khan, A. Jameel, Q. H. Abbasi, and W. Buchanan, "A novel multi-chaos based compressive sensing encryption technique," in *Proc. Int. Conf. Adv. Emerg. Comput. Technol. (AECT)*, Feb. 2020, pp. 1–4.

[39] 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.

[40] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *Eur. Phys. J. Plus*, vol. 135, no. 2, pp. 1–13, Feb. 2020.

[41] Q. Liu, Y. Wang, J. Wang, and Q.-H. Wang, "Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain," *Opt. Rev.*, vol. 25, no. 1, pp. 46–55, 2018.

[42] C. Pak, K. An, and P. Jang, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019.

[43] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Process.*, vol. 172, Jul. 2020, Art. no. 107563.

[44] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106040.

[45] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.

[46] D. Zhang, X. Liao, B. Yang, and Y. Zhang, "A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2191–2208, Jan. 2018.

[47] A. Vaish and M. Kumar, "Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain," *Optik*, vol. 145, pp. 273–283, Sep. 2017.

[48] A. Broumandnia, "The 3D modular chaotic map to digital color image encryption," *Future Gener. Comput. Syst.*, vol. 99, pp. 489–499, Oct. 2019.

[49] Z. Xiong, Y. Wu, C. Ye, X. Zhang, and F. Xu, "Color image chaos encryption algorithm combining CRC and nine palace map," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 31035–31055, Nov. 2019.

[50] Y. P. K. Nkandeu and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 10013–10034, Apr. 2019.

[51] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Gener. Comput. Syst.*, vol. 107, pp. 333–350, Jun. 2020.

[52] F. Ahmed and A. Anees, "Hash-based authentication of digital images in noisy channels," in *Robust Image Authentication in the Presence of Noise*. Springer, 2015, pp. 1–42.

[53] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," *J. Integrative Neurosci.*, vol. 17, nos. 3–4, pp. 447–461, Sep. 2018.

[54] A. Anees, I. Hussain, A. H. AlKhaldi, and M. Aslam, "Linear triangular optimization technique and pricing scheme in residential energy management systems," *Results Phys.*, vol. 9, pp. 858–865, Jun. 2018.

[55] I. Hussain, A. Anees, T. Alassiry Al-Maadeed, and M. T. Mustafa, "A novel encryption algorithm using multiple semifield S-boxes based on permutation of symmetric group," 2020, *arXiv:2004.12264*.

[56] A. Anees and M. A. Gondal, "Construction of nonlinear component for block cipher based on one-dimensional chaotic map," *3D Res.*, vol. 6, no. 2, p. 17, Jun. 2015.

[57] I. Bashir, F. Ahmed, J. Ahmad, W. Boulila, and N. Alharbi, "A secure and robust image hashing scheme using Gaussian pyramids," *Entropy*, vol. 21, no. 11, p. 1132, Nov. 2019.

[58] W. Boulila, H. Ghandorh, M. Ahmed Khan, F. Ahmed, and J. Ahmad, "A novel CNN-LSTM-based approach to predict urban expansion," 2021, *arXiv:2103.01695*.

[59] A. Ferchichi, W. Boulila, and I. R. Farah, "Reducing uncertainties in land cover change models using sensitivity analysis," *Knowl. Inf. Syst.*, vol. 55, no. 3, pp. 719–740, Jun. 2018.

[60] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Secur. Commun. Netw.*, vol. 2018, pp. 1–20, Jun. 2018.

[61] I. Hussain, F. Ahmed, U. M. Khokhar, and A. Anees, "Applied cryptography and noise resistant data security," *Secur. Commun. Netw.*, vol. 2018, Dec. 2018, Art. no. 3962821.

[62] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021.

[63] T. A. Al-Maadeed, I. Hussain, A. Anees, and M. T. Mustafa, "A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes," *Multimedia Tools Appl.*, vol. 80, pp. 24801–24822, Apr. 2021.

[64] F. A. Khan, J. Ahmed, J. Ahmad, J. S. Khan, F. Ahmad, V. Stankovic, and H. Larijani, "A novel chaos-based partial image encryption scheme using lifting wavelet transform," in *Proc. 1st Int. Nonlinear Dyn. Conf.*, 2019.

[65] 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.
[66] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.
[67] Y. Hajjaji, W. Boulila, I. R. Farah, I. Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: A systematic review," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100318.
[68] B. Bai, S. Nazir, Y. Bai, and A. Anees, "Security and provenance for Internet of Health Things: A systematic literature review," *J. Softw., Evol. Process*, vol. 33, no. 5, p. e2335, 2021.
[69] A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," *Multidimensional Syst. Signal Process.*, vol. 32, no. 1, pp. 91–114, Jan. 2021.
[70] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
[71] M. A. Khan, J. Ahmad, Q. Javaid, and N. A. Saqib, "An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box," *J. Mod. Opt.*, vol. 64, no. 5, pp. 531–540, Mar. 2017.
[72] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Opt. Lasers Eng.*, vol. 110, pp. 24–32, Nov. 2018.
[73] X. Chai, X. Zheng, Z. Gan, and Y. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," *Neural Comput. Appl.*, vol. 32, no. 12, pp. 8065–8088, Jun. 2020.
[74] M. H. Annaby, M. A. Rushdi, and E. A. Nehary, "Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion," *Opt. Lasers Eng.*, vol. 103, pp. 9–23, Apr. 2018.
[75] X. Kang and R. Tao, "Color image encryption using pixel scrambling operator and reality-preserving MPFRHT," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 7, pp. 1919–1932, Jul. 2018.
[76] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and chaos," *Comput. Electr. Eng.*, vol. 62, pp. 401–413, Aug. 2017.
[77] N. Zhou, W. Chen, X. Yan, and Y. Wang, "Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system," *Quantum Inf. Process.*, vol. 17, no. 6, pp. 1–24, Jun. 2018.
[78] L. Zhang and X. Zhang, "Multiple-image encryption algorithm based on bit planes and chaos," *Multimedia Tools Appl.*, vol. 79, nos. 29–30, pp. 20753–20771, Aug. 2020.
[79] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19853–19873, Jul. 2020.
[80] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. S. Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," in *Cybersecurity and Secure Information Systems*. Springer, 2019, pp. 31–42.
[81] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019.
[82] T. Li, J. Shi, and D. Zhang, "Color image encryption based on joint permutation and diffusion," *J. Electron. Imag.*, vol. 30, no. 1, Feb. 2021, Art. no. 013008.
[83] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
[84] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process., Image Commun.*, vol. 80, Feb. 2020, Art. no. 115670.
[85] M. J. Aqel, Z. ALQadi, and A. A. Abdullah, "RGB color image encryption-decryption using image segmentation and matrix multiplication," *Int. J. Eng. Technol.*, vol. 7, no. 13, pp. 104–107, 2018.
[86] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.
[87] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019.

ARSLAN SHAFIQUE received the B.E. degree in mechatronics and electrical engineering from the Wah Engineering College, Pakistan, in 2014, and the M.S. degree in mechatronics and electrical engineering from Heavy Industries Taxila Education City (HITEC) University, Pakistan, in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan. He is also working as a Research Associate with the Faculty of Engineering and Applied Sciences, Riphah International University. He has more than ten journal publications with accumulative impact factor of 25+. His research interests include cryptography, secure communication, and machine learning.

MOHAMMAD MAZYAD HAZZAZI received the Ph.D. degree in mathematics from the University of Sussex, Brighton, U.K. He is currently working as an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests include coding theory, cryptography, finite geometry, algebraic geometry, and group theory.

ADEL R. ALHARBI received the Bachelor of Science degree in computer science from Qassim University, Saudi Arabia, in 2008, and the Master of Science degrees in security engineering and computer engineering and the Doctor of Philosophy degree in computer engineering from Southern Methodist University, Dallas, TX, USA, in 2013, 2015, and 2017, respectively. Since 2009, he has been a Faculty Staff Member at the College of Computing and Information Technology, University of Tabuk, Saudi Arabia. He acquired several academic certificates and published many scientific articles. His research interests include research involving mobile and smart device applications, biometric, security, networking, and machine learning techniques.

IQTADAR HUSSAIN received the Ph.D. degree in mathematics, specializing in the area of algebraic cryptography, in 2014. He is currently an Assistant Professor with Qatar University. His current research interests include the applications of mathematical concepts in the field of secure communication and cybersecurity, where he has published 63 articles in well-known journals. His H-index score is 23 and i-10 index score is 34. His articles have 1320 Google scholar citations.