IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 20, 2019, accepted October 30, 2019, date of publication November 6, 2019, date of current version November 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2951749

A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512

AQEEL UR REHMAN[1,2], HUIWEI WANG[3], MALIK M. ALI SHAHID[2], SALMAN IQBAL[2], ZAHID ABBAS[2], AND AMNAH FIRDOUS[4]

[1]College of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
[2]Department of Computer Science, COMSATS University Islamabad, Vehari Campus, Vehari 61100, Pakistan
[3]School of Computer Science and Engineering, South China University of Technology, Guangzhou 51006, China
[4]Department of Computer Science and IT, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan

Corresponding author: Aqeel Ur Rehman (rehmancqu@gmail.com)

This work was supported in part by the China Postdoctoral Science Foundation under Grant 2017M620374, and in part by the Fundamental Research Funds for the Central Universities under Grant XDJK2018B013.

ABSTRACT An innovative approach of selective encryption for color images is proposed that utilizes SHA-512 hash of plain image to modify initial conditions and control parameters of 1-Dimensional (1D) chaotic maps. The three channels (red, green and blue) of a color image are combined into 1D array and permute using sorted index of a pseudo-random sequence. The 1D permuted array is split into three sub-arrays, DNA encoding is applied on every pixel of each channel chaotically and then separate each DNA encoded channel into its Least Significant Bits (LSB) and Most Significant Bits (MSB). The substitution is carried out in two phases using addition and exclusive-or operations on MSB of each channel only. In 1^{st} phase, the DNA addition operation is applied on chaotically selected MSB of a pixel of one channel to LSB part of a pixel of other channel in a twisted fashioned named cross-substitution. The translated DNA bases from pseudo-random numbers are exclusive-or with cross substituted output to surge the complexity. The second substitution phase is accomplished by combining MSB part of a channel with randomly selecting LSB at pixel level. The novel algorithm is highly suitable for real time applications as it requires single round of permutation/substitution which can resist all possible statistical and differential attacks. The simulation results and analysis show that the proposed technique has the best quality output and highly efficient.

INDEX TERMS Chaos, color image encryption, DNA rules, cross substitution, selective, SHA-512.

I. INTRODUCTION

With modern times, communications technologies and methods are changing with an enormous pace, the momentum has seen advancements in computing, physical networks and software protocols. The big share of bandwidth across all mediums has now gone to multimedia communications; the users have come way forward from exchange of simple texts. It's the era of embedded media, real streams, live videos, 3D pictures and videos, virtual reality and lot more. The variety of forms a multimedia message can take is huge, so are the sources and applications using it. Along with it conventional theories and soft technologies are revolutionizing like vision tech, robotic eyes, pattern classifications, medical sensing and imaging, laser and ultraviolet imaging, 3D plans for remote video assistance, security camera and situation detections. These all demand a secure transmission of underlying image and video streams and messages. The internet being public and highly accessible in terms of network and applications is insecure by nature and any multimedia communication inherits this limitation. The researchers have seen the significance of the algorithms, encryption schemes, crypto systems that can solve this problem efficiently, systematically and without the loss of actual media. The images by nature contain high correlation and duplication of grayscale values in all neighboring groups of pixels, this makes the existing crypto schemes like IDEA, RS4 and IDEAS inefficient and inappropriate [1].

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

Theory of chaos mothered a new breed of encryption algorithms with its determinable but non-predictive characteristics [2]–[6]. The Chaos falling in type of nonlinear functions is highly sensitive to seeded values, initial conditions, ergodicity and randomization, hence highly suitable for the construction of a crypto system. Being the fundamental structure of an encryption algorithm chaos provides enhanced security, improved complexity, and better speed when compared with its non-chaotic rivals [7]–[16]. Liu and Wang [7] generated the initial conditions for chaotic maps from MD5 of the recorded mouse position and called One-time key system. Wang *et al.* [8] used neural network and Lorenz chaotic system called perceptron model for the image encryption. In 2011, Liu and Wang [9] proposed an image encryption technique based on the permutation of transformed binary matrix from color image at bit-level by piecewise linear chaotic map (PWLCM). In 2019, [17] parallel computing technique was used for encrypting images based on chaos. These features of chaos making it the choice of researchers and developers.

DNA was firstly brought by L.Adleman (1994) in encryption schemes to help to resolve computational complexity [18]. The DNA encoding was used to convert digital data into cipher and then revert it back [19]. The DNA sequence based algorithms have properties of parallelism and info density like DNA molecules [20]–[26]. The researchers have made a clear dent in improving existing cryptosystems in terms of their robustness to text-attacks by using DNA sequencing [21], [23], [27]–[30]. The DNA based schemes being new and less mature has seen cracking due to low dimensionality of chaotic maps causing periodicity [24], [32], [33]. According to Zhang et al. binary coded algos depict low efficiency on the other side chaotic controlled key is vulnerable to cracking [24]. Similarly, Xie et al suggests crypto schemes by only using scrambling, having no diffusion functions, are less secure causing disassociation of cipher with the plaintext [32]. Liu et al recreated the parallel key by using known partial values of plain or cipher and cracked a crypto scheme built upon DNA sequencing with the help of differential attack [33].

In the current decade, a number of selective encryption techniques for the multimedia data have been proposed [35]–[42]. But we have found few articles on selective encryption techniques on digital images using DNA method [40]–[42]. These selective techniques are proposed for the gray images only. The Cipher Block Chaining (CBC) method is used by author in Ref. [40] to encrypt the most significant bits (MSB) of an image. The pixels of an image are encoded into DNA bases by randomly selecting the DNA rules and then split into fixed size blocks. The MSB of each pixel is diffused by adding with LSB part. After encrypting one block, the secret keys are modified and LSB of the last pixel is used to perform the encryption of 1st pixel of 2nd block and so on. The diffusion process require two rounds to satisfy the process. Kulsoom *et al.* [41] proposed a system in which image is split into MSB and LSB part and then each part is encoded into DNA bases and then added to get encrypted MSB part. The diffused MSB part is combined sequentially to get the ciphered image [41]. The driving force to construct a newer algorithm by using DNA complementary rules with a bit-level confusion function is the formulation of a competitive crypto scheme which can be ranked higher at existing benchmarks.

In the proposed scheme, a new substitution mechanism is introduced called cross substitution for the color images. The substitution is performed on most significant bits (MSB) of each pixel of plain image under DNA addition and XOR operations. The core idea of the proposed cipher is 24-bit colored image is transformed into 1-dimensional array for pixel permutation then split into three sub-arrays; each representing a color channel. The DNA encoding is applied on each pixel by randomly selecting one of eight DNA complementary rules. Each pixel of the DNA encoded color channels is split into its LSB and MSB parts composed of two DNA bases. The cross substitution is applied between LSB part of a pixel with randomly selected MSB part of a pixel of different channel in cross fashion. The word "cross" is used to refer two concepts, one is that MSB part of a pixel of one channel is added to the LSB part of a pixel of other channel. The second concept is that DNA base of LSB part at 1st position is added to the DNA base of MSB part at the 2^{nd} position to substitute MSB part of a pixel at 1st position. In order to enforce the strong substitution, the translated DNA bases from pseudo random sequence are XORed with the MSB part to finalize the substitution. The initial conditions and control parameters of 1D chaotic maps are fabricated using SHA-512 of plain image to change the secret keys with a change in the plain image; without any intervention from the user. This modification benefits the system to hinder the common attacks. The prime advantage of this new modified scheme is that it is capable to decrypt into original image despite the accumulation of noise due to transmission channel.

The core achievement of the proposed method is in retrieving original text with a good readable quality from the noise polluted cipher. In this document section II contains literature review, sectionIII describes the proposed design, Section IV illustrates the achieved results, while robustness of the scheme is compared in section V. Lastly, section VI is for concluding the research.

II. BACKGROUND

A. NEW MODIFIED 1-DIMENSIONAL CHAOTIC MAPS

The most common used chaotic map in image cryptography is logistic map which can be represented with the Equation $x_{n+1} = \mu \times x_n \times (1 - x_n)$. The control parameter μ has range from [0-4] and $x_0$is the seed that has the range [0-1]. The logistic map is in chaotic mode when control parameter μ is in the range [3.57-4] which is very short. But once the logistic map enters in chaotic state for $\mu[3.57-4]$, but enters in stable region (non-chaotic area) for $3.85724 > \mu > 3.82843$ and the quantitative score of Lyapunov Exponent becomes negative. Another problem is the distribution of

TABLE 1. Eight kinds of DNA mapping rules.

1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

TABLE 2. XOR operation for DNA sequence.

XOR	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

TABLE 3. Addition and subtraction algebraic operation for DNA sequence.

+	A	G	C	T	-	A	G	C	T
A	A	G	C	T	A	A	T	C	G
G	G	C	T	A	G	G	A	T	C
C	C	T	A	G	C	C	G	A	T

pseudo-random numbers that are generated from Logistic map which do not possess the uniformity in the range of [0-1]. The poorly distributed pseudo-random numbers affect the permutation-substitution phases of image encryption which in turn affects the uniform distribution of the encrypted data [11]. C. Pak has devised new version of 1D chaotic maps to deal with such type of problems discussed above [11]. The Equation of new and improved 1D Logistic map is as follows,

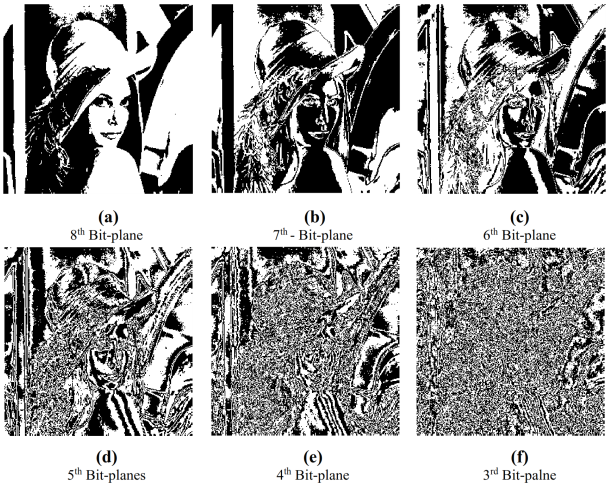
$$x_{n+1} = \mu \times x_n \times (1 - x_n) \times 2^k - floor\left((\mu \times x_n \times (1 - x_n)) \times 2^k\right) \quad (1)$$

In Equation (1), μ has range of [0-10] and k has the range [8-20]. The author proved that new version has better positive Lyaponuv Exponent value and has better distribution than the traditional Logistic map. The similar modifications applied to Chebyshev-Chebyshev system (CCS) as follows,

$$x_{n+1} = \cos\left((\mu + 1) \times \arccos(x_n)\right) \times 2^k - floor\left((\cos(\mu + 1) \times \arccos(x_n)) \times 2^k\right) \quad (2)$$

B. DNA COMPLEMENTARY RULES

The Deoxyribonucleic Acid is a material which forms the basic structure of the Gene for living creature. There are four nucleic acids, A (Adenine), C (Cytosine), G (Guanine) and T (Thymine) which works in pair to form the basic structure. The concept of biological structures can be used to encode and decode the pixels of a digital image. Each pixel consists of 8-bits and can be represented by four DNA bases in which each DNA base represents two bits either 00, 01, 10 or 11. There are four DNA bases, hence 4! = 24 kinds of encoding/decoding rules can exist. But only eight of them can be used in digital applications which meet the Watson-Crick complementary rules [43] are shown in Table 1. There are some operations like excluisve-OR, addition and subtraction that can be applied on DNA bases are displayed in Tables 2, and 3.


(a) 8th Bit-plane

(b) 7th - Bit-plane

(c) 6th Bit-plane

(d) 5th Bit-planes

(e) 4th Bit-plane

(f) 3rd Bit-palne

FIGURE 1. Amount of image information at different bit position.

III. PROPOSED SCHEME

The atomic unit of an image is called pixel that may have any score between [0-255] to represent a gray value. The individual pixel requires 8-bits to store its gray value and each bit has different weight corresponding to its location. The most significant bit at positions 8^{th} alone contribute 50% of an image information, 7^{th} bit contains 25%, 6^{th} contains 12.5% and so on. This concept is portrayed in Figure 1 in which 1(a) is for 8^{th} bit and 1(b) for 7^{th} bit. The bits at lower position has less information hence overall images in 1(d) to 1(f) loss its visual worth. This amount of image information at each bit can be computed using Equation (3) [40]. This provides us a clue that four most significant bits have 93.75% of information and are sufficient to achieve image encryption.

$$p(i) = 2^i / \sum_{i=0}^{7} 2^i \quad (3)$$

A. GENERATION OF INITIAL CONDITIONS

The work considers effective key generation process such that change in one bit of any of the secret key will spread the change on all of the secret keys used in the cryptographic algorithm. To fulfil the goal, initial seeds, provided by key strokes are added up under modulus 1 and a new initial key is calculated denoted by $'key'$. A hash function known SHA-512 is used to generate the initial conditions and control parameters of the proposed system. It is good to explain how to use 128-hexadecimal digits. The string of 512 bits is divide into eight blocks $h_1, h_2, \cdots, h_8$ and each block is transformed into decimal value of range 0 to 0.0625 by applying $h_i/2^{68}$;

$$\begin{gathered}\underbrace{b_1, \cdots, b_{64}}_{h_1}\underbrace{b_{65}, \cdots, b_{128}}_{h_2}\underbrace{b_{129}, \cdots, b_{192}}_{h3}\\ \underbrace{b_{193}, \cdots, b_{256}}_{h4}\underbrace{b_{257}, \cdots, b_{320}}_{h5}\underbrace{b_{321}, \cdots, b_{384}}_{h6}\\ \underbrace{b_{385}, \cdots, b_{448}}_{h7}\underbrace{b_{449}, \cdots, b_{512}}_{h8}\end{gathered} \quad (4)$$

At this stage, system requires the initial seeds as keyboard inputs from the user for 1D chaotic maps. These keys should belong to the interval [0-1] for symmetric encryption and denoted by μ_1, μ_2, μ_3, μ_4,w_0, x_0, y_0 and z_0. These keyboard inputs are added to form single key named *'key'*. The benefit of creating single key is that change in one initial condition or control parameter will affect all other keys which in turn will completely change the output (encrypted image). The single *'key'* is generated as follows:

$$key = \mu_1 + \mu_2 + \mu_3 + \mu_4 + w_0 + x_0 + y_0 + z_0 mod 1 \quad (5)$$

New initial values are calculated using *key* and the hash generated values by the following formulas,

$$\begin{cases} w'_0 = w_0 + key + h_1 \\ x'_0 = x_2 + key + h_2 \\ y'_0 = y_0 + key + h_3 \\ z'_0 = z_0 + key + h_4 \end{cases} mod 1 \quad (6)$$

$$\begin{cases} \mu'_1 = \mu_1 + key + h_5 \\ \mu'_2 = \mu_2 + key + h_6 \\ \mu'_3 = \mu_3 + key + h_7 \\ \mu'_4 = \mu_4 + key + h_8 \end{cases} mod 1 \quad (7)$$

The above Equations ensures the secret keys will be changed seamlessly on changing the input image without changing the common keys [40].

B. IMAGE ENCRYPTION ALGORITHM

The proposed encryption process is described in the following four sub-sections, which includes permutation, DNA encoding, cross substitution and DNA decoding. The inputs to the system are, 24-bit color image $P(M, N)$, common (μ_1, w_0), (μ_2, x_0), (μ_3, y_0) and (μ_4, z_0) keys along with value of k to be used for 1D chaotic maps called LSS and CSS. The output will be an encrypted colored image named E. Before going into the details of image encryption algorithm, 512-bits hash value from plain image P is computed to modify the initial conditions and the system parameters as described in the section III-A. The design of the proposed system is briefly depicted in Figure 2.

1) PERMUTATION

The correlation in the adjacent pixels of a channel and correlation between the channels of the color image are very strong in the plain image. The permutation is a method to reduce the correlation of an image. For this, a chaotic sequence W is generated by iterating Equation (2) $3MN + t$ times using μ'_1 and w'_0. The first t elements are discarded to avoid transient effect and then W is sorted and record their index as shown in Equation (8). A copy of W before sorting is maintained which will be used later. The 24-bit color image is transformed into 1D vector of size $1 \times 3MN$. The recorded index array f_w is used to shuffle the positions of pixels to permute the image P as shown below,

$$[l_w, f_w] = sort(W) \quad (8)$$

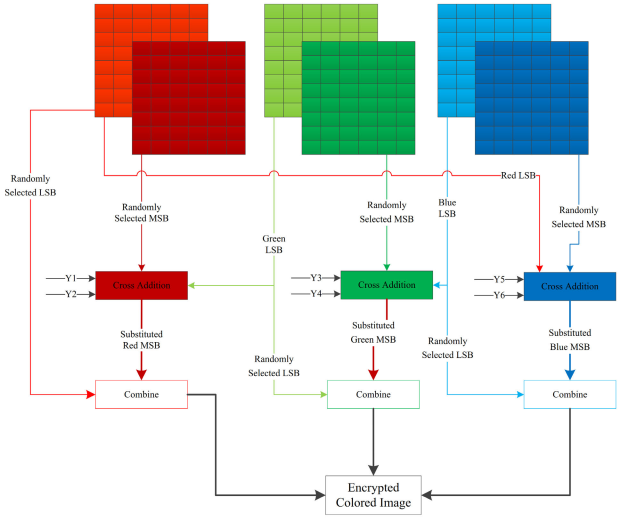


FIGURE 2. Theme of the proposed image encryption algorithm.

TABLE 4. Addition and subtraction algebraic operation for DNA sequence.

S#	Chaotic interval	Encoding	Decoding
1	0.01-0.05, 0.50-0.55,0.95-0.99	AGCT	CTAG
2	0.05-0.10, 0.45-0.50, 0.9-0.95	GTAC	TCGA
3	0.20-0.25, 0.35-0.40, 0.55-0.60	TGCA	ACGT
4	0.15-0.20, 0.25-0.30, 0.75-0.80	GATC	CATG
5	0.60-0.65, 0.30-0.35	CATG	GATC
6	0.70-0.75, 0.80-0.85	ACGT	TGCA
7	0.40-0.45, 0.65-0.70	TCGA	GTAC
8	0.10-0.15, 0.85-0.90	CTAG	AGCT

The Equation (8) depicts sequencing index functionality as $[\bullet, \bullet] = \text{sort}(\bullet)$, l_w is the generated sequence, where W is sorted in ascending. The f_w holds index value of l_w to rearrange the items of P depicted by Equation (9).

$$P' = P[f_w] \quad (9)$$

2) DNA ENCODING

Now split P into three vectors, each of size $1 \times MN$ representing a color channel called R, G and B. These permuted channels are encoded into DNA bases using DNA complementary rules according to Table 4. This operation requires three pseudo-random sequences for the selection of DNA rules, which are obtained by splitting copy of W into three sub-arrays called W_1, W_2 and W_3.

$$\begin{aligned} R' &= Encode(R, W_1) \\ G' &= Encode(G, W_2) \\ B' &= Encode(B, W_3) \end{aligned} \quad (10)$$

3) CROSS SUBSTITUTION

For selective cross substitution, the image should be split into LSB and MSB parts. So, encoded R', G' and B' are separated into its LSB and MSB part as follows,

$$\begin{aligned} \left[R'_M(i), R'_L(i)\right] &= R'(i) \\ \left[G'_M(i), G'_L(i)\right] &= G'(i) \\ \left[B'_M(i), B'_L(i)\right] &= B'(i) \end{aligned} \quad (11)$$

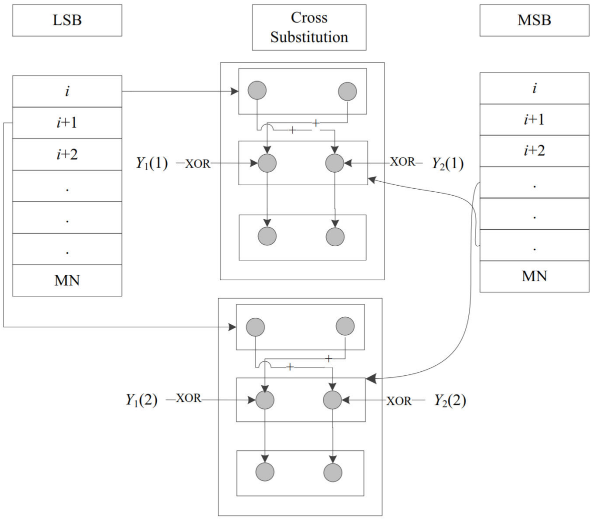


FIGURE 3. Theme of the proposed image encryption algorithm.

In the above Equation (11), $i = 1, 2, \cdots, MN$ and $R'(i)$ represent a pixel of red channel whereas $R'_M(i)$, $R'_L(i)$, are MSB and LSB parts of $R'(i)$. Each MSB and LSB slice consists of two DNA bases and same for other channels. The substitution process requires three pseudo-random sequences of size $1 \times MN$, so LLS is iterated $3MN$ times using modified seeds μ'_2 and x'_0 to get X. The X is split into three sub-vectors called X_1, X_2 and X_3 for the random selection of MSB part of each channel. These chaotic sequences are sorted to generate index value as follow;

$$\begin{aligned}[lx_1, fx_1] &= Sort(X_1)\\ [lx_2, fx_2] &= Sort(X_2)\\ [lx_3, fx_3] &= Sort(X_3)\end{aligned} \tag{12}$$

Here,lx_1 is the new sequence after x_1 sorting in ascending order;fx_1 is the index value of lx_1. In the similar fashion, fx_2 and fx_3 are obtained. Each slice of a pixel in R'_M is composed of two DNA bases. The cross addition of these two portions of a pixel is as follows,

$$\begin{aligned}MSB &= R'_M\left(fx_1(i)\right)\\ R''_M(i,1) &= \left(G'_L(i,1) + MSB(1,2)\right) \oplus Y_1(i)\\ R''_M(i,2) &= \left(G'_L(i,2) + MSB(1,1)\right) \oplus Y_2(i)\end{aligned} \tag{13}$$

where $i = 1, 2, \cdots, MN$ in the above Equation. The process of cross addition is shown in Figure 3. In the above Equation (13), Y_1 and Y_2 are DNA bases, which are produced from Y pseudo random sequence. This Y is generated by iterating Equation (2) or CSS map up to $1 \times 6MN$ times using μ'_3 and y'_0. Before utilizing in substitution process, Y is processed as shown in Equation (14),

$$Y(i) = round\left(Y(i) \times 10^{14}\right) \bmod 4 \tag{14}$$

Now split Y into six sub-vectors each having size of $1 \times MN$ called Y_1, Y_2, Y_3, Y_4, Y_5 and Y_6. These sub-vectors are translated into DNA bases as 0 = A, 1 = G, 2 = C and 3 = T and Exclusive-ORed with the DNA bases in the substitution. The Equation (13) will be applied on G'_M, B'_L, B'_M,and R'_L using fx_2, fx_3, Y_3, Y_4, Y_5 and Y_6 to obtain G''_M and B''_M. The LSB and MSB parts of a channel are concatenated/combined in random way that need a pseudo-random vector of $1 \times MN$. For this, Z pseudo-random vector of size $1 \times 3MN$ is produced by iterating Equation (2) with μ'_0 and z'_0. The Z is split into three sub-vectors having same size of $1 \times MN$ called Z_1, Z_2 and Z_3 and sort as follows;

$$\begin{aligned}[lz_2, fz_1] &= Sort(Z_1)\\ [lz_2, fz_2] &= Sort(Z_2)\\ [lz_3, fz_3] &= Sort(Z_3)\end{aligned} \tag{15}$$

Apply the following on of R''_M, and R'_L, B''_M and B'_L, C''_M and C'_L as follows,

$$\begin{aligned}\bar{R}(i) &= Cat\left[R''_M(i), R'_L\left(fz_1(i)\right)\right]\\ \bar{G}(i) &= Cat\left[G''_M(i), G'_L\left(fz_2(i)\right)\right]\\ \bar{B}(i) &= Cat\left[B''_M(i), B'_L\left(fz_3(i)\right)\right]\end{aligned} \tag{16}$$

4) DNA DECODING

Decode each pixel of $\bar{R}$, $\bar{G}$ and $\bar{B}$ using the same chaotic sequences which are X_1, X_2 and X_3 used for decoding according to intervals in Table 4. The decoding process is shown in Equation (17) and then combine all channels to get RGB cipher image in Equation (18).

$$\begin{aligned}\hat{R} &= Decode\left(\bar{R}, X_1\right)\\ \hat{G} &= Decode\left(\bar{G}, X_2\right)\\ \hat{B} &= Decode\left(\bar{B}, X_3\right)\end{aligned} \tag{17}$$

$$E = cat(3, \hat{R}, \hat{G}, \hat{B}) \tag{18}$$

C. STEPS IN ALGORITHM

Inputs: A 24-bit color image $P(M; N)$ and common keys(μ_1, w_0), (μ_2, x_0), (μ_3, y_0) and (μ_4, z_0) along with value of k to be used for 1D chaotic maps called LSS and CSS.
Output: Encrypted colored image

1) Hash function with 512 bits of output called SHA-512 is applied on original image P to alter the initial conditions as seen in Section III-A.
2) Generate four chaotic sequences W, X, Y and Z through Equation (1) using the modified initial conditions and control parameters.
3) Transform 24-bit color image into 1D vector of size $1 \times 3MN$ and sorted index of pseudo-random sequence W; is used to permute image P using Equations (8) and (9).
4) The permuted image P' is split into three vectors, called R, G and B, then encoded every pixel of each channel into DNA bases using DNA complementary rules according to Table 4. The whole process is presented in Equation (10) by employing three chaotic maps W_1, W_2 and W_3.

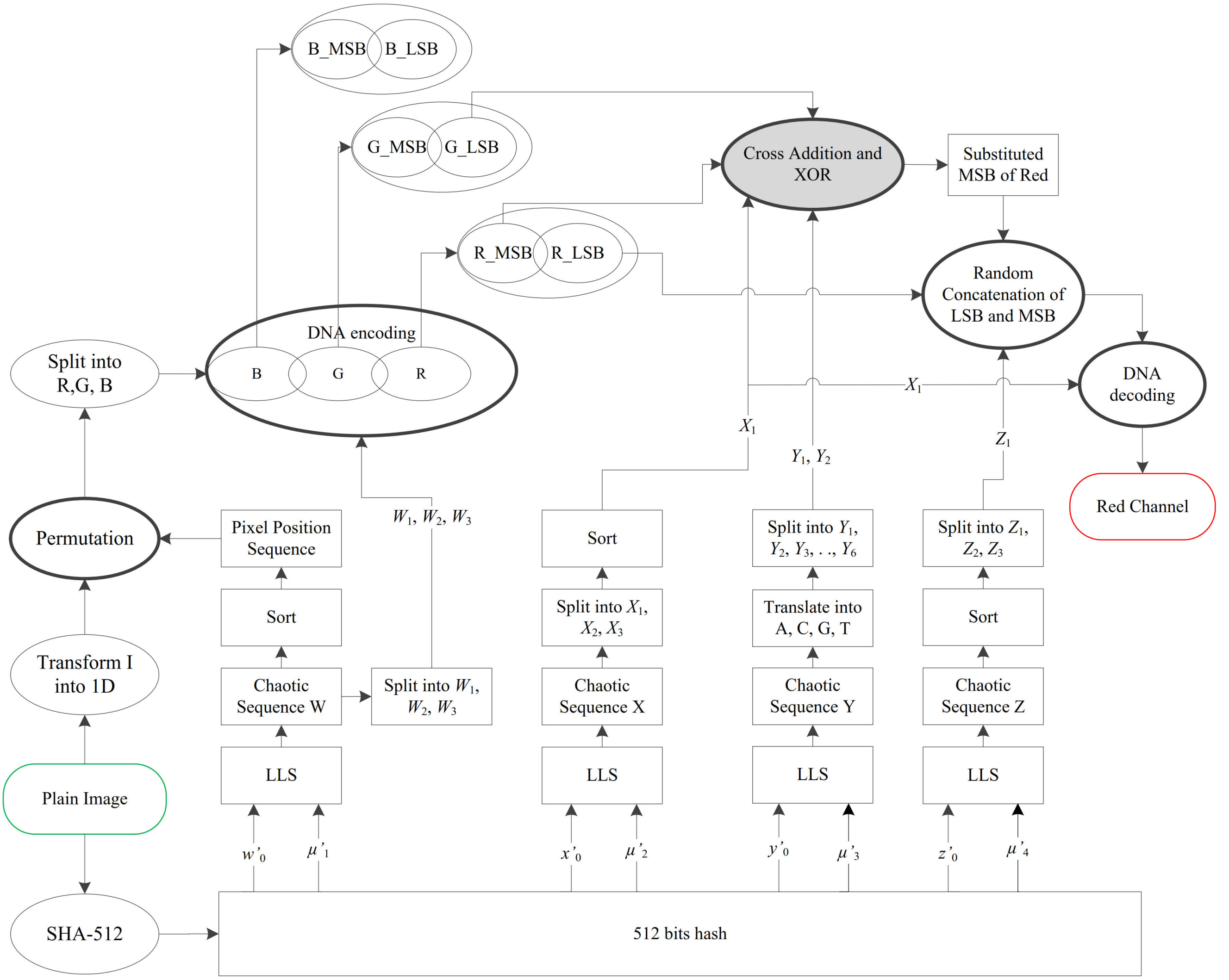


FIGURE 4. Theme of the proposed image encryption algorithm.

5) Separate LSB and MSB parts of DNA encoded R',G' and B'channels of an image illustrated in Equation (11).
6) For substitution, LLS is iterated $3MN$ times using μ'_2 and x'_0 to get X and split into X_1, X_2 and X_3 for the random selection of MSB part of each pixel for R, G and B. The cross substitution is applied on each channel independently using Equation (14) in which Y_i is an array of DNA bases that translated from pseudo-random sequence according to Table 4.
7) The LSB and MSB parts of a channel are concatenated/combined using Z pseudo-random vector. The Z is split into three sub-vectors Z_1, Z_2 and Z_3 that are sorted to record their indexes. These sorted indexes are used to select LSB part of a pixel of a channel to combine sequentially with MSB part shown in Equation (16).
8) Decode each pixel of $\bar{R}$, $\bar{G}$ and $\bar{B}$ using the chaotic sequences X_1, X_2 and X_3 according to intervals in Table 4. The complete process is shown in Equation (17) and then combine all channels to get RGB cipher image as in Equation (18). The complete framework of the proposed algorithm is shown in Figure 4.

D. DECRYPTION PROCESS

The decryption procedure is straightforward. First of all, split cipher image E into three channels ER, EG and EB then encoding each pixel chaotically of every channel into DNA bases by employing chaotic sequences $X1$, $X2$ and $X3$ according to Table 4. After this, split each encoded channels into its MSB and LSB parts using Z_1, Z_2 and Z_3. For the cross substitution process, pseudo random sequence Y is translated into DNA bases and divide into six sub vectors. The cross substitution in the decryption process will be as shown in Equation (19). Similar process will be applied on EG_M, EB_L, and EB_M, ER_L to get back the plaintext of green and blue MSB. The last steps are to combine MSB and LSB of each channel, decode DNA bases into decimal values and then

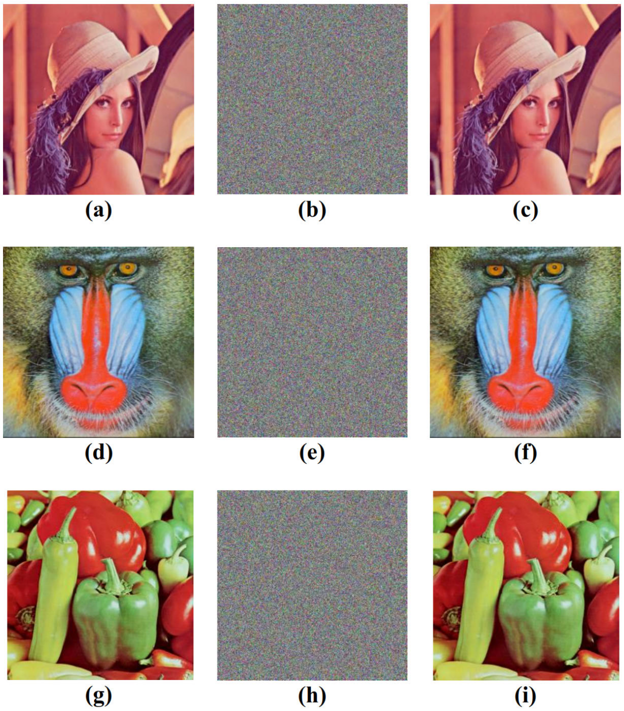


FIGURE 5. Encrypted and decrypted images. (a) Original Lena image. (b) Encrypted Lena image. (c) Decrypted Lena image. (d) Original Baboon image. (e) Encrypted Baboon image. (f) Decrypted Baboon image. (g) Original Pickle image. (h) Encrypted Pickle image. (i) Decrypted Pickle image.

invert the permutation process using W chaotic sequence.

$$\begin{aligned} MSB &= ER_M(i) \\ R'_M\,(fx_1(i),1) &= (MSB(1,2) \oplus Y_2(i)) - EG_L(i,2) \\ R'_M\,(fx_1(i),2) &= (MSB(1,1) \oplus Y_1(i)) - EG_L(i,1) \end{aligned} \tag{19}$$

IV. EXPERIMENTS AND RESULTS

This section contains multi-perspective results for the proposed scheme. The proposed scheme employs SHA-512 hash-value functions for the production of seeds. This hash function has become de-facto standard for the chaotic map based encryption schemes to make ciphers highly sensitive for the plaintext. The results are produced by using multi-resolution images to check the validation. The color channels have gone through linear transformation and set of primitive initial seeds are $\mu_1 = 9.84098765432101$, $\mu_2 = 8.85123456789011$, $\mu_3 = 7.75123409876541$, $\mu_4 = 2.64098765712341$, $w_0 = 0.01234567890123$, $x_0 = 0.99876543210983$, $y_0 = 0.45678902630000$ and $z_0 = 0.12345609330000$, common parameter $k_1 = 14$, $k_2 = 15$, $k_3 = 16$ and $k_4 = 14$ for the generation of four pseudorandom sequences through 1D chaotic maps. The Figure 5 contains the encrypted and decrypted images of Lena, Baboon and Pepper.

A. KEY SPACE ANALYSIS

The chaotic system structure is highly sensitive to initial conditions. A crypto scheme is graded high quality if having sufficient computational complexity with an extreme sensitivity to change in the secret key. Such cryptosystems are hard to crack by the simplest attacks. In the proposed work, 1D chaotic map is used which requires two inputs; μ_0 and x_0 simultaneously but encryption algorithm requires eight pseudo-random sequences so we have used four pairs of secret keys with floating precision of 10^{-14}. The key space is also comprised of 512 bits of the hash function so the total key space is 10^{254} and comparison is provided in Table 5.

TABLE 5. Comparison of key space.

Algorithm	Key space
Proposed	10^{254}
Ref. [26]	10^{192}
Ref. [28]	10^{94}
Ref. [29]	10^{161}
Ref. [30]	10^{70}
Ref. [36]	2^{128}
Ref. [40]	2^{209}
Ref. [41]	$10^{50.27}$
Ref. [44]	2^{138}

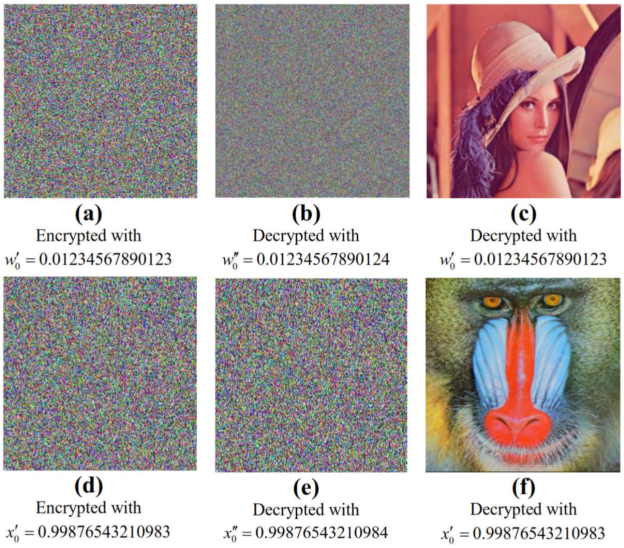
B. KEY SENSITIVITY AND DIFFERENTIAL ANALYSIS

There are two most important test metrics for image ciphers to validate its robustness called key sensitivity and plaintext sensitivity/differential analysis. The first metric is the measure of how much is the difference in two outputs of an algorithm when slightly different keys are employed and second is used to measure the difference in outputs when the input text/image is modified by 1-bit. In Figure 6, encrypted images of Lena and Baboon are displayed using secret keys $w_0 = 0.01234567890123$ and $x_0 = 0.99876543210983$. The decryption of Figure 6(a) and Figure 6(d) fail when done with modified secret keys $w''_0 = w'_0 + 10^{-14}$ and $x''_0 = x'_0 + 10^{-14}$ shown in Figure 6(b) and 6(e). The plain images which is shown in Figure 6(c) and Figure 6(f) are regenerated when applied same secret keys that were used in encryption process. Hence, the proposed system is highly sensitive to any minute change in the secret keys.

The secret keys discussed in section III-A are presented as a set of secret key called $\gamma_0 = [\mu'_1, \mu'_2, \mu'_3, \mu'_4, w'_0, x'_0, y'_0, z'_0]$. The key set γ_1 came into existence on changing one of the secret key in the set γ_0 by one bit. In the similar way, eight different keys sets $[\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6, \gamma_7, \gamma_8]$ can be formed beside γ_0. These key sets are used to test the robustness of key sensitivity for encrypting the plain images and decrypting the ciphered images. In this regard, the plain image Lena shown in Figure 5(a) is used. The statistical results for key sensitivity are measured using Net Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). These two tests metrics are proposed by Biham and Shamir [45] and it's mathematical representation are displayed in Equations (20) to (22). The statistical score close to 100% for NPCR and 33% for UACI are considered to be effective as it proves that system is robust for minute change in the secret keys and also to differential attacks. Now, there are different ways to test the effect of secret key

TABLE 6. Difference of two encrypted images using different key sets for Lena (256 × 256).

Key Set	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	Fig. 5(a)
γ_0	0	-	-	-	-	-	-	-	99.6317
γ_1	99.5920	0	-	-	-	-	-	-	99.6073
γ_2	99.6017	99.6307	-	-	-	-	-	-	99.6190
γ_3	99.6119	99.6012	99.5855	0	-	-	-	-	99.6338
γ_4	99.6170	99.6083	99.6134	99.6129	0	-	-	-	99.6002
γ_5	99.6088	99.6358	99.6124	99.1080	99.6078	0	-	-	99.6154
γ_6	99.6216	99.6394	99.5860	99.6175	99.6145	99.6195	0	-	99.6083
γ_7	99.6053	99.6018	99.6033	99.6175	99.6496	99.5880	99.5965	0	99.6001
γ_8	99.6073	99.6022	99.6109	99.6018	99.6190	99.5946	99.6277	99.6129	99.5692
Average	99.6082	99.6171	99.6019	99.5115	99.6227	99.6007	99.6121	99.6129	99.6094


(a) Encrypted with $w_0' = 0.01234567890123$

(b) Decrypted with $w_0'' = 0.01234567890124$

(c) Decrypted with $w_0' = 0.01234567890123$

(d) Encrypted with $x_0' = 0.99876543210983$

(e) Decrypted with $x_0'' = 0.99876543210984$

(f) Decrypted with $x_0' = 0.99876543210983$

FIGURE 6. Decrypted results with right and wrong key sequences.

changes on the output of the cryptographic algorithm for encryption and decryption. The adopted methods of testing the key sensitivity used in this paper are graphically shown in Figure 7(a) to 7(c).

$$N(E^1, E^2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{D(i,j)}{M \times N} \times 100\% \tag{20}$$

$$U(E^1, E^2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left|C^1(i,j) - C^2(i,j)\right|}{L \cdot M \times N} 100\% \tag{21}$$

where $M \times N$ represents the dimension of input/output images, $E_1(i,j)$ and $E_2(i,j)$ are the pixel values in the ith row and the jth column of two evaluated images and $D(i,j)$ is defined as follows,

$$D(i,j) = \begin{cases} 0. & if\, E^1(i,j) = E^2(i,j) \\ 1, & if\, E^1(i,j) \neq E^2(i,j). \end{cases} \tag{22}$$

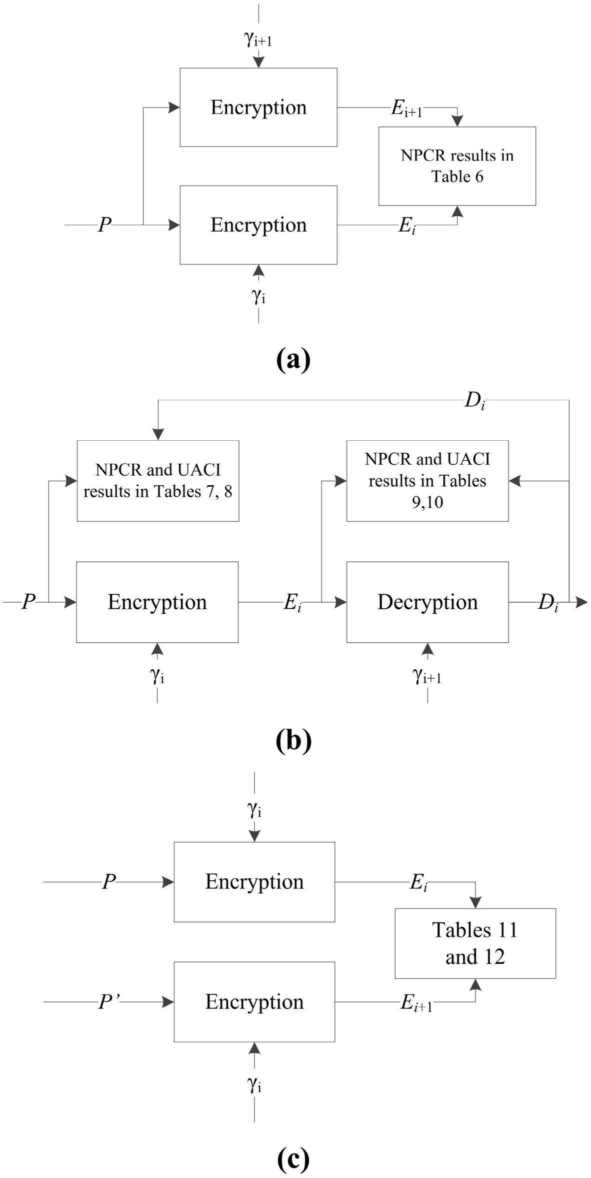


FIGURE 7. Diagram to represent the methods used to compute the results in Tables 6, 7, 8, 9, 10, 11 and 12.

The Figure 7(a) exhibited the first method to measure the key sensitivity in which ciphered image E_i is obtained using plain image P and key set in encryption process and then again P is encrypted using a different key set to get E_{i+1}. The NPCR score is computed for (E_i, E_{i+1}) for all key sets shown in Table 6. The NPCR score will be "0" or zero when encryption and decryption key sets are same. The result in the last column of Table 6 is the NPCR score between encrypted and plain image (E_i, P). Most important aspect of

TABLE 7. Difference of two encrypted images using different keysets for Lena (256 × 256).

Key Sets	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
γ_0	**0**	99.5834	99.6089	99.6267	99.6144	99.6022	99.6134	99.6221	99.6038
γ_1	99.5925	**0**	99.6109	99.5859	99.6089	99.6119	99.5987	99.6170	99.6084
γ_2	99.6160	99.6266	**0**	99.5956	99.6063	99.6211	99.6134	99.6205	99.6033
γ_3	99.6231	99.6012	99.5925	**0**	99.6246	99.2047	99.6032	99.5987	99.6160
γ_4	99.6251	99.6266	99.5900	99.6043	**0**	99.6246	99.6104	99.6012	99.6140
γ_5	99.6149	99.6109	99.6058	99.1072	99.6465	**0**	99.6195	99.5981	99.6139
γ_6	99.6053	99.6089	99.6042	99.6358	99.6205	99.5992	**0**	99.6206	99.5997
γ_7	99.5946	99.6180	99.6287	99.6032	99.6093	99.6078	99.6115	**0**	99.6053
γ_8	99.5982	99.6088	99.6099	99.6195	99.6124	99.6114	99.6089	99.5961	**0**
Average	99.6087	99.6105	99.6064	99.5473	99.6179	99.5604	99.6099	99.6093	99.6080

TABLE 8. UACI of encrypted and decrypted image with different key sets for Lena (256 × 256).

Key Set	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	Fig. 5(a)
γ_0	0	30.2960	30.4464	30.3334	30.3536	30.3703	30.3180	30.3568	30.4372
γ_1	30.3652	0	30.4464	30.3414	30.1839	30.3213	30.3588	30.3323	30.3162
γ_2	30.3709	30.3390	0	30.1345	30.3321	30.3730	30.3163	30.3247	30.3374
γ_3	30.3940	30.3557	30.3214	0	30.3791	30.3509	30.2938	30.3149	30.3615
γ_4	30.3417	30.2802	30.3465	30.3457	0	30.3183	30.3191	30.3674	30.4541
γ_5	30.3856	30.4281	30.3777	30.4866	30.3424	0	30.4926	30.3687	30.3973
γ_6	30.3418	30.4223	30.3955	30.3722	30.3539	30.3867	0	30.3341	30.3305
γ_7	30.3128	30.3513	30.4187	30.3642	30.4395	30.3255	30.4642	0	30.4119
γ_8	30.3508	30.3217	30.4104	30.3605	30.3425	30.3158	30.4151	30.3958	0
Average	30.3578	30.3493	30.3954	30.3423	30.3409	30.3452	30.3722	30.3493	30.3808

TABLE 9. UACI of encrypted and decrypted image with different key sets for Lena (256 × 256).

Key Set	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	Fig. 5(a)
γ_0	**99.6042**	99.6139	99.6032	99.5854	99.5900	99.5991	99.6160	99.6048	99.5946
γ_1	99.6033	**99.6007**	99.6170	99.5961	99.6124	99.6083	99.6088	99.5997	99.6338
γ_2	99.6292	99.6164	**99.6042**	99.6268	99.6485	99.6207	99.5824	99.6073	99.6261
γ_3	99.5951	99.5905	99.6134	**99.6154**	99.6078	99.6206	99.6017	99.5976	99.6409
γ_4	99.6068	99.5966	99.5910	99.6017	**99.5956**	99.6204	99.6063	99.6368	99.5743
γ_5	99.6129	99.6022	99.6480	99.6150	99.6200	**99.6104**	99.6256	99.6119	99.5870
γ_6	99.6398	99.6338	99.6032	99.6073	99.6078	99.5997	**99.5941**	99.6150	99.6058
γ_7	99.6266	99.5930	99.5885	99.6119	99.6225	99.6017	99.6064	**99.6206**	99.6369
γ_8	99.6185	99.5982	99.6180	99.5824	99.6120	99.6383	99.5855	99.5925	**99.6327**
Avg. with BF	99.6152	99.6050	99.6097	99.6047	99.6130	99.6132	99.6030	99.6096	99.6147
Average	99.6165	99.6056	99.6103	99.6033	99.6151	99.6136	99.6041	99.6082	99.6124

the proposed system is robustness for minute change in any of the secret key which is evident for 100% NPCR score in Table 6. The lowest NPCR score is for key set γ_3 which is 99.5115% and highest score is for γ_4 that is 99.6227%.

The Figure 7(b) displayed the mechanism that is used to test the key sensitivity for decryption process. If the wrong key set is used to decrypt the image, the output must be entirely different from the plain image as well as different from the encrypted image. The E_i is the resultant image of encrypting P using key set γ_i and then the E_i is decrypted with a different key set γ_{i+1}. The output of decryption process D_i is used to measure NPCR(P, D_i), NPCR(E_i, D_i), UACI(P, D_i) and UACI(E_i, D_i) for all key sets. The scores are assembled in Tables 6, 7, 8 and 9. NPCR scores are close to 100% and UACI are close 33% which in turn proves that proposed system fail to recover the plain image by using slightly modified secret key. The key sets on the first row of Tables 7, 8, 9, and 10 are used to generate E_i. The key sets in first column are used to produce D_i. The boldface scores at diagonal locations of Table 7 and 8 are zero (0) because the encryption and decryption are performed on the same secret key set so D_i is same as P. The highest NPCR and the lowest UACI scores in Tables 7 and 8 are produced by key set γ_4, 99.6179% and 30.3409% respectively while the lowest NPCR score 99.5473% and highest UACI score 30.3954% are produced by key sets γ_3 and γ_2, respectively.

The Tables 9 and 10 represents the statistical results of NPCR(E_i, D_i), UACI(E_i, D_i) in which E_i is produced by γ_i in encryption process and D_i is produced after the decryption process with key set γ_{i+1}. The D_i becomes P when same key set is used in decryption process hence the boldface scores at diagonal locations are between (E_i, P). Therefore, the average results are measured with and without boldface values are shown in Tables 9 and 10.

The statistical results of plaintext sensitivity shown in Tables 11 and 12 are measured according to the method shown in Figure 7(c) in which one-bit is different in input (Plain image P and P') are used while keeping the same

TABLE 10. UACI of encrypted and decrypted image with different key sets for Lena (256 × 256).

Key Set	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	Fig. 5(a)
γ_0	**30.3412**	33.5612	33.4099	33.4339	33.4762	33.4199	33.4619	33.4203	33.5259
γ_1	33.4994	**30.4038**	33.4719	33.4264	33.2708	33.4698	33.4853	33.4169	33.4877
γ_2	33.4867	33.3870	**30.3470**	33.3852	33.4465	33.4885	33.4527	33.5004	33.4531
γ_3	33.4975	33.4028	33.6579	**30.3381**	33.4010	33.5220	33.4413	33.3439	33.5719
γ_4	33.4600	33.3104	33.4031	33.4986	**30.3821**	33.4156	33.4382	33.5400	33.4974
γ_5	33.4639	33.5348	33.3672	33.4530	33.4139	**30.3877**	33.4802	33.4931	33.4568
γ_6	33.3913	33.4764	33.3920	33.5047	33.4735	33.4598	**30.3629**	33.5339	33.4931
γ_7	33.4816	33.4709	33.4393	33.5023	33.4121	33.3684	33.4876	**30.4302**	33.5838
γ_8	33.4315	33.4890	33.4699	33.4534	33.3509	33.3965	33.4589	33.5323	**30.4474**
Avg with BF	33.1170	33.1151	33.1065	33.1106	33.0697	33.1031	33.1188	33.1346	33.1686
Average	33.4640	33.4541	33.4514	33.4572	33.4056	33.4426	33.4633	33.4726	33.5087

TABLE 11. Comparison of differential attack for plaintext sensitivity: NPCR (512 × 512).

Image	Channel	proposed	Ref. [26]	Ref. [30]	Ref. [29]	Ref. [28]	Ref. [6]	Ref. [41]	Ref. [40]
Lena	Red Green Blue	99.5983 99.6429 99.6261	99.6586 99.5409 99.6697	99.3218 99.2945 99.3027	99.6551 99.5909 99.6301	99.6001 99.5998 99.5997	99.6139	99.61	99.6089
Baboon	Red Green Blue	99.6078 99.6025 99.6281	99.7350 99.5940 99.6541	99.1689 99.2749 99.2321	99.6109 99.6414 99.6155	99.6099 99.6058 99.5956	—-	99.5758	99.6178
Avgerage	-	**99.6176**	**99.6420**	**97.5991**	**99.6240**	**99.6108**	**99.6139**	**99.5929**	**99.6133**

TABLE 12. Comparison of differential attack for plaintext sensitivity: UACI (512 × 512).

Image	Channel	proposed	Ref. [26]	Ref. [30]	Ref. [29]	Ref. [28]	Ref. [6]	Ref. [40]	Ref. [41]
Lena	Red Green Blue	33.4310 33.4833 33.3970	33.1154 33.9966 33.8975	31.2189 31.4183 31.3621	33.4927 33.5522 33.5292	33.3575 33.4287 33.3683	32.6602	33.4671	33.4600
Baboon	Red Green Blue	33.4429 33.4587 33.5892	33.3521 33.6231 33.9012	31.3478 31.2473 31.2956	33.5852 33.4235 33.5400	33.3743 33.3829 33.5604	—-	33.4499	33.4017
Avgerage	-	**33.4670**	**33.6476**	**31.3150**	**33.5205**	**33.4120**	**32.6602**	**33.4585**	**33.4308**

key sets. The results are compiled for each color channel of images Lena and Baboon with standard size (512 × 512). The average NPCR score of proposed system is better than [6], [28], [30] and comparable to [29]. The average UACI score of proposed algorithm is better [6], [28] and that of [30].

C. STATISTICAL ANALYSIS

In this section, different statistical aspects of the algorithm are tested.

1) HISTOGRAM ANALYSIS

The histogram of plain/encrypted image provides the statistical information through which one can measure the robustness of encryption algorithm against the statistical analysis. In reality, histogram describes the distribution of gray values of an image, bumpy distribution can reveal the loop holes exist in the algorithm which can be used by attacker to launch chosen-ciphertext attack through statistical analysis. Therefore, it's necessary to make the distribution of histogram uniform for a good cryptography. The Figure 8 shows the color histograms of plain and ciphered images and one can observe visually that distribution of the pixels in the ciphered images are quite uniform for all channels but plain image has some peaks.

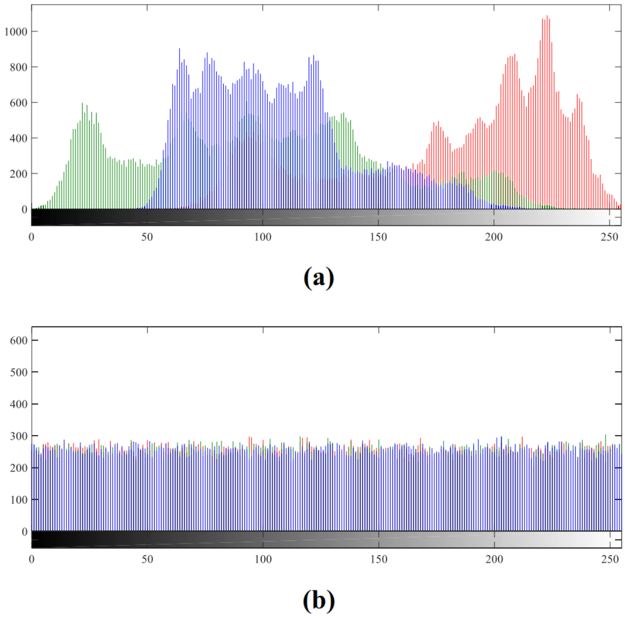


FIGURE 8. Combined histograms of R, G and B channels of Lena. (a) Histogram of Plain Lena. (b) Histogram of encrypted Lena.

Histogram variance is used for the quantification of encrypted image, this further leads to key analysis as well. If the amount of variance is low the stronger the uniformity in the encrypted image. Two encrypted images are generated using distinct secret keys but with the same input image. If the

TABLE 13. Variances of histograms compared among all secret keys in the proposed algorithm.

Technique	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9
Lena	5451.124	5454.776	5457.531	5469.989	5446.493	5461.263	5451.427	5456.848	5464.319	-
BARB	5468.817	5455.559	5447.197	5467.908	5461.089	5465.959	5461.074	5463.018	5475.472	-
Avg.	**5459.971**	**5455.167**	**5452.364**	**5468.948**	**5453.791**	**5463.611**	**5456.251**	**5459.933**	**5459.971**	-
Ref. [28]	5434.707	5438.051	5439.770	5460.511	5439.295	5437.264	5445.300	5443.725	5443.691	2727.896
Ref. [29]	5458.921	5454.342	2735.435	2731.396	2734.463	2732.050	2740.564	-	-	-
Ref. [46]	5174.858	5200.905	5126.327	5398.865	5256.426	5261.749	-	-	-	-
Ref. [41]	5465.259	5481.524	5466.723	5438.669	-	-	-	-	-	-

TABLE 14. Percentage of variances difference of histograms compared among all secret keys in the proposed algorithm.

Technique	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9
Lena	0.07	0.11	0.34	0.08	0.18	0.005	0.10	0.24	-
Barbara	0.242	0.395	0.016	0.141	0.052	0.141	0.106	0.121	-
Avg.	0.156	**0.252**	0.178	0.110	0.116	0.073	**0.103**	0.180	-
Ref. [28]	0.346	0.283	0.495	0.496	0.158	0.523	0.451	0.419	0.411
Ref. [29]	0.426	0.428	0.157	0.202	0.143	0.104	-	-	-
Ref. [46]	9.495	1.44	4.465	1.59	2.5	-	-	-	-
Ref. [41]	0.281	0.330	0.407	-	-	-	-	-	-

TABLE 15. Correlation coefficient analysis in all directions of Lena and Baboon.

Technique	Channel	Lena			Baboon		
		H	V	D	H	V	D
Proposed	Red	-0.0034	0.0012	-0.0030	-0.0222	-0.0213	-0.0105
	Green	-0.0046	0.0003	0.0033	-0.0018	-0.0006	-0.0318
	Blue	0.0023	-0.0017	-0.0017	-0.0113	-0.0037	-0.0260
Ref. [26]	Red	0.0144	0.0083	-0.0468	0.0186	-0.0064	-0.0013
	Green	0.0163	-0.0180	0.0427	0.0066	0.0164	0.0092
	Blue	-0.0838	0.0127	0.0783	0.0067	0.0012	0.0171
Ref. [30]	Red	0.0356	0.0127	0.0783	-	-	-
	Green	0.0763	0.0067	0.0562	-	-	-
	Blue	0.0012	0.0098	0.0058	-		- -
Ref. [29]	Red	-0.0047	0.0028	-0.0043	0.0193	0.0250	-0.0067
	Green	-0.0023	-0.0060	-0.0069	0.0098	-0.0116	0.0337
	Blue	-0.0038	-0.0057	-0.0112	0.0312	0.0082	-0.0042
Ref. [28]	Red	-0.0073	0.0010	-0.0013	-0.0001	0.0055	0.0076
	Green	0.0011	-0.0020	0.0078	0.0263	-0.0167	0.0154
	Blue	-0.0061	0.0058	-0.0003	0.0002	0.0133	0.0427
Ref. [40]	Gray	-0.0007	0.0006	-0.0031	0.0096	0.0043	0.0143
Ref. [41]	Gray	0.0027	0.0005	0.0045	0.0124	0.0295	-0.0320

variances are close enough, this exhibits the better uniformity of encrypted images. Histogram variances are shown below:

$$Var(Z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}(z_i - z_j) \tag{23}$$

In Equation (23), Z denotes the vector from histogram and $Z = \{z_1, \cdots, Z_{256}\}$ contains count of the pixels. In this set grayscale values are mapped to z_i and z_j correspondingly. To hold the experiment, an input image is taken and encrypted using different secret keys. Histogram variances are calculated with the help of Equation (23) for both decrypted sets. All secret key sets γ_i are different by one parameter only. For testing one iteration of encryption is performed on Lena and Barbara. The variances of all key sets are shown in Table 13. The variance values in Column-1 are computed with standard key set γ_0 and column-2 have variance values are computed with one parameter change in the secret key set. The maximum variance value found is 622571.4908 for Lena. This variance value is the highest among all the encrypted images as shown in Table 13. In Table 14, percentages of difference of variances for the proposed system are computed and the minimum and maximum values are 0.103 and 0.252. This percentage of difference in histogram are far better than that of Refs. [28]–[41]. This also proves the efficiency of the proposed scheme.

2) CORRELATION COEFFICIENT

The correlation coefficient of the two adjacent pixels provided the information of randomness which is a parameter to compute the the robustness of a cipher and can be calculated by using Equation (24). It is computed within a cipher and plain image in horizontal, diagonal and vertical directions by arbitrary selection of adjacent pixels. The range for the coefficient score is between −1 to +1, lower the coefficient score for encrypted image, higher is the quality of cipher to resist the statistical attack. The random selection of 3000 pairs of pixels in all three directions are made and the coefficient scores for Lena and baboon images (512 × 512) are given in Table 15. The results are close to zero hence proposed encryption scheme shows no information leakage. The same

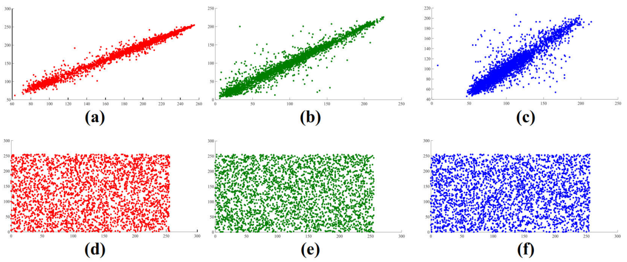


FIGURE 9. Correlation analysis of Lena image. (a) - (c) Correlation in Horizontal (Red), Diagonal (Blue) and Vertical (Green) directions of Plain image. (d)-(e) Correlation in Horizontal (Red), Diagonal (Blue) and Vertical (Green) directions of ciphered image.

concept is graphically represented in Figure 9(a) to 9(c) for original image and Figure 9(d) to 9(f) for the cipher image.

$$r = \frac{n\left(\sum_{i=1}^{n} x_i y_i\right) - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right)}{\sqrt{\left[n\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)^2\right]\left[n\left(\sum_{i=1}^{n} y_i^2\right) - \left(\sum_{i=1}^{n} y_i\right)^2\right]}} \tag{24}$$

where $n(\sum_{i=1}^{n} x_i y_i) - (\sum_{i=1}^{n} x_i)(\sum_{i=1}^{n} y_i)$ represents sample variation, $\left[n(\sum_{i=1}^{n} x_i^2) - (\sum_{i=1}^{n} x_i)^2\right]$ and $\left[n(\sum_{i=1}^{n} y_i^2) - (\sum_{i=1}^{n} y_i)^2\right]$ are the sample standard variation of X_j and Y_j.

The next step is to measure the normal distribution of correlation coefficients for ciphered image that whether a cipher follows a normal distribution or not. The correlation coefficients for Lena image are computed by randomly selecting 3000 pairs in each of three directions and this process is repeated for 300 times. The histogram of 300 values of correlation coefficient in three direction for colored channels are displayed in Figure 10(a) to 10(i). In Figure 11(a) to 11(c), the frequency of correlation coefficients scores for Horizontal, Vertical and Diagonal of each channel are combined. The Figure 12(a) to 12(c) are the frequency plot of [28]. The histograms plot clearly show that ciphered image follow normal distribution for correlation coefficients scores. To verify this, single sample K-S test is applied. The result of a test is either accepted or rejected based on some hypothesis,

H0: Correlation coefficients of the encrypted image obey normal distribution.

H1: Correlation coefficients of the encrypted image don't obey normal distribution.

$$D = \max |F_{n2}(x) - F_0(x)| \tag{25}$$

The mean $\hat{\mu}$ and $\hat{\sigma}^2$ standard deviation are computed in order to obtain $F_0(x)$ which are parameters of normal distribution in **H0**. The Equations $\hat{\mu}$ and $\hat{\sigma}^2$ are $\hat{\mu} = \frac{1}{n_2}\sum_{i=1}^{n_2} xi = \bar{x}$ and $\hat{\sigma}^2 = \frac{1}{n_2}\sum_{i=1}^{n_2}(x_i - \bar{x})^2$. In Equation (25), $F_{n2}(x) = F/n^2$, F represents cumulative frequency, and $n2$ represents sample size. When $D > D(n_2, \alpha)$ ($\alpha = 0.05$ is the significance level), reject **H0**. Otherwise, accept **H0**.

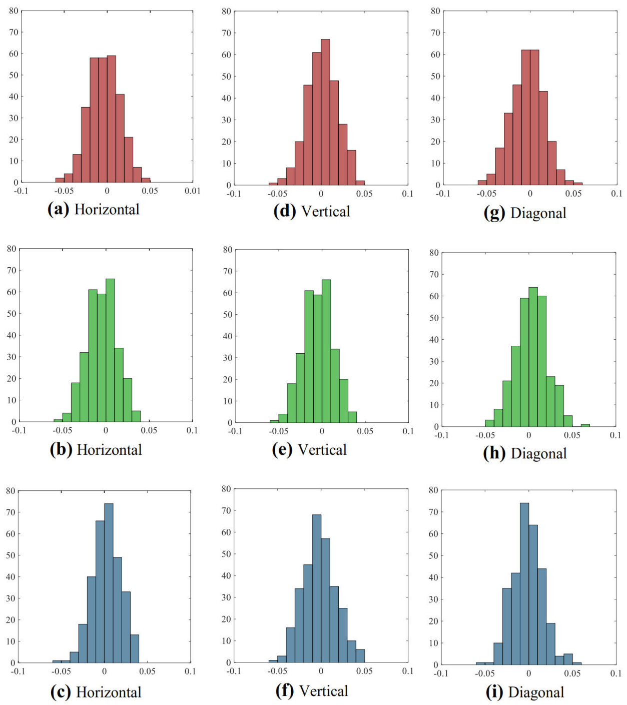


FIGURE 10. Histograms of correlations in three directions for red, green and blue.

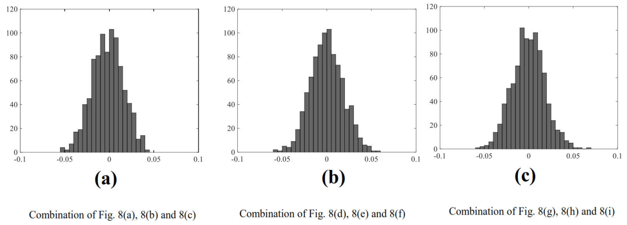


FIGURE 11. Combination of histograms for Red, Green and Blue channels from Figure 10.

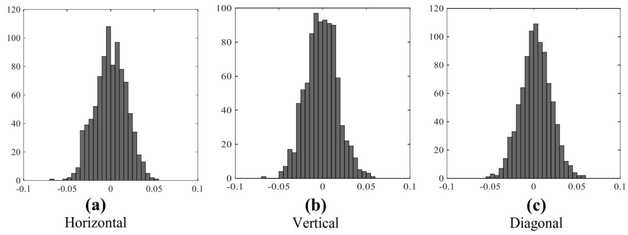


FIGURE 12. Histograms of correlation coefficient for red, green and blue channels of Lena image in three directions using [28].

The Matlab 2018b is used for K-S test, the results are demonstrated in Table 16 for R, G and B channels. The progressive significant for the proposed method is 0.9887 and the minimum value is 0.7593 shorter range than that of Ref. [6] which is 0.6251 and maximum is 0.9645. The K-S test proved that the proposed system has better correlation coefficient distribution than that of [6], [28], [29].

The correlation not only exists in the neighboring pixels of a channel; it also exists between the channels of a colored

TABLE 16. One-sample K-S test for correlation coefficient of encrypted image.

Image	Horizontal			Verical			Diagonal		
	$\hat{\mu}$	$\hat{\sigma}^2$	Sign. (Two-Sides)	$\hat{\mu}$	$\hat{\sigma}^2$	Sign. (Two-Sides)	$\hat{\mu}$	$\hat{\sigma}^2$	Sign. (Two-Sides)
Proposed (R)	-0.0034	0.0181	0.9177	0.0012	0.0178	0.8687	-0.0030	0.0187	0.9848
Proposed (G)	-0.0046	0.0173	0.8682	0.0003	0.0179	0.9894	0.0033	0.0184	0.9259
Proposed (B)	0.0023	0.0166	0.9904	-0.0017	0.0190	0.9058	-0.0017	0.0174	0.9740
Proposed (Avg.)	-0.0019	0.0176	0.7593	-0.00006	0.0183	0.8506	-0.0004	0.0184	0.9887
Ref. [6]	0.0015	0.0432	0.6850	0.0021	0.0658	0.7870	0.0043	0.0913	0.7540
Ref. [29]	0.0024	0.0174	0.6125	0.0030	0.0177	0.8717	-0.0027	0.0177	0.5183
Ref. [28]	-0.0002	0.0181	0.6792	-0.0011	0.0181	0.7555	0.0026	0.0174	0.9872

TABLE 17. Intra-channel correlation of Lena and Baboon.

	Lena			Baboon		
	Red-Green	Red-Blue	Green-Blue	Red-Green	Red-Blue	Green-Blue
Correlation	0.0013	0.0024	-0.0020	-0.0051	-0.0030	0.0036
NPCR	99.5865	99.5895	99.6262	99.5972	99.6337	99.5956
UACI	33.3800	33.3459	33.4992	33.5132	33.5340	33.3847

TABLE 18. Correlation of NPCR and UACI of two images shown in Figure 13(b) and 13(e).

	Lena			Baboon		
	Red-Red	Green-Green	Blue-Blue	Red-Green	Red-Blue	Green-Blue
Correlation	0.0033	-0.0011 -0.0043	0.0040	0.0017	-0.0067	
NPCR	99.4390	99.5092	99.4711	99.4924	99.4268	99.4619
UACI	33.4764	33.5977	33.5947	33.5152	33.5936	33.5687

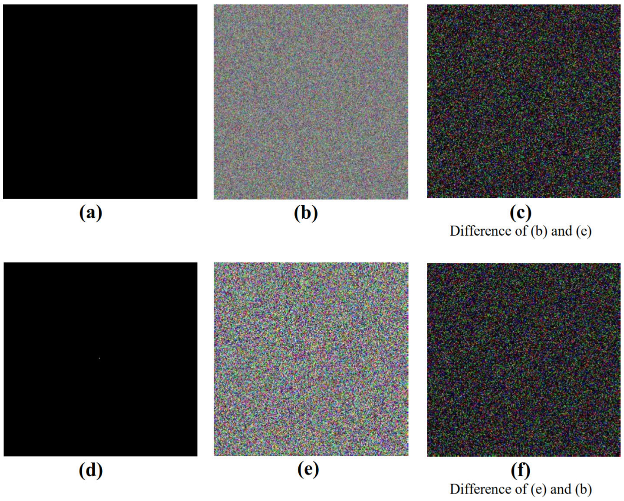

(a) (b) (c) Difference of (b) and (e)
(d) (e) (f) Difference of (e) and (b)

FIGURE 13. Encryption results for black image.

image or intra-channel correlation. The cryptographic algorithm should be designed in such a way that it can also breaks the intra-channel correlation for encrypted color images. The intra-channel correlation of encrypted images of Lena and Baboon are computed in Table 17 as well as NPCR and UACI are also listed. In the next move, the image having zero information displayed in Figure 13(a) is encrypted and shown in Figure 13(b). The Figure 13(d) is same as Figure 13(a) except one pixel having gray value 255 and the encrypted output is shown in Figure 13(e). The differences of 13(b) and 13(e), 13(e) and 13(b) are computed and results are displayed in Figure 10(c) and 10(f). The NPCR, UACI and correlation of10(b) and 10(e) are listed in Table 18 which clearly indicates that proposed system is sensitive for minute change in plaintext.

D. INFORMATION ENTROPY ANALYSIS

Information entropy is the measure of how arbitrary distribution have plaintext or multimedia files and can be computed by Equation given as follows [47],

$$H(s) = \sum_{i=0}^{L-1} p(s_i) log_2 \frac{1}{p(s_i)} \tag{26}$$

In the Equation (26), $p(s_i)$ is the ith gray value, s_i is the probability of ith gray value. The arbitrary distribution of message s_i must be as high as close to 8 for 8-bit channel of color image [48]. The cipher is robust against statistical attack as the message m_i has the highest value that is close to 8. The entropy values for three colored pieces of an image are provided in Table 19 and those are compared to some known ciphers.

$$H_{k,T_B}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{27}$$

The (k, T)-local Shannon entropy [49] is utilized to measure the local randomness of the images. The plain I and encrypted image E with L intensities are divided into non-overlapped k blocks where $E_1, \cdots, E_k$ with every blocks has T number of pixels. We have randomly selected K number of blocks and used Equation (27) to compute the mean of local entropy of k blocks. In the simulation, $K = 32$ and $T = 1936$ are used. As seen from Table 20, the average local Shannon entropy values of R, G, B components of the cipher image

TABLE 19. Comparison of information entropy.

Image	Lena			Baboon		
	Red	Green	Blue	Red	Green	Blue
Proposed	7.9993	7.9992	7.9994	7.9993	7.9992	7.9993
Ref. [26]	7.9962	7.9993	7.9995	7.9968	7.9964	7.9960
Ref. [30]	7.9928	7.9912	7.9932	7.9945	7.9920	7.9932
Ref. [29]	7.9973	7.9965	7.9969	7.9962	7.9965	7.9972
Ref. [28]	7.9966	7.9972	7.9967	7.9967	7.9970	7.9969
Ref. [6]		7.8679		-	-	-
Ref. [40] Gray		7.9991			7.9992	
Ref. [41]Gray		7.9990				

TABLE 20. Comparison of local information entropy.

Image	Plain Image			Ciphered Image		
	Red	Green	Blue	Red	Green	Blue
Lena	6.4268	6.8551	6.4169	7.9033	7.9024	7.9043
Baboon	7.1419	7.1165	7.1466	7.9040	7.9031	7.9045
Tiffany	3.6051	3.7965	5.7340	7.8930	7.8993	7.8987
Splash	5.5898	5.6437	5.0970	7.9031	7.9005	7.9025
Pepper	6.8790	6.7956	6.5000	7.9010	7.9018	7.9011
Avg.	5.9285	6.0415	6.1789	7.9009	7.9010	7.9018
Ref. [29]	6.0212	6.5238	6.2479	7.8941	7.8942	7.8945
Ref. [28]	6.0212	6.5238	6.2479	7.8526	7.8529	7.8541

TABLE 21. Comparison of speed performance of 8-bit gray level images for different sizes(s).

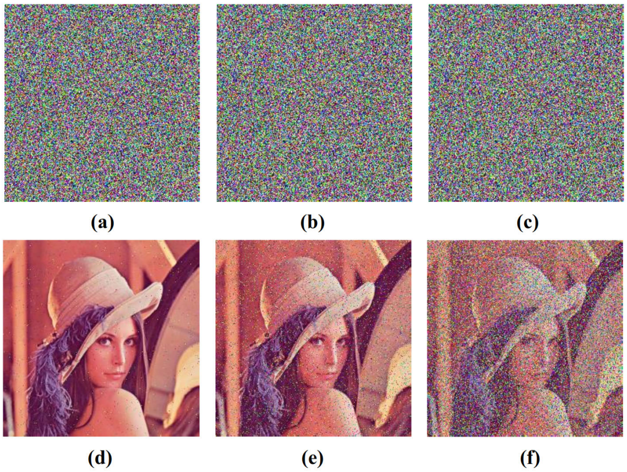
Image$M \times N$	Proposed	Ref. [29]	Ref. [28]	Ref. [40]	Ref. [30]	Ref. [6]	Ref. [41]	Ref. [36]
64 × 64	0.09	0.207	1.65	0.19	-	-	0.057	2.1
128 × 128	0.42	0.791	3.94	0.29	-	-	0.159	-
256 × 256	1.26	3.70	12.17	6.01	5.35	0.76	0.601	-
512 × 512	5.47	12.89	50.03	35.59	-	-	2.142	85.56

TABLE 22. Comparison of noise robustness for Salt & Pepper noise (PSNR *(dB)*).

Noise	Proposed	Ref. [29]	Ref. [28]	Ref. [55]	Ref. [41]
0.005	30.11	31.02	30.87	30.50	32.59
0.05	20.33	20.92	20.77	20.73	22.12
0.5	10.45	10.98	10.79	10.75	12.26

TABLE 23. PSNR between plain and decrypted image under different clipping size (PSNR *(dB)*).

Clipping	Proposed	Ref. [29]	Ref. [28]	Ref. [52]	Ref. [41]
1/16	18.84	20.73	20.57	37.63	21.12
1/8	16.48	17.70	17.57	34.58	18.20
1/4	12.89	14.72	14.59	32.22	15.17


(a) (b) (c)

(d) (e) (f)

FIGURE 14. Noise Robustness against Salt & Pepper noise.

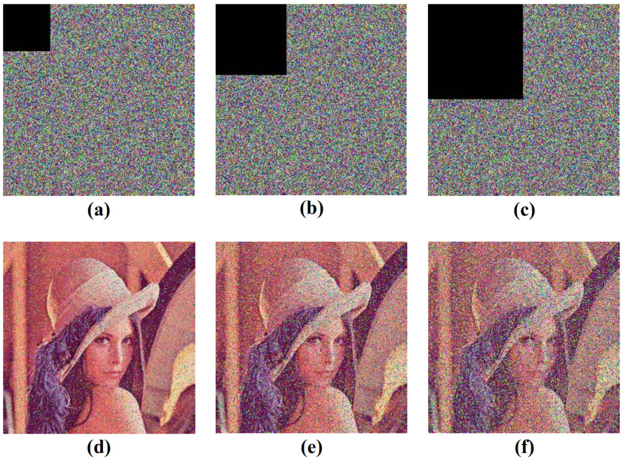
are more than 7.90, whereas those of the plain image are less than 6, which means that the cipher images obtained by our algorithm have good local randomness and our algorithm can resist entropy attacks.

E. EXECUTION TIME ANALYSIS

The encryption speed is a good measure to prove the applicability of the proposed algorithm on the current system. The high speed of encryption/decryption can be achieved when both processes use less time consuming operations such as addition and BIT-XOR. The computational efficiency is related to processor clock rate, RAM size, OS etc. The specification of the Laptop is set to 8.00GB RAM, Intel (R) Core (TM) i5-4300M CPU @ 1.90GHz and the operating system is Windows 10 professional. The proposed algorithm is simulated on the MATLAB R2015a platform. The Matlab is a brilliant simulation software with a disadvantage of efficiency. The Matlab have low efficiency as compared to other programming language. But, it still satisfies the needs of a real time cryptography as the proposed system satisfy all the requirements in one round of permutation and substitution. The compiled statistics in Table 21 proves that

TABLE 24. Summary of performance comparison of different color image schemes for encrypted Lena (256 × 256).

Algorithm	Key Space	Correlation			Avg. Entropy	Avg. NPCR	Avg. UACI	EDT	$\tilde{\chi}^2$	Noise
		H$_{R,G,B}$	V$_{R,G,B}$	D$_{R,G,B}$						
Proposed	10^{254}	-0.0238	-0.0013	0.0006	7.9989	99.6129	33.5623	1.26	245	Yes
Ref. [28]	10^{230}	-0.0080	0.0136	-0.0370	7.9983	99.6231	33.6698	-	-	No
Ref. [29]	10^{94}	-0.0025	0.0023	-0.0002	7.9968	99.5999	33.3848	12.17	285	Yes
Ref. [26]	10^{161}	-0.0036	-0.0030	-0.0075	7.9969	99.62537	33.5247	3.70	283	Yes
Ref. [30]	10^{70}	0.0422	0.0464	0.0056	7.9923	95.9730	31.3331	-	-	No
Ref. [55]	10^{90}	-0.0084	0.0004	0.0015	7.9864	99.6097	33.4819	-	-	Yes
Ref. [3]	$10^{148.41}$	-0.0097	-0.0087	0.0065	7.9970	99.60	33.44	5.35	-	Yes
Ref. [53]	4×10^{130}	0.0016	0.0017	0.0003	7.9975	99.6100	33.52	1.02	-	No
Ref. [44]	$10^{77.06}$	-0.0064	0.0107	0.0051	-	99.61	33.5133	0.82	-	No
Ref. [54]	$10^{163.31}$	0.0002	0.0006	0.0009	7.9973	99.6831	32.6602	0.17	-	No
Ref. [6]	$10^{38.53}$	0.0024	0.0029	0.0021	7.8679	99.6139	33.4412	0.76	256	No
Ref. [55]	10^{169}	-0.0065	0.0006	0.0054	7.9930	99.61	33.46	-	-	No
Ref. [52]	$10^{38.53}$	-0.0040	-0.0244	0.0072	7.9967	99.65	33.59	4.97	-	No
Ref. [57]	4×10^{118}	0.0024	0.0058	0.0170	7.9870	99.60	33.89	-	-	No
Ref. [41]	$10^{50.27}$	-0.0045	0.0118	0.0146	7.9972	99.61	33.43	0.602	-	Yes
Ref. [40]	$10^{62.91}$	-0.0007	0.0006	-0.0031	7.9972	99.61	33.46	6.01	-	No
Ref. [36]	2^{128}	0.0014	0.0014	0.0014	7.9973	99.6292	27.7360	7.24	-	No
Ref. [17]	$10^{144.49}$	0.0013	0.0020	0.0025	7.9987	99.6043	33.477	-	230	Yes
Ref. [48]	-	0.0023	0.0023	0.0023	7.9962	99.45	22.61	2.12	-	No
Ref. [14]	2^{256}	0.0166	0.0174	-0.0055	-	99.65	33.43	-	-	No
Ref. [12] Arnold	6.15×10^{215}	0.0003	0.0145	0.0841	7.9989	99.6445	33.4767	6.83	-	No
Ref. [12] 2DMCM	1.24×10^{372}	0.0287	0.0217	0.0179	7.9989	99.6204	33.5014	5.5087	-	No
Ref. [12] 3DMCM	6.13×10^{501}	0.0269	0.0038	0.0094	7.9990	99.5995	33.4763	0.83	-	No


(a) (b) (c)

(d) (e) (f)

FIGURE 15. Robustness against Loss attack.

proposed algorithm has excellent speed performance over Ref. [28]–[30], [40].

V. NOISE ROBUSTNESS

The encrypted data is inexorably bare multiple noises as it flows through physical communication channels. These noises can become a source of problem in recovering of the original image as in Refs. [40], [50]. Therefore, the cipher algorithm must be robust that despite accumulation of noise, it can decrypt the encrypted data successfully. The Peak Signal-to-Noise Ratio (PSNR) is used to measure the quality of the decrypted image after the attack. For the components of the image, PSNR can be calculated using Equations (28) and (29) [55]. The PSNR values for Salt & Pepper noises at 0.5%, 5% and 50% are in Table 22 and the proposed system has equivalent capacity for noise resistance as [28], [29], [41], [55] and visual impact shown in Figure 14. In the next step, 1/16, 1/8 and 1/4 part of encrypted images are removed and then decrypted to measure the quality of recovered image shown in Figure 15 and PSNR score compiled in Table 23. The summary of the performance comparison is presented in Table 24 with many of the similar works.

$$PSNR = 10 \times \log_{10}\left[\frac{255 \times 255}{MSE}\right] \tag{28}$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\|P(i,j) - D(i,j)\|^2 \tag{29}$$

In the above Equations, *MN* represents the dimension of images, *P* is plaintext image and *D* is the decrypted image.

VI. CONCLUSION

A selective cross substitution method for color image encryption is proposed based on 1D chaotic maps, DNA complementary rules and SHA-512 function. The color image is split into three channels after pixels permutation using sorted index of Logistic-Logistic system. The floating-point pseudo-random sequence is divided into eight groups to randomly select the DNA rules for encoding of each pixel. For selective cross substitution, each encoded color channel is split into two arrays representing MSB and LSB. The substitution is achieved by adding MSB and LSB arrays of different channels along with XORing DNA bases which are translated from pseudo-random seqeunce. This addition and exclusive-or process takes place at pixel in cross fashion. The 2^{nd} substitution phase carried out by sequentially combining MSB of a channel to randomly selecting LSB of same channel at pixel level. The simulated results and analysis show that proposed technique has NPCR>99.61%, UACI>33.46% and requires single round of permutation/substitution that make it suitable for the real time applications. Beside these, technique is robust against transmissions' noises as well.

REFERENCES

[1] D. Arroyo, G. Alvarez, J. M. Amigó, and S. Li, "Cryptanalysis of a family of self-synchronizing chaotic stream ciphers," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 805–813, 2011.

[2] H. Bouslehi and H. Seddik, "Innovative image encryption scheme based on a new rapid hyperchaotic system and random iterative permutation," *Multimedia Tools Appl.*, vol. 28, no. 1, pp. 30841–30863, Dec. 2018.

[3] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, 2018.

[4] B. Wang, F. C. Zou, and J. Cheng, "A memristor-based chaotic system and its application in image encryption," *Optik*, vol. 154, pp. 538–544, Feb. 2018.

[5] L. Sui and B. Gao, "Single-channel color image encryption based on iterative fractional Fourier transform and chaos," *Opt. Laser Technol.*, vol. 48, pp. 117–127, Jun. 2013.

[6] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on logistic map and dynatomic modular curve," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8911–8938, Apr. 2018.

[7] 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.

[8] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.

[9] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011.

[10] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.

[11] C. Pak and L. L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

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

[13] A. Broumandnia, "Designing digital image encryption using 2D and 3D reversible modular chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 188–198, Aug. 2019.

[14] I. T. Almalkawi, J. N. Al-Karaki, A. Alsarhan, R. Abu-Ajamiyah, and D. Al-Mughrabi, "An efficient digital image encryption using pixel shuffling and substitution for wireless networks," in *Proc. IEEE Jordan Int. Joint Conf. Elect. Eng. Inf. Technol. (JEEIT)*, Apr. 2019, pp. 266–271.

[15] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Opt. Lasers Eng.*, vol. 115, pp. 131–140, Apr. 2019.

[16] A. S. Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," *Pattern Anal. Appl.*, vol. 22, no. 1, pp. 243–257, 2019.

[17] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

[18] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[19] G. Cui, L. Qin, Y. Wang, and X. Zhang, "An encryption scheme using DNA technology," in *Proc. 3rd Int. Conf. Bio-Inspired Comput., Theories Appl.*, Sep./Oct. 2008, pp. 37–42.

[20] R. Enayatifar, A. H. Abdullah, and I. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014.

[21] A. Soni and A. K. Acharya, "A novel image encryption approach using an index based chaos and DNA encoding and its performance analysis," *Int. J. Comput. Appl.*, vol. 47, no. 23, pp. 1–6, 2012.

[22] K. Singh and K. Kaur, "Image encryption using chaotic maps and DNA addition operation and noise effects on it," *Int. J. Comput. Appl.*, vol. 23, no. 6, pp. 17–24, 2011.

[23] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[24] Y. Zhang, "Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik*, vol. 126, no. 2, pp. 223–229, 2015.

[25] X. Su, W. Li, and H. Hu, "Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy," *Multimed. Tools Appl.*, vol. 76, no. 12, pp. 14021–14033, 2017.

[26] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," *Optik*, vol. 126, no. 24, pp. 5703–5709, Dec. 2015.

[27] A. ur Rehman, D. Xiao, A. Kulsoom, M. A. Hashmi, and S. A. Abbas, "Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 9355–9382, 2019.

[28] A. ur Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018.

[29] A. U. Rehman and X. F. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 2105–2133, Jan. 2019.

[30] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012.

[31] Y. Zhang, W. Wen, M. Su, and M. Li, "Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik*, vol. 125, no. 4, pp. 1562–1564, Feb. 2014.

[32] T. Xie, Y. Liu, and T. Jie, "Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik*, vol. 125, no. 24, pp. 7166–7169, Dec. 2014.

[33] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Optics Laser Technol.*, vol. 60, no. 5, pp. 111–115, 2014.

[34] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 186–192, Mar. 2014.

[35] 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.

[36] A. M. Ayoup, A. H. Hussein, and M. A. A. Attia, "Efficient selective image encryption," *Multimedia Tools Appl.*, vol. 75, no. 24, pp. 17171–17186, 2016.

[37] M. Hamdi, R. Rhouma, and S. Belghith, "A selective compression-encryption of images based on SPIHT coding and Chirikov standard map," *Signal Process.*, vol. 131, pp. 514–526, Feb. 2017.

[38] M. Grangetto, E. Magli, and G. Olmo, "Multimedia selective encryption by means of randomized arithmetic coding," *IEEE Trans. Multimedia*, vol. 8, no. 5, pp. 905–917, Oct. 2006.

[39] G. Bhatnagar and Q. M. J. Wu, "Selective image encryption based on pixels of interest and singular value decomposition," *Digit. Signal Process.*, vol. 22, no. 4, pp. 648–663, 2012.

[40] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimedia Tools Appl.*, vol. 74, no. 13, pp. 4655–4677, Jul. 2015.

[41] A. Kulsoom, D. Xiao, Aqeel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 1–23, Jan. 2016.

[42] L. Li, Y. Yao, and X. Chang, "Plaintext-dependent selective image encryption scheme based on chaotic maps and DNA coding," in *Proc. Int. Conf. Dependable Syst. Appl. (DSA)*, Oct./Nov. 2017, pp. 57–65.

[43] J. D. Watson and F. H. C. Crick, "Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid," *Nature*, vol. 171, pp. 737–738, Apr. 1953.

[44] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field Z_N," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21803–21821, 2018.

[45] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.

[46] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci. (Ny).*, no. 273, pp. 329–351, 2014.

[47] X.-Y. Wang, F. Chen, and T. Wang, "A new compound mode of confusion and diffusion for block encryption of image based on chaos," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 9, pp. 2479–2485, 2010.

[48] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: Parallel sub-image encryption with hyper chaos," *Nonlinear Dyn.*, vol. 67, no. 1, pp. 557–566, Jan. 2012.

[49] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

[50] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons, Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008.

[51] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.

[52] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[53] Z. Gan, X. Chai, K. Yuan, and Y. Lu, "A novel image encryption algorithm based on LFT based S-boxes and chaos," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8759–8783, 2018.

[54] H. Liu and C. Jin, "A novel color image encryption algorithm based on quantum chaos sequence," *3D Res.*, vol. 8, no. 1, p. 4, Mar. 2017.

[55] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Inf. Sci.*, vols. 349–350, pp. 137–153, Jul. 2016.

[56] X.-L. Chai, Z.-H. Gan, Y. Lu, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chin. Phys. B*, vol. 25, no. 10, 2016, Art. no. 100503.

[57] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, Mar. 2014.

AQEEL UR REHMAN received the M.Sc. degree in computer science from The Islamia University of Bahawalpur, the second master's degree in computer engineering from UET Taxilla (CASE campus) Islamabad, Pakistan, and the Ph.D. degree in computer science and technology from Chongqing University, China. He was an Assistant Professor with the Department of Computer Science, Institute of Information Technology, COMSATS University Islamabad, Vehari Campus, Pakistan, where he is currently on a study leave. He is also a Senior Research Fellow with Southwest University, Chongqing, China. He has published more than ten research articles in impact factor journals. His primary research interests include non-linear dynamics and cryptography. He is also a Reviewer of *Optics and Laser Technology*, *Optics and Lasers in Engineering*, and *An International Journal Engineering Science and Technology*.

HUIWEI WANG received the B.S. degree in information and computing science and the M.E. degree in computer application from Chongqing Jiaotong University, China, in 2008 and 2011, respectively, and the Ph.D. degree in computer science from Chongqing University, China, in 2014. He is currently pursuing the Ph.D. with the South China University of Technology, Guangzhou, China. He was a Postdoctoral Research Associate with Texas A&M University at Qatar, Doha, Qatar, from 2014 to 2016. He is currently an Associate Professor with the College of Electronic and Information Engineering, Southwest University, China. His research interests include neural networks, multiagent networks, wireless sensor networks, and smart grids.

MALIK M. ALI SHAHID received the master's degree in computer engineering from the Center for Advance Studies in Engineering (CASE) and the Ph.D. degree in software engineering from the University of Technology Malaysia (UTM). He was with Behria University Islamabad, from 2002 to 2004, and with Air University Islamabad, from 2004 to 2010. He is currently with the Department of Computer Science, COMSATS University Islamabad, Vehari. His research interests include software reliability engineering, software product line, and image-based encryption.

SALMAN IQBAL received the M.S. (CS) degree from COMSATS University Islamabad, Lahore, Pakistan, in 2009, and the Ph.D. degree in network security from the University of Malaya, Malaysia, in 2017. He is currently an Assistant Professor with COMSATS University Islamabad, Pakistan. He has published more than eight research articles in high-impact ISI index journals. His research interests include various aspects of network security, the IoT, and cybersecurity.

ZAHID ABBAS received the B.Sc. degree in mathematics and physics from Bahauddin Zakariya University Multan, Pakistan, in 2000, the master's degree from the Punjab University College of Information Technology (PUCIT), University of the Punjab, Lahore, Pakistan, in 2004, the M.S. degree from Uppsala University, Uppsala, Sweden, in 2008, and the Ph.D. degree from the Faculty of Computing, University Technology Malaysia (UTM), Malaysia, in 2017, all in computer science. He is currently an Assistant Professor with the Faculty of Computer Science, COMSATS University Islamabad, Pakistan. He has authored several research articles in internationally renowned journals. His research interest includes the areas of routing and monitoring in wireless sensor networks, UWSN, LSN, WMN, and the IoT. He has been serving as a Reviewer for numerous journals, such as the *Journal of Network and Computer Applications* and IEEE Access, and the *IEEE Communication Magazine*.

AMNAH FIRDOUS received the bachelor's degree and the master's degree in computer science (MSCS) from The Islamia University of Bahawalpur, Pakistan, where she is currently pursuing the Ph.D. degree in computer science. She is a Lecturer with the Computer Science Department, COMSATS Institute of Information Technology, Vehari, Punjab, Pakistan, where she is on a study leave. Her primary research interests include image processing, Petri nets, and cryptography.