IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 31, 2020, accepted September 14, 2020, date of publication September 18, 2020,
date of current version September 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3024994

A Color Image Encryption Algorithm Based on One Time Key, Chaos Theory, and Concept of Rotor Machine

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

[1]College of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
[2]Department of Computer Science, COMSATS University Islamabad, Vehari Campus, Vehari 63110, Pakistan
[3]Department of Computer Science and IT, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[4]School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China

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 method proposed for encrypting color images is comprised of one-time keys and chaos theory using a distinctive concept of rotor machine. The novelty of this scheme is that the rows and columns of 2-dimensional images are converted into circular object called rotor and can be rotated at 360 degrees in clockwise or anti clockwise direction. The rotation will change the existing rotor into new one and can be used in substitution process of plain image. This process can be repeated β times and each time a new rotor is created just by a simple rotation. The rotation is performed in terms of pixels so degree of angle is converted into number of pixels. Using this method, same object with new face (after rotation) is used for encryption. The pixels of color image are permuted using the sorted index of logistic sequence. Then, three pseudo-random images are created from Piecewise Linear Chaotic Map (PWLCM). For substitution, both the permuted color channels and pseudo-random images are transformed into rotors. The angle is obtained from Chen chaotic system. The one-time keys are for chaotic maps are generated by using 512-bits hash of plain image. The simulated outcomes demonstrate that the proposed system has high quality of results and requires only single round of encryption to achieve high encryption along with high robustness against the transmission noises.

INDEX TERMS Chaos theory, color image encryption, SHA-512, rotor machine, one time key.

I. INTRODUCTION

Information security is an active research area from decades. Even in the old era, the transmission of information required security and can be accessed by unauthorized eavesdroppers. Since, the issue gave rise to construction of techniques and algorithms, like steganography and cryptography which could effectively encrypt and decrypt the target information. With the start of digital era, digital cryptography heavily utilized and adopted different forms of information hiding, as medical images, grayscale images, color images and binary images. This type of information hiding requires a different track of research and development and ciphering techniques to cope the associated issues and challenges [1], [2].

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

The charming evolution of networked multimedia, transmission over the past decade has heavily increased the online data traffic comprised of video, audio and image contents. The security concerns associated legality and unauthorized access of data and its movement on internet are gaining interest in research. The image security techniques are indifferent to text and other secured information, as strong correlation between neighboring pixels do exist in an image. The indifference caused conventional encryption techniques as Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Standard (IDES) and Linear Feedback Shift Register (LFSR), [3], [4] inefficient. These techniques are primarily built for small sized text information, on contrary images and videos contain large data volumes, strong correlation among data pixels which makes these techniques quite slow and inefficient computationally. Few newer techniques were coined to handle image cryptography like wavelet transform [5], Fibonacci transform [6], vector quantization [7], gray code [8], hash [9], DNA computing [8]–[14], compression techniques [15] and chaos [16]–[25] and [84]. The chaos has a wide variety of applications in various fields such as [79]–[82] and [83].

Among all above techniques, chaos acquired a lot of attention due to its simple structure and high sensitivity of its initial conditions [26]. Mathews became the first scientist to use chaos in an image encryption [27]. Chaotic image encryption techniques can be classified in two categories i). One-dimension (1D) and ii) Multi-dimension (MD). The MD chaotic maps have proven its worth in image security [52]–[54] because of its inherent complex structures and multiple parameters. But MD chaotic maps are complex in nature and time consuming [55]. On the contrary, 1D chaotic systems have less complex structure and are easy to implement in hardware/software [56]. The ID chaotic maps have also weaknesses of short chaotic periods, non-uniform distribution of chaotic output and vulnerable to cryptanalyzed using correlation functions and low computational analysis [57].

Gan *et al.* [16] used the SHA-256 hash function and the bit planes of images are encrypted in 3-dimension. The Galois field of order 256 is used to construct substitution boxes through Linear Fractional Transformation [17]. In substitution, Forward Substitution Process (FSP) and Reverses Substitution Process (RSP) are applied on of the pixels of image. Yang and Liao [18] used finite field to generalize the Logistic map and then find an auto morphic mapping between two Logistic maps to device the parameters over finite field ZN. Liu and Jin [19] has utilized the coupling of the 2D logistic map and quantum chaotic map by nearest-neighboring coupled-map lattices at the higher complexity and giving better randomness this is applied to build an image cipher. Li *et al.* [20] generated the dynamic modular curve and its relationship with a logistic map for image encryption scheme. Although few weaknesses have been revealed after cryptanalysis of chaos-based image encryption algorithms and limited image encryption techniques as these are unable to withstand the attacks [23], [25], [50], [58], [59]–[61]. One such attack is the chosen plaintext attacks on the cryptosystems, which is independent of secret keys on the plaintext. Wang *et al.* [62] crypt-analyzed the Chanil Pak scheme [23] using a chosen plaintext attack [63]. Fan *et al.* [64] exploited the weakness in the encryption scheme proposed by Hsiao and Lee [25] using the chosen-plaintext attack while Rhouma *et al.* [65] break the cipher presented by Patidar *et al.* [58] using the same technique to recover the original image without knowing the secret key. Similarly, Zhang *et al.* [66] cryptanalyzed the Liu *et al.* [59] designed technique using a chosen plaintext attack. In the suggested scheme the secret keys are modified without user intervene with the very slight changes in the plaintext. This dependency is spawned by SHA-512 hash function for the plaintext to survive against chosen plaintext attack. In the proposed framework, the chaotic maps are used for higher sensitivity with respect to initial conditions and system parameter for simple and basic structure.

The rotor machines are an electro-mechanical device used for poly-alphabetic substitution. A number of inventors gave the concept of using rotor machines in cryptography. Two Dutch naval officers, Theo A. Van Hengel, and R. P. C. Spengler are considered the inventors of the first rotor cipher machine in 1915. Later, Edward Hebern, Arvid Damm, Hugo Koch and Arthur Scherbius also created their own cryptographic rotor machines. The quite famous rotor machine is Enigma developed by Germans during WWII [67]–[69]. A Rotor Machine consists of multiple independent rotatable cylindrical plates called rotors. Rotor is a device which is electro-mechanical in nature to cipher and deciphers plaintext for which security is required. The electrical pulses can flow through rotors and each rotor contains' input pins and 'n' output pins, internal wiring is done in a way that each input pin is connected to a unique output pin usually with a letter of the alphabet. On each input event, 1^{st} rotor maps input value to some fixed output value and rotate one step ahead. This mapping is actually a monotype substitution mechanism. The output of 1^{st} rotor is again mapped to another fixed value by the 2^{nd} rotor and 2^{nd} rotor move one step ahead after 1^{st} rotor completes a cycle. On completion of a cycle, the 2^{nd} rotor rotates one-step ahead and this process continues and the output of the last rotor is the encrypted value of the input. Hence, all rotors of a cipher machine work like the odometer of an auto vehicle and multiple mono-substitutions behave in poly substitution manner. After encryption of a letter, rotors advance one-step to enhance the security by changing the substitution pattern.

Based upon the concept of a rotating cylinder, a color image encryption technique is proposed which uses multiple chaotic maps and rotating behavior. The one-time pad is used to modify the common initial conditions of chaotic maps by 512-bits hash of plain image to survive against chosen plaintext attack. To break the correlations among pixels, three channels of a plain image are arranged into one-dimensional array and the pixels are permuted using logistic sequence. This one dimensional permuted vector is split into three 2-dimensional matrices. Further, three pseudo-random images are such as made from the Piecewise Linear Chaotic map (PWLCM). The rows and columns of permuted channels and the pseudo-random images are transformed into rotors. The substitution phase is actually based on the concept of rotor cipher in which each alphabet is mapped to some fixed alphabet and rotors rotate one step. In this technique, a rotor of a plain image is added under the modulus 2 operation with a pseudo-rotor generated from the random image. Like the rotational behavior of rotor cipher, the pseudo-rotor is rotated around an angle $+\theta$ or $-\theta$ and again added with the previously substituted rotor of the plain image. In this way, each rotation to a pseudo-rotor creates another pseudo-rotor like an electromechanical cylinder for substitution. This process continues for a random number of times to complete the substitution of a rotor. The angle is obtained from Chen chaotic system. The rotors of all three channels are treated in a similar fashion to achieve the encryption.

In this paper, section II discusses the preliminaries of chaotic components like Logistic, PWLCM, Chen chaotic systems and formation of rotors from a digital image. In the third section, the detailed methodology is provided, fourth section contains the comprehensive results, section V discusses the robustness against common attacks and last section comprises of the efficient version of the proposed cipher.

II. PRELIMINARY OF PROPOSED SYSTEM

A. LOGISTIC SYSTEM

The logistic map is very [18] simple however extensively applied dynamic method for image encryption. Here is the explanation of conventional logistic map by,

$$S_{i+1} = \mu \times s_i(1 - s_i) \tag{1}$$

In the above Equation (1), μ controls the behavior and it can have values in range $0 < \mu < 4$ and $s_i \in (0, 1)$, $i = 0, 1, \cdots, n$. The above system has chaotic behavior for $\mu > 3.568945672$ and generates a random number for pixel permutation of plain image.

B. PIECEWISE LINEAR CHAOTIC MAPS (PWLCM)

The widely studied one-dimensional non-linear system is PWLCM, which has high invariant natural density [9]. It is widely adopted by researchers in their proposed work [70], [71] due to its efficiency and ease of implementation as shown in Equation (2). The PWLCM is highly sensitive for seeds, which are set to be precision of $10^{(-14)}$ for new and proposed system.

$$t_{i+1} = \begin{cases} t_i/p_0 & 0 \le t_i < p_0 \\ (t_i - p_0)/(0.5 - p_0) & p_0 \le t_i < 0.5 \\ (1 - t_i) & t_i \ge 0.5 \end{cases} \tag{2}$$

C. CHEN CHAOTIC SYSTEM

The hyper-chaotic system devised by Chen is significantly sensitive for initial values and the control parameters; which is defined as follows,

$$\begin{aligned} \dot{w} &= a(x - w) \\ \dot{x} &= -wy + dw + cx - z \\ \dot{y} &= wx - by \\ \dot{z} &= w + k \end{aligned} \tag{3}$$

In Equation (3), a, b, c, d, and k are the system parameters, when $a = 36$, $b = 3$, $c = 28$, $d = 16$ and $-0.7 \le k \le 0.7$, the system of equation is chaotic state and can be utilized to generate pseudo-random numbers. In this paper, $k = 0.2$, initial conditions (0.3, −0.5, 1.2, 1.0) for Chen chaotic [12] system is used to generate sequence. The fourth-order Runge-Kutta method is used to explain and solve the Equations and to obtain the sequences W, X, Y and Z, and all these four sequences are combined in from one array.

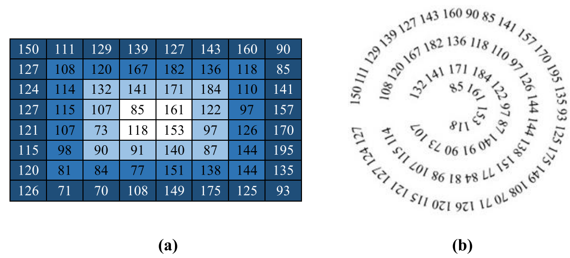

FIGURE 1. (a) 8 × 8 Plain Image (b) Four Rotors created from (a).

D. ROTOR CIPHER/MACHINE

A rotor machine is electromechanical devices that consist of several rotors in series connection. For each input letter, the rotors move in unique ways, some by one position and some only several steps. The cryptographic security depends upon the number of rotors and other intrinsic settings. The idea of rotor cipher is much fascinating and widely used to build many secure ciphers during mid-70ś and 80ś [67]–[69]. The proposed system uses the idea of rotor substitution cipher to achieve image encryption using chaotic maps. A digital image consists of rows and column, first row, last column, last row, and first column are considered rotors of the image. To encrypt this rotor, one pseudo-rotor is generated from the chaotic map. This pseudo-rotor will serve as the multi-rotors machine to perform encryption using addition operation in modulus 2. The rotor of pseudo-image is rotated around some angle to create another rotor and then added in modulus 2 again with the rotor of the simple plain image. This mechanism is repeated for multiple times depending upon the user input.

E. ROTOR FORMATION

If a 24-bit color image of size N^2 is given as input is shown in Figure 1(a), the system will generate rotors using layers of rows and columns. The first rotor r will form by combining Row 1, Column 1, Row N and Column N of the input image as displayed in Figure 1(b). Later the size of input matrix will be reduced to $(N-2) \times (N-2)$ and this new matrix is treated as an input for the next rotor. This process continues till all the rows and columns are converted into Rotors. Finally, it yields $N/2$ numbers of rotors and at each step, the size of a rotor can be calculated as,

$$\begin{aligned} r_i &= 4n_i - 4 \\ n_i &= N - 2 \times (i - 1) \end{aligned} \tag{4}$$

where $i = 1, 2, \cdots, N/2$

An example image of size 8 × 8 is shown in Figure 1(a), which is used as input to form rotors shown in Figure 2(b). A total of 8/2 possible rotors can be formed according to the algorithm. The first rotor consists of 28 pixels, 2^{nd} consists of 20, 3^{rd} consists of 12 and the last rotor comprises of four pixels. Figure 2 demonstrates the rotation of rotor r_1 around 255, 75 and -287 degree to build three rotors.

$$n_1 = 8 - 2 \times (1 - 1) = 8$$

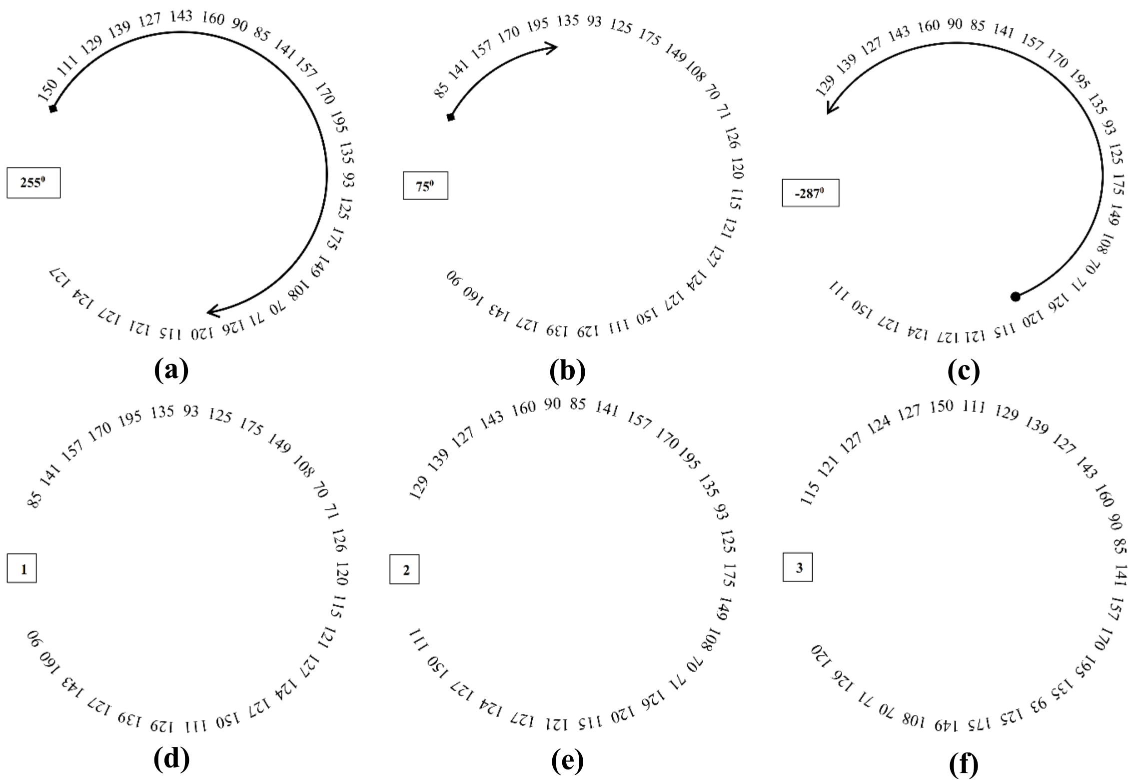

FIGURE 2. 1^{st} rotor shown in Figure 2(b):(a) Rotated at 255^0, (b) Rotated at 75^0,(c) Rotated at -287^0 (d) Result of 3(a), (e) Result of 3(b), (f) Result of 3(c).

$$\begin{aligned} r_1 &= 4 \times 8 - 4 = 28 \\ n_2 &= 8 - 2 \times (2 - 1) = 6 \\ r_2 &= 4 \times 6 - 4 = 20 \\ n_3 &= 8 - 2 \times (3 - 1) = 4 \\ r_3 &= 4 \times 4 - 4 = 12 \\ n_4 &= 8 - 2 \times (4 - 1) = 2 \\ r_4 &= 4 \times 2 - 4 = 8 \end{aligned} \quad (5)$$

III. PROPOSED SCHEME

A. SEED/KEY GENERATION

The concept of the seed/key generation process is taken from the established research [71]. A hash digest H of 512 bits is obtained by inputting the plain image to the SHA-512 hash function. The message digest H consists of 128 hexadecimal digits, first 84 hexadecimal digits are split into seven equal sized blocks m_i and each block composed of twelve hexadecimal digits. Each of these blocks is transformed into a number in the range $[0 - 0.0156]$ by applying following Equation,

$$m_i = \frac{hex2dec\,(m_1, \cdots, m_7)}{2^{54}} \quad (6)$$

where $i = 1, 2, \cdots, 7$

The logistic map shown in Equation (1) needs initial seed s_0 to generate random numbers, new seed value is calculated as follows,

$$s'_0 = s_0 + m_1 + CK \mod 1 \quad (7)$$

One Dimensional PWLCM shown in Equation (2) requires two values, initial seed t_0 and control parameter p_0 which are modified as follows,

$$\begin{cases} t'_0 = t_0 + m_2 + CK \\ p'_0 = p_0 + m_3 + CK \end{cases} \mod 1 \quad (8)$$

If seed values for Chen chaotic system are u_0, v_0, x_0 and x_0 then these can be modified as follows,

$$\begin{cases} u'_0 = u_0 + m_4 + CK \\ v'_0 = v_0 + m_5 + CK \\ w'_0 = w_0 + m_6 + CK \\ x'_0 = x_0 + m_7 + CK \end{cases} \mod 1 \quad (9)$$

The CK is the common key used in all the above Equations, which is generated as follows,

$$CK = s_0 + p_0 + t_0 + u_0 + v_0 + w_0 + x_0 \mod 1 \quad (10)$$

The last 44 hexadecimal digits of H are used as follows,

$$\begin{cases} sIdxR = hex2dec(H_{85}, \cdots, H_{98}) \\ sIdxG = hex2dec(H_{99}, \cdots, H_{112}) \\ sIdxB = hex2dec(H_{113}, \cdots, H_{128}) \end{cases} \mod VAL \quad (11)$$

The *idxR*, *idxG* and *idxB* serve as the staring index value among the array of angles θ.

$$VAL = (N \times N) - [Total\_Rotors \times \beta] \tag{12}$$

In the above equation, β is number of rotational angles to perform circular rotation on each rotor of pseudo-image. The *VAL* is a decimal value that provides the modulus operation to select angles θ up to $Total\_Rotors \times \beta$.

1) DIFFUSION

The method of diffusion employed for the proposed system using 24-bit image is simple. Firstly, 24-bit image I is transformed into a 1D array of size $1 \times 3N^2$. The Equation (1) is used to yield chaotic sequence S up to $3 \times N^2$ times using modified initial condition s'_0. The S is sorted to record its index using Equation (13) and the pixels of plain image I are re-arranged using the sorted index of S as follows,

$$\begin{aligned} S &= \{s_i, s_{i+1}, \cdots, s_{3\times N^2}\} \\ [valS, idxS] &= sort(S) \\ I' &= I\,(idxS) \end{aligned} \tag{13}$$

To create three channels independently, the permuted image is separated into three arrays of size $1 \times N^2$ called R', G', and B' as follows,

$$\begin{cases} R' = \{I'_1, I'_2, \cdots, I'_{N^2}\} \\ G' = \{I'_{N^2+1}, I'_{N^2+2}, \cdots, I'_{2N^2}\} \\ B' = \{I'_{2N^2+1}, I'_{2N^2+2}, \cdots, I'_{3N^2}\} \end{cases} \tag{14}$$

The R', G' and B' are transformed into 2D matrices.

2) CONFUSION / SUBSTITUTION

The 2D matrices R', G' and B' are used in (4) to create $Rotors_red$, $Rotors_reen$, and $Rotors_blue$ shown in Equation (15).

$$\begin{cases} Rotors\_red = R'\{rr_i, rr_{i+1}, \cdots, rr_{N/2}\} \\ Rotors\_green = G'\{gr_i, gr_{i+1}, \cdots, gr_{N/2}\} \\ Rotors\_blue = B'\{br_i, br_{i+1}, \cdots, br_{N/2}\} \end{cases} \tag{15}$$

An array T is generated by iterating PWLCM $3 \times N^2$ and transformed into $(0 - 255)$. After that, split T' into 2-Dimensional matrices called T_1, T_2, and T_3, each of size N^2.

$$T' = [round(T \times 10^{14})] \bmod 256 \tag{16}$$

$$\begin{cases} T_1 = \{T'_1, T'_2, \cdots, T'N^2\} \\ T_2 = \{T'_{N^2+1}, T'_{N^2+2}, \cdots, T'_{2N^2}\} \\ T_3 = \{T'_{2N^2+1}, T'_{2N^2+2}, \cdots, T'_{3N^2}\} \end{cases} \tag{17}$$

The matrices T_1, T_2 and T_3 are transformed into rotors and called as $pseudo_red$, $pseudo_green$ and $pseudo_blue$ where each rotor has a variable size that can be calculated using the Equation (4),

$$\begin{cases} pseudo\_red = T_1\{rr_i, rr_{i+1}, \cdots, rr_{N/2}\} \\ pseudo\_green = T_2\{gr_i, gr_{i+1}, \cdots, gr_{N/2}\} \\ pseudo\_blue = T_3\{br_i, br_{i+1}, \cdots, br_{N/2}\} \end{cases} \tag{18}$$

To begin with confusion phase, besides image rotors and pseudo rotors, the algorithm requires angles about which pseudo-rotors are rotated before performing addition in modulus 2 operation. For this, Chen chaotic system is iterated $N^2 + 2000$ times with new common keys calculated by Equation (9). The obtained four sequences U, V, W and X are merged into the one-dimensional array called C as follows:

$$C_{4i-3} = U_i;\quad C_{4i-2} = V_i;\ C_{4i-1} = W_i;\ C_{4i} = X_i \tag{19}$$

The values of C are transformed into $(-360^0$ - $360^0)$ called angles θ by applying modulus operation as follows,

$$\begin{aligned} & if\, C(i) < 0 \\ & temp = C(i) \bmod 360 \\ & else \\ & C(i) = C(i) \bmod 360 \\ & end \end{aligned} \tag{20}$$

where $i = 1, 2, 3, \ldots, N^2$ The array C consists of N^2 angles and the proposed system requires only a few of these to rotate the rotors created from pseudo images. The Equation (11) compute the beginning of random selection of angles from C. The total numbers of angles required for a color channel depends upon the number of rotations β to each rotor and total number of rotors are $N/2$ of an image.

$$\begin{cases} Total\_Rotors = N/2 \\ Totol\_angles = Total\_Rotors \times \beta \\ angles\_red \\ = C\,[sIdxR + 1, idxR + 2, \cdots, Total\_angles] \\ angles\_green \\ = C\,[sIdxG + 1, idxG + 2, \cdots, Total\_angles] \\ angles\_blue \\ = C\,[sIdxB + 1, idxB + 2, \cdots, Total\_angles] \end{cases} \tag{21}$$

Then *angles_red*, *angles_green*, *angles_blue* are transformed into 2-Dimensional matrix of size of $Total\_rotors \times \beta$ in which all β values of a row are used to rotate single pseudo rotor. The ALGORITHM 1 depicts the operations involved in applying the confusion operation on rotors of *Rotors_red*. The flow diagram of the complete encryption procedure is illustrated in Figure 3 and substitution process is elaborated in Figure 4.

3) SUMMARY OF METHODOLOGY

The plain image I is used in system, has size of $N2 \times 3$ and encryption is achieved using following steps:

Input: The I is a 24-bit color image,s_0, t_0, p_0, w_0, x_0, y_0, and β are the seeds for different chaotic systems.

Output: A ciphered image i.e., E

Algorithm 1 Substitution Algorithm

```
procedure Substitution(Rotors_red, pseudo_red, angles_red)          ▷ The size of inputs are N/2
    for i ← 1 to N/2 do
        size ⟵ Computesize(Rotors_red(i))                            ▷ Compute the size of ith rotor
        Pixels_Per_Degree ← size/360      ▷ compute the number of pixels used in rotation for 1 degree
        CipherRed(i) ← Rotors_red(i) + pseudo_red(i) mod 2           ▷ Add plain and pseudo rotor
        for j ← 1 to β do
            θ ⟵ round(Pixels_Per_Degree × angles_red(i, j))
            pseudo_red(i) ⟵ rotate(pseudo_red((i), θ)                ▷ Rotate pseudo rotor around angle θ
            CipherRed(i) ← CipherRed(i) + pseudo_red(i) mod 2        ▷ Add confused rotor and pseudo rotor
        end for
    end for
end procedure
```

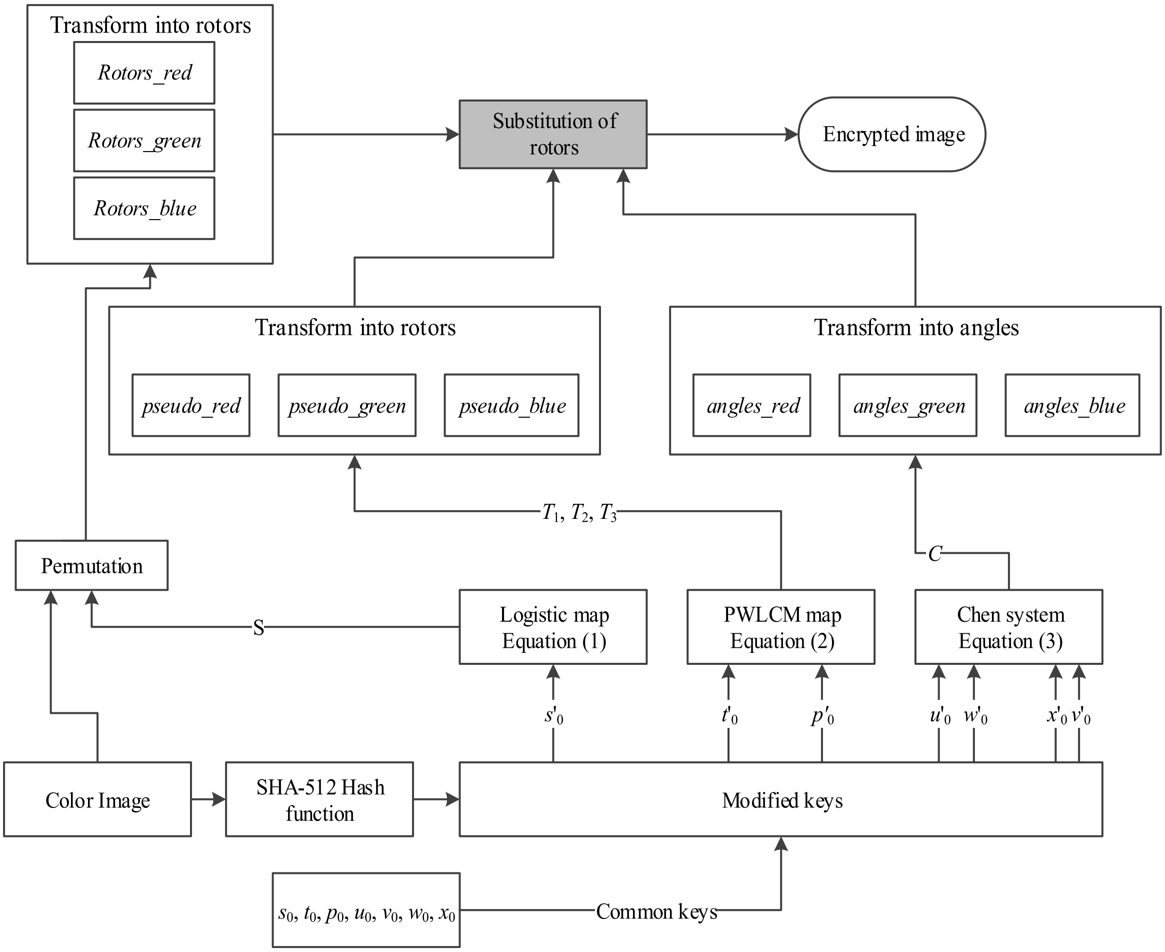

FIGURE 3. Flow diagram of proposed image encryption algorithm.

1) Create one-time key by using 512-bits hash value of I and modify common keys to get new common keys as mentioned in subsection III-A.
2) The 24-bit image I is converted into $1 \times 3N^2$ and get sequence S up to $3N^2 + M$ by using Equation (1) with new s_0'. The first M elements are discarded and diffuse the pixels of I discussed in section III-A1. At last, divide the diffused image into three different 2D matrices of size $N \times N$.
3) Create rotors from plain image using Equation (15) called *Rotors_red*, *Rotors_green* and *Rotors_blue* from 2D matrices R', G' and B'.
4) Get an array T of random numbers by iterating PWLCM map up to $3N^2$ times, converted into T' and

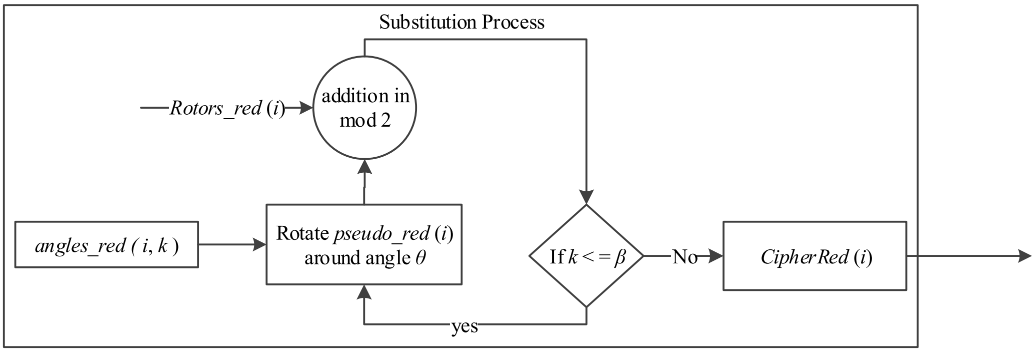

FIGURE 4. Theme of the proposed image encryption algorithm.

then transform into 2D matrices called T_1, T_2 and T_3, each of size N^2 using Equation (16) and (17).

5) Create rotors from T_1, T_2 and T_3 and called *pseudo_red*, *pseudo_green* and *pseudo_blue* shown in Equation (18).
6) Iterate Chen system chaotic and merge W, X, Y and Z into 1-D array named as C shown in Equation (19) and create rotational angles from C using Equation (20).
7) The *angles_red*, *angles_green* and *angles_blue* are separated randomly from C using *sIdxR*, *sIdxG* and *sIdxB*. The arrays created from C are transformed into 2D matrices of size $Total\_rotors \times \beta$.
8) Perform substitution operation on rotors in pairs, *Rotors_red* and *pseudo_red*, *Rotors_green* and *pseudo_green*, *Rotors_blue* and *pseudo_blue* rotors. The pseudo-code of substitution of *Rotors_red* and *pseudo_red* is represented as ALGORITHM 1 and can also be applied for *Rotors_green* and *Rotors_blue*. The simplest addition in modulus 2 operation is applied for substitution.
9) Rearrange the encrypted rotors into rows and columns, then create a matrix of size $3 \times N^2$ called color encrypted image E. The result is shown in Figure 4.

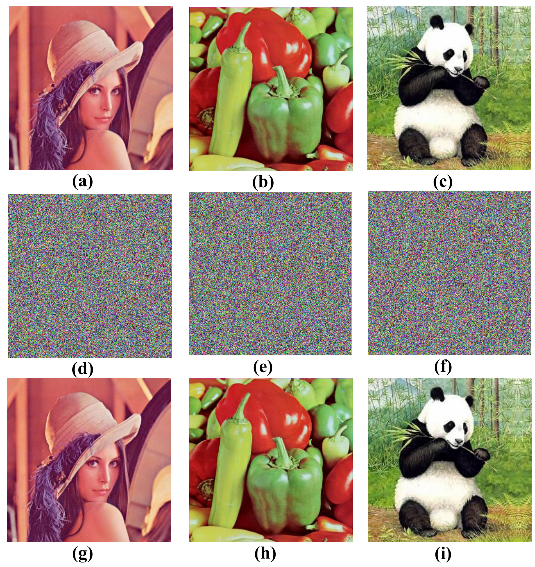

FIGURE 5. Encryption results: (a) Lena; (b) Pepper; (c) Panda; (d) Ciphered image of (a); (e) Ciphered image of (b); (f) Ciphered image of (c); (g) Deciphered image of (d); (h) Deciphered image of (e); (i) Deciphered image of (f).

B. DECRYPTION PROCESS

The proposed system uses symmetric encryption method so that decryption procedure is applied from bottom to top step (9) to step (1) to retrieve back the plain image. The cipher image is split into three channels and then transformed into rotors, three pseudo-random images are generated through PWLCM and then transformed into pseudo-rotors. To decrypt single rotor of cipher image; firstly a *pseudo_rotor* is rotated around angle θ up to β times and new rotors are saved as *Rotors_computed*. After that, addition of modulus 2 is applied between *rotors_computed* and rotors of the ciphered image in reverse order to obtain the rotor of plain image. The pseudo-code is described as ALGORITHM 2 shown as follows.

IV. EXPERIMENTS AND RESULTS

The trials have been applied on PC of Corei5 clocked at 2.8GHz with 8GB RAM using images of size $256 \times 256 \times 3$). The test images Lena, Peppers, Panda, Vegetables, and Goat are used in the experiments. The initial seeds used for trials/simulation are required by Logistic, PWLCM maps are: $s_0 = 0.123456789010$, $p_0 = 0.2345678900$ and $t_0 = 0.3456789012$. The initial seeds of Chen system are $u_0 = 0.2456789012$, $v_0 = 0.4567890124$, $w_0 = 0.5678901234$ and $x_0 = 0.6789012346$. The β is set to 3 for simulations that are the number of rotations to perform on a pseudo-rotor around angles θ.

All the above initial seeds used for chaotic maps can be called a key set named as γ_0. By changing one of the initial seed in γ_0, a new key set produce called γ_1. So there are total eight common keys used in the proposed system so one can produce eight different key sets as $\gamma_1, \gamma_2, \gamma_2, \gamma_4, \gamma_5, \gamma_6, \gamma_7, \gamma_8$. There are different images used in simulations known as Lena, Pepper and Panda are demonstrated in Figure 5(a) to 5(c) and the results of encryption of these images are illustrated in Figure 5(d) to 5(f) distinctly.

Algorithm 2 Decryption Algorithm

```
procedure Substitution(CipherRed, pseudo_red, angles_red)          ▷ The size of inputs are N/2
    for i ← 1 to N/2 do
        size ⟵ Computesize(CipherRed(i))                            ▷ Compute the size of ith rotor
        Pixels_Per_Degree ← size/360           ▷ compute the number of pixels used in rotation for 1 degree
        Rotors_computed(1) = pseudo_red(i)                          ▷ Save pseudo rotor without rotation
        for j ← 1 to β do
            θ ⟵ round(Pixels_Per_Degree × angles_red(i, j))
            Rotors_computed(j + 1) ⟵ rotate(pseudo_red((i), θ)     ▷ Save rotated pseudo rotor in Rotors_computed
        end for
        for k ← β to 2 do
            CipherRed(i) ← CipherRed(i) + Rotors_computed(k) mod 2  ▷ Add confused rotor and pseudo rotor
        end for
        Rotors_red(i) ← (CipherRed(i) + Rotors_computed(1)) mod 2
    end for
end procedure
```

All cipher-images have information that is random like and have no visual effect at all.

A. KEY SPACE ANALYSIS

The secret keys in the proposed system have different floating-point precision ranging from 10^{10} to 10^{14}. The initial seed s_0 for the Logistic map key space $K_{Logistic} = K_{S_0} = 10^{14} \cong 2^{46.50}$. The key space for PWCLM is $K_{p_0} \times K_{t_0} = 10^{24} \cong 2^{79.23}$ with the precision of 10^{12} and Chen system, which uses four inputs (0.3, - 4, 1.2 and 1.0) with each having floating point precision of 10^{10}. The last but most important is that common keys are modified using SHA-512 hash function which has better security feature compared to SHA-1 shown in Table 1. The total key space for proposed system is $K_{Total} = K_{Logistic} \times K_{PWLCM} \times K_{Chen} \times K_{SHA-512} = 10^{232} \cong 2^{717}$. This key space is extremely high and larger than the existing systems shown in Table 2.

TABLE 1. Analysis of Hash function.

Hash function	Input Size	Block Size	Word Size	Output size	Security
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-512	$< 2^{128}$	1024	64	512	256

B. KEY SENSITIVITY AND DIFFERENTIAL ANALYSIS

The key sensitivity is the measure for analyzing the strength of the encryption technique against the brute- force attack. The cryptographic algorithm must be resilient against insignificant modification in secret key so that it must absolutely change the output to provide the full sense of key space. In the proposed system, three chaotic systems are utilized, the Logistic, PWLCM and the Chen system that is very sensitive to a minor change in initial conditions. In order to make the crypto-system more robust, a new common key is generated by adding all the initial conditions, which make sure that change in a single key will spread to all common keys. For this, Figure 6(a) is the plain image of Panda and Figure 6(b) shows the Ciphered image using the set of secret key called γ_0.

TABLE 2. Comparison of Key space.

Algorithm	Key space
Proposed	10^{232}
Ref. [10]	10^{94}
Ref. [11]	10^{230}
Ref. [12]	10^{70}
Ref. [14]	10^{90}
Ref. [16]	2^{318}
Ref. [17]	4×10^{130}
Ref. [18]	2^{256}
Ref. [19]	2^{128}
Ref. [20]	2^{128}

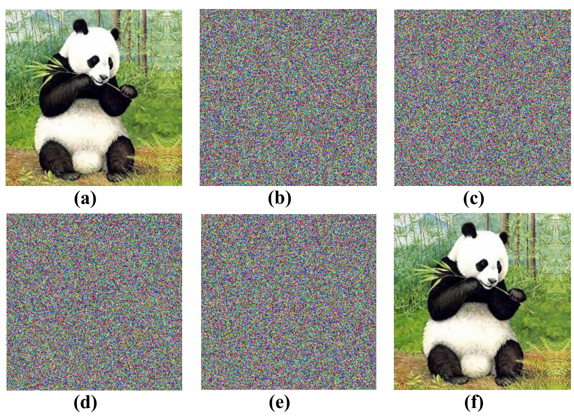

FIGURE 6. Encrypted and decrypted images. (a) Original Lena image; (b) Encrypted Lena image; (c) Decrypted Lena image; (d) Original Baboon image; (e) Encrypted Baboon image; (f) Decrypted Baboon image; (g) Original Pickle image; (h) Encrypted Pickle image; (i) Decrypted Pickle image.

The initial condition for the Logistic system is altered as $s_0 = 0.123456789011$ while others keys are kept same, this new key set is calledγ_1, and it is used to encrypt Panda image;

TABLE 3. Difference in values of two ciphered-images produced with a bit of different keys.

Key Set	Lena	Vegetable	Panda	Goat	Avg.
$\gamma_1\ (s''_0 = s'_0 + 10^{-12})$	99.6048	99.6083	99.6134	99.6043	99.6077
$\gamma_2\ (t''_0 = t'_0 + 10^{-12})$	99.6277	99.5875	99.6099	99.6312	99.6148
$\gamma_3\ (p''_0 = t'_0 + 10^{-12})$	99.5972	99.6048	99.6104	99.5941	99.6016
$\gamma_4\ (u''_0 = t'_0 + 10^{-12})$	99.6109	99.6063	99.6098	99.6145	99.6104
$\gamma_5\ (v''_0 = t'_0 + 10^{-12})$	99.6012	99.6460	99.6199	99.6292	99.6241
$\gamma_6\ (w''_0 = t'_0 + 10^{-12})$	99.6190	99.6221	99.5982	99.6017	99.6102
$\gamma_7\ (x''_0 = t'_0 + 10^{-12})$	99.5981	99.6134	99.6124	99.6099	99.6084
$\gamma_8\ (\beta' = \beta + 1)$	99.6096	99.6108	99.6138	99.6115	99.6148
Avg.	**99.6096**	**99.6108**	**99.6138**	**99.6115**	**99.61143**
Ref. [10]	99.6073	99.6106	99.6056	99.6111	99.60620
Ref. [14]	99.6073	99.6103	99.6003	99.6069	99.6103
Ref. [72]	99.6147	99.6065	99.6137	99.6063	99.6086

TABLE 4. Difference of two encrypted images using different key sets 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	99.6068	99.6195	99.6256	99.6093	99.6180	99.6307	99.6155	99.6002
γ_1	0	0	99.5803	99.5926	99.6282	99.6093	99.5992	99.6104	99.6216
γ_2	0	0	0	99.6078	99.6180	99.5875	99.6099	99.5982	99.6134
γ_3	0	0	0	0	99.5926	99.6384	99.5997	99.5992	99.6511
γ_4	0	0	0	0	0	99.6236	99.6216	99.6246	99.6028
γ_5	0	0	0	0	0	0	995982	99.6007	99.6251
γ_6	0	0	0	0	0	0	0	99.6083	99.6302
γ_7	0	0	0	0	0	0	0	0	99.6089

the results are shown in Figure 6(c). The key set γ_1 is used to decrypt the image of Figure 6(b), which resulted in failure as shown in Figure 6(d). In a similar way, key set γ is used to decrypt image of Figure 6(c) and it failed as well, but when γ_0 is used for decryption of Figure 6(b), the result is a success, which is shown in Figure 6(e) that proved the robustness proposed system. The difference in the encrypted image obtained through slight modification in keys is shown in Table 3 and the results are better than schemes shown in Refs. [10] and [14]. Further, the proposed system is put into another test to measure the difference between encrypted images generated from keys sets $\gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6, \gamma_7, \gamma_8$. The average difference is greater than 99.60%.

In the next phase, the sensitivity of the secret keys are measured for decryption. The purpose of this measurement is that if one of the key is different in a keyset then decrypted image must be 100% different from the original image. This 100% difference makes sure that attacker will not able to get any clue between the key and original image. The Table 5 represents this phenomenon and average difference generated by any key is greater than 99%.

C. STATISTICAL ANALYSIS

1) HISTOGRAM ANALYSIS

A histogram represents frequency distribution of an image. If the distribution is uniform it means that encryption quality is better. In the plain image, some of the gray levels do not exist (or contain zero frequency) and some gray levels have the very high frequency. However, in the histogram of an encrypted image, frequency of all gray levels should be equal. For an RGB color image, there will be three histograms and all three should have good uniform distribution for the encrypted image to stand again the statistical attack. The histograms for Red, Green and Blue channels of plain image Lena and its decrypted image are displayed in Figure 7. The plain image is represented in Figure 7(a) to 7(c) and the Figure 7(d) to 7(f) represent ciphered image. It is very clear from the figures that histograms for all channels of cipher image are fairly uniformed. The quantitative analysis which is mentioned in Refs. [10], [14] are used to produce the results of Tables 6 and 7.

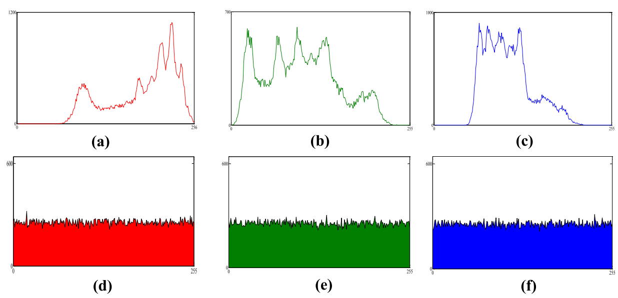

FIGURE 7. Histograms analysis of Lena, Upper row, Histograms of three channels of plain image, Lower row, Histograms of three channels for ciphered image.

The consistency of ciphered image is tested through calculating the variance of histograms. The evenness of histograms is displayed through the closeness of variance values of two encrypted images produced by a little different key sets. This concept is illustrated in Table 6 for ciphered images of Lena, Vegetables, and Panda. In Table 6, variances for first column are prepared with the help of initial secret key sets, whereas variances in other columns are achieved via simply changing one of the secret key of γ_0, correspondingly. The variance

TABLE 5. Difference of Plain and Decrypted 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	γ_8
γ_0	0	99.6175	99.6109	99.6017	99.6211	99.5977	99.6175	99.6073	99.6145
γ_1	99.6063	0	99.6089	99.6251	99.5875	99.6063	99.5992	99.5916	99.6175
γ_2	99.6267	99.6165	0	99.5951	99.5794	99.6007	99.6150	99.5946	99.6170
γ_3	99.5753	99.6170	99.6089	0	99.6033	99.6094	99.6160	99.6104	99.6246
γ_4	99.6078	99.5992	99.5956	99.6109	0	99.6078	99.6119	99.6155	99.6028
γ_5	99.6048	99.5967	99.5885	99.5982	99.5982	0	99.6114	99.6114	99.6073
γ_6	99.6490	99.5931	99.6216	99.6002	99.6119	99.6114	0	99.6145	99.6424
γ_7	99.6073	99.6175	99.5946	99.6104	99.6155	99.6114	99.6145	0	99.6134
γ_8	99.6145	99.5916	99.6170	99.6246	99.6028	99.6073	99.6424	99.6134	0
Avg.	**99.6115**	**99.6061**	**99.6058**	**99.6083**	**99.6024**	**99.6065**	**99.6160**	**99.6073**	**99.6174**

TABLE 6. 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
Lena	5464.1291	5461.8595	5456.9325	5464.5805	5468.0397	5467.8610	5463.4146	5451.0288	5455.3431
Vegetable	5465.9066	5459.7787	5454.2604	5463.0131	5468.0150	5463.6690	5462.2204	5458.8092	5462.1975
Panda	5452.8065	5465.8314	5469.0648	5458.0379	5456.7077	5455.4785	5462.6394	5468.2224	5469.2419
Avg.	**5460.9470**	**5462.490**	**5460.0860**	**5461.8770**	**5464.2540**	**5462.3360**	**5462.7580**	**5459.3530**	**5462.2610**
Ref. [10]	5463.7930	5461.8340	3652.8720	5456.6600	5468.1730	5459.9780	5475.6740	5456.5800	5470.5670
Ref. [14]	5464.4630	5473.1795	5465.8971	5458.3007	5458.3007	5458.3934	5465.781	5466.2373	5468.3108

TABLE 7. Percentage of variance of histogram for the cipher images.

Technique	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
Lena	0.04	0.13	0.008	0.07	0.07	0.01	0.23	0.16
Vegetable	0.11	0.21	0.05	0.04	0.04	0.07	0.13	0.11
Panda	0.24	0.30	0.09	0.07	0.05	0.18	0.28	0.24
Avg.	**0.13**	**0.21**	**0.05**	**0.06**	**0.05**	**0.09**	**0.21**	**0.17**
Ref. [10]	0.10	0.30	0.30	0.23	0.22	0.26	0.22	0.20
Ref. [14]	0.16	0.14	0.26	0.12	0.18	0.16	0.17	0.15

TABLE 8. Analysis of Chi-square results.

Image	Plain			Proposed			Ref. [10]		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	75994.46	31563.71	95867.65	261.41	240.47	265.03	338.80	304.07	354.82
Vegetables	31058.60	16590.25	95772.59	290.32	264.22	209.87	1597.93	1594.37	1632.41
Panda	40982.13	46124.86	22366.85	271.50	2.5337	255.85	898.23	933.79	862.91
Avg.	**49345.06**	**31426.27**	**71335.69**	**274.41**	**169.07**	**243.58**	**944.98**	**944.08**	**950.05**

of histogram are listed in Table 6 while the percentage of variances is mentioned in Table 7. The average change of variance for the proposed system is 0.21%, which is lower than the scheme in Refs. [10], [14] which were 0.30% and 0.26% respectively.

2) CHI-SQUARE TEST

The histogram of a digital image depicts the frequency for every gray level which shows the level of uniform distribution. This can also measured by Chi-square test and defined as follows,

$$\chi^2 = \sum_{k=1}^{256} \frac{(v_k - 256)^2}{256} \tag{22}$$

In Equation (22), v_k are the observed frequencies of each gray level $(0 - 255)$. The lower value of the chi-square shows the enhanced uniformity. The chi-square values are computed for Lena, Panda and Vegetables and are lower than Ref. [10] shown in Table 8. The proposed system has passed the test successfully for critical level $\alpha = 0.05$, Chi-square reported the values for all the channels of different plain/cipher images, should not be greater than 295.25. Our proposed system has better χ^2 and on an average only 3.5 images have χ^2 greater than 295.25 depicted results in Table 9.

3) CORRELATION COEFFICIENT

The color digital image contains a stronger correlation not only in adjacent pixels but also it has a strong correlation between the three channels. Moreover, images are composed of different regions to depict visual information. The pixels of a region have the similar gray intensity and the objective of the cryptography is to break this correlation to dismantle such regions. To measure the correlation in adjacent pixels, the Equation 23 is used, here ρ_{xy} is the correlation coefficient and its value varies from $+1$ to -1. The correlation is considered strong if the coefficient score is closer to $+1$ and weak if the coefficient score is closer to -1. The results for

TABLE 9. Chi-square results for below critical level $\alpha = 0.05$.

Image	Mean χ^2			$\chi^2 > 295.25$		
	Red	Green	Blue	Red	Green	Blue
Lena	256.1278	255.8259	257.1185	3	3	5
Panda	255.7910	253.4655	253.2714	3	4	4
Vegetables	257.7026	252.6147	256.9827	5	5	2
Goat	256.2216	251.5923	251.6307	5	1	2
Avg.	**256.4608**	**253.3746**	**254.7508**	**4**	**3.25**	**3.25**
Avg. of all		**254.8621**			**3.5**	

TABLE 10. Adjacent correlation analysis between R, G and B channels of plain and ciphered image.

Image Directions	Red Horizontal	Red Vertical	Red Diagonal	Green Horizontal	Green Vertical	Green Diagonal	Blue Horizontal	Blue Vertical	Blue Diagonal
Plain	0.9568	0.9733	0.9564	0.9475	0.9685	0.9461	0.9266	00.9504	0.9134
Encrypted	-0.0412	-0.0376	0.0075	0.0020	-0.0013	-0.0046	0.0071	-0.0423	-0.0009
Ref. [10]	-0.0073	0.0010	-0.0013	0.0011	-0.0020	0.0078	-0.0061	0.0058	-0.0003
Ref. [11]	0.01441	0.00831	-0.04678	0.0163	-0.0180	0.0427	-0.0838	-0.01869	-0.00845
Ref. [12]	0.03562	0.01275	0.0783	0.0763	0.00673	0.0562	0.0012	0.00983	0.00582
Ref. [19]	0.00022	0.0001	0.00015	0.00024	0.00056	0.00086	0.00054	0.00063	0.0015
Ref. [14]		-0.0084			0.0004			-0.0015	
Ref. [16]		-0.0097			-0.0087			0.0065	
Ref. [17]		0.0016			0.0017			0.0003	
Ref. [18]		-0.0064			0.0107			0.0051	
Ref. [20]		0.0024			0.0029			0.0021	

TABLE 11. Correlation coefficient analysis in all directions of Lena.

Channel	Plain Image			Ciphered Image		
	Red-Green	Red-Blue	Green-Blue	Red-Green	Red-Blue	Green-Blue
Lena	0.8813	0.6849	0.9181	-0.0030	-0.0021	-0.0010
Girl	0.8104	0.6788	0.9447	-0.0001	0.0043	0.0012
White	-	-	-	0.0061	0.0086	-0.0005
Black	-	-	-	0.0076	-0.0011	-0.0072

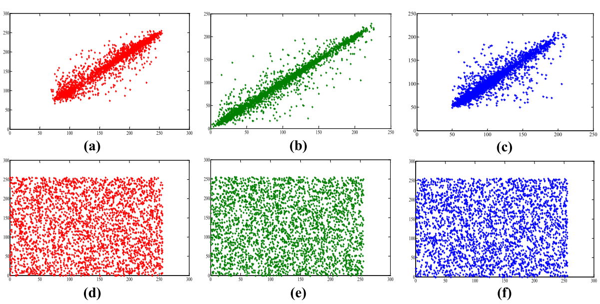

FIGURE 8. Correlation analysis of Lena image; (a) - (c) Horizontal (Red), Diagonal (Blue) and Vertical (Green) directions of Plain image; (d)-(e) Horizontal (Red), Diagonal (Blue) and Vertical (Green) directions of ciphered image.

correlation in three directions known as Horizontal, Vertical, and diagonal are measured by randomly selecting 3000 pairs in all directions. In Table 10 the results are given. So, it can be observed that the proposed scheme has better correlation coefficient for encrypted images than that of given in Refs. [10]–[12], [14], [16]–[20]. The correlations for plain and ciphered images are shown in Figure 8 in which 8(a) to 8(c) denote the plain image and Figure 8(d) to Figure 8(f) show correlations of ciphered images.

$$\rho_{xy} = \frac{|Cov\,(x, y)\,|}{\sqrt{D(x) \times D(y)}} \tag{23}$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\,(y_i - E(y)) \tag{24}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{25}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{26}$$

In Equation (23); x, y, and $D(x)$, $cov(x, y)$ represent gray values, mean and variance values of two adjacent pixels respectively. The correlation between these two color channels are measured and shown in Table 11 and one can observe that correlations between Red-Green, Red-Blue and Green-Blue are close to 0 for different images.

4) PEAK SIGNAL TO NOISE RATIO (PSNR)

The following Equation is used to compute the PSNR score between plain and ciphered image,

$$PSNR(P, C) = 10 \times \log 10 \frac{255^2 \times M \times N}{\sum_{\forall i,j} C(i, j) - P(i, j)} dB \tag{27}$$

where M and N are the size of an image, P and C represent plain and cipher images respectively. The PSNR results of proposed system are shown in Table 12 and proposed scheme

TABLE 12. PSNR analysis in all directions of Lena.

	Lena			Baboon		
	Red	Green	Blue	Red	Green	Blue
Proposed	7.8882	8.6081	9.6660	8.9588	9.4883	8.5673
Ref. [10]	7.8720	8.5687	9.6748	8.9350	9.4984	8.5642
Ref. [11]	10.3684	10.5925	11.9237	11.3713	11.7247	11.7247
Ref. [12]	11.5673	11.7893	11.6543	12.0014	12.4322	12.2849

TABLE 13. Entropy analysis for different images.

Technique	Image	Plain Image			Cipher Image		
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	7.2417	7.5767	6.9170	7.9982	7.9972	7.9974
	Vegetables	7.8277	7.8245	7.3598	7.9972	7.9976	7.9977
	Panda	7.7335	7.6452	7.7969	7.9981	7.9973	7.9974
	Goat	7.2804	7.2596	7.1626	7.9984	7.9975	7.9978
	Peppers	7.3388	7.4962	7.0583	7.9972	7.9976	7.9975
	Baboon	7.6051	7.3574	7.6662	7.9974	7.9971	7.9971
	Avg.	**7.5045**	**7.5266**	**7.3268**	**7.9977**	**7.9974**	**7.9975**
Ref. [10]	Lena	7.2417	7.5767	6.9170	7.9966	7.9972	7.9967
	Vegetables	7.8277	7.8245	7.3598	7.9848	7.9846	7.9835
	Panda	7.7335	7.6452	7.7969	7.9903	7.9902	7.9903
	Goat	7.2804	7.2596	7.1626	7.9970	7.9970	7.9970
	Peppers	7.3388	7.4962	7.0583	7.9910	7.9918	7.9905
	Avg.	**7.4844**	**7.5604**	**7.2589**	**7.9919**	**7.9922**	**7.9916**
Ref. [12]	Lena	-	-	-	7.9928	7.9912	7.9928
	Baboon	-	-	-	7.9945	7.9920	7.9932
	Avg.	-	-	-	**7.9936**	**7.9916**	**7.9930**
Ref. [14]	Lena	7.2933	7.5812	7.0856	7.9893	7.9896	7.9803
	Vegetables	7.7971	7.8215	7.3539	7.9895	7.9895	7.9894
	Panda	7.7118	7.6278	7.7939	7.9894	7.9898	7.9897
	Goat	7.2804	7.2596	7.1627	7.9886	7.9894	7.9894
	Peppers	7.3319	7.5242	7.0793	7.9891	7.9890	7.9897
	Avg.	**7.4829**	**7.5629**	**7.2951**	**7.9892**	**7.9895**	**7.9877**

is comparatively better than the schemes given in Refs. [11] and [12].

5) INFORMATION ENTROPY

The objective of cryptography is to transform meaningful information into noise or randomness. The entropy is used to compute the noisy condition of a message. As each color channel is 8-bit image independently, the ideal entropy score of the encrypted channel should be closed to 8, and a higher score is better. The uniform distribution and cryptosystem will be stronger against statistical attack if entropy is higher. The Entropy is defined as:

$$H(s) = \sum_{i=0}^{L-1} p(s_i) log_2 \frac{1}{p(s_i)} \tag{28}$$

In Equation (28), L and p demonstrate gray level and probability of occurrence of any intensity L in image. The entropy score for non-identical images of size 256×256 are calculated and shown in Table 13. The average scores for each color channel of all images (plain and encrypted) are shown in bold characters and by value inspection proposed cipher has shown better performance than given in schemes [10], [12] and [14]. The information entropies for color Lena image of size 512×512 are in Table 14 which is comparably better than the scheme in Refs. [10] and [11].

$$H_{k,T_B}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{29}$$

The Equation (29) is used to measure the local distribution/randomness of encrypted image. The I and E are plain and encrypted images with L intensities. These images are split into k blocks that must be non-overlapped in which $E_1, \cdots, E_k$ are splitted blocks with T number of pixels in each block. The Equation (29) is used to compute the mean of local entropy of randomly selected k blocks. For the experiment, $K = 32$ and $T = 1936$ are used. As seen from Table 15, the average local Shannon entropy values of Red, Green and Blue components of the cipher image are more than 7.90 which is far better than Ref. [14]. Hence, the proposed system passed the local entropy test. The Ref. [14] has failed to pass the test.

D. DIFFERENTIAL ANALYSIS

Two famous researchers Biham and Shamir [73], [74] devised two metrics called Number of Changing Pixel Rate (NPCR) and Unified Averaged Changed Intensity (UACI) to evaluate the ciphers against differential attacks. The given Equations (30) and (31) provide the computational scores of NPCR and UACI among two encrypted images generated

TABLE 14. Comparison of entropy for Lena (512 × 512).

Algorithm	Plain Image			Cipher Image		
	Red	Green	Blue	Red	Green	Blue
Proposed	7.2531	7.5940	6.9684	7.9993	7.9994	7.9993
Ref. [10]	7.2531	7.5940	6.9684	7.9990	7.9982	7.9990
Ref. [11]	-	-	-	7.9962	7.9993	7.9995
Ref. [16]	7.2531	7.5940	6.9684	7.9994	7.9992	7.9993
Ref. [17]		7.4456			7.9993	
Ref. [18]		7.4767			7.9997	

TABLE 15. Comparison of local entropy values for Lena (512 × 512).

Algorithm	Proposed			Ref. [14]		
	Red	Green	Blue	Red	Green	Blue
Lena	7.9045	7.9069	7.9012	7.7885	7.7895	7.7886
Vegetables	7.9035	7.9020	7.9047	7.8991	7.9010	7.9001
Panda	7.9013	7.9046	7.9023	7.8948	7.8974	7.8947
Goat	7.9032	7.9030	7.9020	7.9029	7.9018	7.9008
Avg.	**7.9031**	**7.9041**	**7.9025**	**7.8713**	**7.8724**	**7.8710**

TABLE 16. comparison of NPCR scores for Lena and Baboon.

Algorithm	Lena				Baboon			
	Red	Green	Blue	**Avg.**	Red	Green	Blue	**Avg.**
Proposed	99.5788	99.6155	99.6445	**99.6129**	99.6478	99.6429	99.6317	**99.6408**
Ref. [10]	99.6001	99.5998	99.5997	**99.5999**	99.6099	99.6058	99.5956	**99.6038**
Ref. [11]	99.6586	99.5409	99.6697	**99.6231**	99.7350	99.5940	99.6541	**99.6610**
Ref. [12]	99.3218	99.2945	89.3027	**95.9730**	99.1689	99.2749	99.2321	**99.2253**
Ref. [16]	99.61	99.62	99.61	**99.6133**	99.62	99.62	99.63	**99.6233**
Ref. [17]	99.61	99.61	99.61	**99.6100**	-	-	-	**99.61**
Ref. [18]	99.61	99.61	99.61	**99.6100**	99.62	99.62	99.6	**99.62**
Ref. [19]	-	-	-	**99.6831**	-	-	-	-
Ref. [20]	-	-	-	**99.6139**	-	-	-	-

TABLE 17. Comparison of UACI scores for Lena and Baboon.

Algorithm	Lena				Baboon			
	Red	Green	Blue	**Avg.**	Red	Green	Blue	Avg.
Proposed	33.4664	33.6457	33.5748	**33.5623**	33.4796	33.5731	33.4532	**33.5020**
Ref. [10]	33.3575	33.4287	33.3683	**33.3848**	33.3743	33.3829	33.5604	**33.4392**
Ref. [11]	33.1154	33.9966	33.8975	**33.6698**	33.3521	33.6231	33.9012	**33.6255**
Ref. [12]	31.2189	31.4183	31.3621	**31.3331**	31.3438	31.2473	31.2956	**31.2956**
Ref. [16]	33.42	33.53	33.54	**33.4966**	33.52	33.46	33.42	**33.4667**
Ref. [17]	-	-	-	**33.5200**	-	-	-	**33.50**
Ref. [18]	32.23	33.96	34.35	**33.5133**	33.46	32.22	34.23	**33.3033**
Ref. [19]	-	-	-	**33.4412**	-	-	-	-
Ref. [20]	-	-	-	**32.6602**	-	-	-	-

from two plain images differ in one bit only.

$$N(E^1, E^2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{M \times N} \times 100\% \tag{30}$$

$$U(E^1, E^2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C^1(i,j) - C^2(i,j)\right|}{L \bullet M \times N}100\% \tag{31}$$

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,

$$D(i,j) = \begin{cases} 0, & if\ E^1(i,j) = E^2(i,j) \\ 1, & if\ E^1(i,j) \neq E^2(i,j) \end{cases} \tag{32}$$

The NPCR and UACI results of three channels of Lena and Baboon are computed and recorded in Tables 16 and 17. The average NPCR scores of Lena and Baboon are NPCR>0.9961, NPCR>0.9964 respectively which is good enough to resist the differential attack. Similarly, the average UACI score of Lena and Baboon are UACI>0.3356 and UACI>0.3350. To assess the sensitivity of the plaintext in depth, one hundred and fifty encrypted images are produced for different plain images by changing one pixel by 1 bit only at a time using same secret key set γ_0. The results are compiled in Tables 18 and 19 for 150 encrypted images and boldface scores represents average values of 150 images. In the next step, an image with zero information is shown in Figure 9(a) and its encrypted result is displayed in Figure 9(c). To measure the NPCR and UACI scores, a single

TABLE 18. Average NPCR for three colored channels of Plaintext sensitivity 150 image.

Images	Proposed System			Ref. [14]			Ref. [10]		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	99.6107	99.6060	99.6131	99.6100	99.6092	99.6099	99.6078	99.6088	99.6081
Panda	99.6088	99.6130	99.6073	99.6132	99.6041	99.6093	99.6084	99.6087	99.6099
Vegetables	99.6105	99.6074	99.6114	99.6089	99.6093	99.6083	99.6193	99.6090	99.6102
Goat	99.6067	99.6108	99.6092	99.6128	99.6123	99.6165	99.6091	99.6129	99.6086
Peppers	99.6090	99.6099	99.6080	99.6083	99.6075	99.6094	99.6081	99.6096	99.6143
Avg.	**99.6091**	**99.6094**	**99.6098**	**99.6107**	**99.6085**	**99.6107**	**99.6105**	**99.6098**	**99.6102**
Avg.of all		**99.6094**			**99.6099**			**99.6101**	

TABLE 19. Average UACI for three colored channels of Plaintext sensitivity 150 image.

Images	Proposed System			Ref. [14]			Ref. [10]		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	33.4754	33.4485	33.4915	33.4639	33.5042	33.4776	33.4291	33.4252	33.4219
Panda	33.4730	33.4671	33.4525	33.4627	33.4704	33.5041	33.5030	33.4973	33.4920
Vegetables	33.4369	33.4018	33.5314	33.4860	33.4433	33.4546	33.5106	33.5011	33.5096
Goat	33.4272	33.5438	33.5419	33.4854	33.4434	33.4148	33.4234	33.4307	33.4247
Peppers	33.4618	33.4738	33.4335	33.4939	33.4295	33.4856	33.4256	33.4255	33.4217
Avg.	**33.4549**	**33.4670**	**33.4902**	**33.4784**	**33.4552**	**33.4673**	**33.4583**	**33.4560**	**33.45398**
Avg. of all		**33.4707**			**33.4680**			**33.4561**	

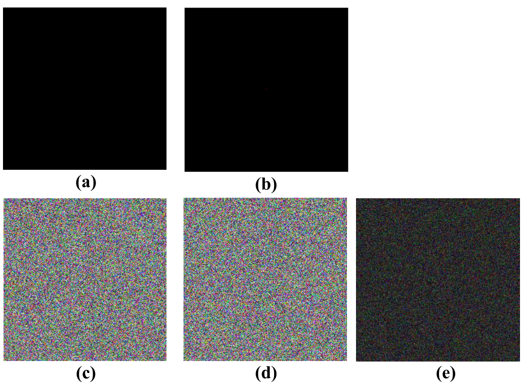

FIGURE 9. Zero information image; (b) 1-bit different image from (a); (c) Ciphered image of (a); (d) Ciphered image of (b); (e) Differences of (c) and (d) image.

pixel is changed from zero to 255 represented in Figure 9(b) and its encrypted result is shown in Figure 9(d). The scores for NPCR, UACI, Variance, and Chi-Square are computed for the black and white images shown in Table 20. The proposed scheme has comparatively better results than that Ref. [16]. The difference in Figure 9(c) and 9(d) is displayed in Figure 9(e).

At last, we have estimated the critical value test for NPCR and UACI. For this purpose, Lena image is used to generate 100 encrypted images by supplying 1-bit different plain image to the proposed algorithm. The critical NPCR value of $\alpha_{0.001}$, $\alpha_{0.01}$ and $\alpha_{0.05}$ are 99.5341, 99.5527 and 99.5693, respectively. In our test, not a single encrypted image out of 100 has NPCR score lower than 99.5341(%), 99.5527(%) or 99.5693(%). This fact is shown in Figure 10(a). The critical UACI value has upper and lower bound for $\alpha_{0.001}$, $\alpha_{0.01}$ and $\alpha_{0.05}$. The UACI critical scores are 33.1596(%) and 33.7677(%) for lower and upper bounds respectively under $\alpha_{0.001}$ while 33.2255(%) and 33.7016(%) are for $\alpha_{0.01}$. Similarly, for $\alpha_{0.05}$, the critical scores boundary lie within 33.2824(%) and 33.6447(%). The UACI scores for 100 encrypted lie within the upper and lower bounds for different critical level $\alpha_{0.001}$, $\alpha_{0.01}$ and $\alpha_{0.05}$ shown in 10(b).

V. ROBUSTNESS AGAINST NOISE ATTACKS

This section discusses the robustness of common noises caused by the physical communication channel. A significant change in the encrypted image can result in failure to decrypt the image [75], which states that an error even in a single pixel and the original image is lost. The preferred way to test robustness is to compute the loss in encrypted image, Gaussian noise, Salt & Pepper noise, Histogram Equalization, and Contrast enhancement to confirm the strength and robustness of the proposed system.

A. CROPPING

During the internet communication, any part of image can be vanished. For this kind of serious threat the proposed cipher must be capable enough to the deciphering of lossy image in a proper way. For such validation an encrypted Lena image of size $512 \times 512 \times 3$ is used, $64 \times 64 \times 3$ or 1.65%, $128\times128\times3$ or 6.25%, $256\times256\times3$ or 25% and $256\times512\times3$ or 50% of image data have been removed which displayed in Figure 11(a) to 11(d) respectively. These lossy images are deciphered using the scheme given in Ref. [16], results are displayed in Figure 11(e) to 11(h). The results of deciphering by the proposed scheme are displayed in Figure 11(i) to Figure 11(l). The recovered images still have plain image information. This proves the toughness of the proposed cipher against the lossy attacks.

B. HISTOGRAM ATTACK

The histogram attack means that Equalization process is applied on the histogram on an image. The histogram

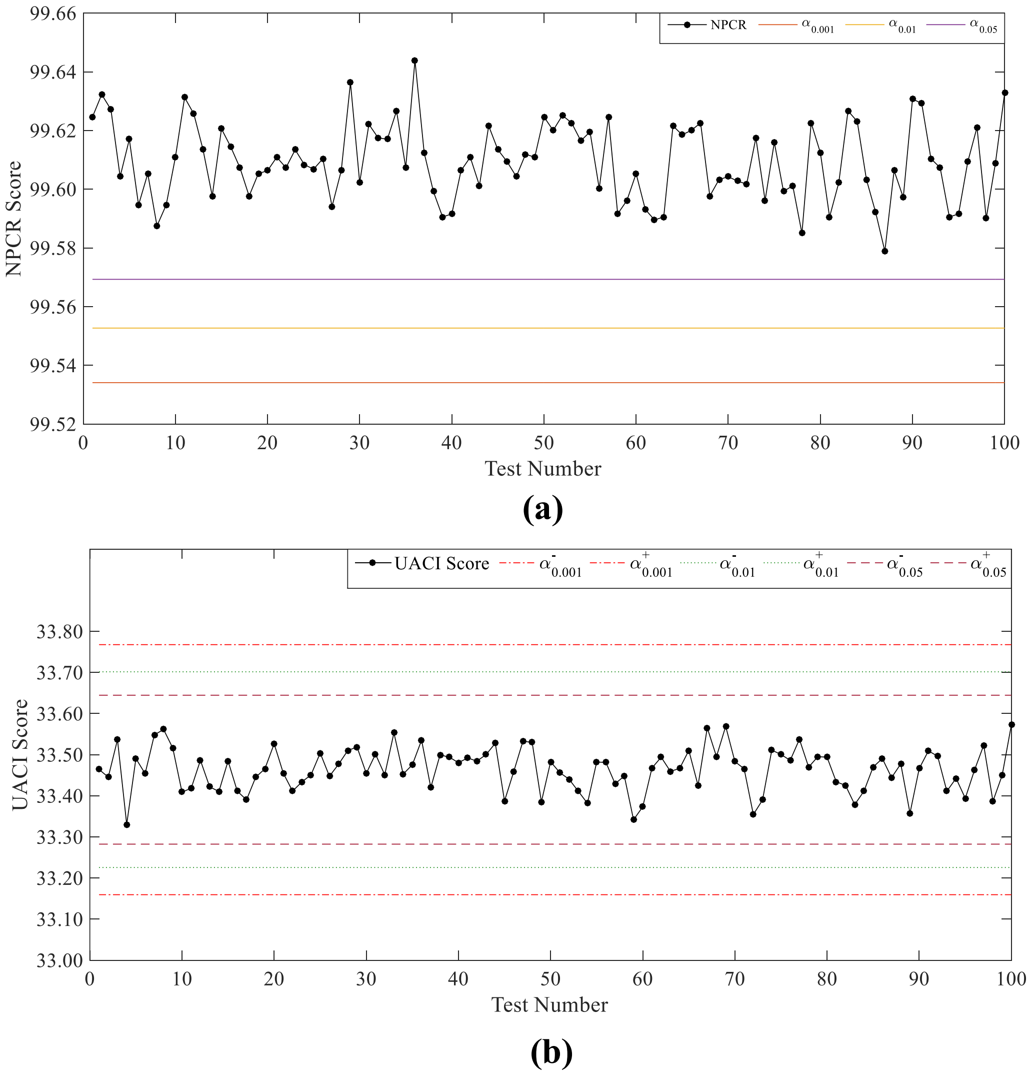

FIGURE 10. Estimated critical NPCR and UACI test for 100 encrypted images.

TABLE 20. Correlation, NPCR and UACI of two ciphered images vary in one pixel for Black and white.

Algorithm	Image	Test	Plain Image			Cipher Image			-
			Red	Green	Blue	Red	Green	Blue	**Avg.**
Proposed	Black	NPCR	0.000003	0	0	99.6117	99.6212	99.6071	**99.61**
		UACI	0.000003	0	0	33.4672	33.4277	33.3983	**33.43**
		Variance	268,435,456	268,435,456	268,435,456	989.22	966.15	1035.71	**997.02**
		Chi-Square	66,846,720	66,846,720	66,846,720	246.33	240.60	257.92	**248.28**
	White	NPCR	0	0.000003	0	99.5827	99.6136	99.6063	**99.60**
		UACI	0	0.000003	0	33.4624	33.5294	33.3905	**33.46**
		Variance	268,435,456	268,435,456	268,435,456	1103.72	1055.70	1105.89	**1088.40**
		Chi-Square	66,846,720	66,846,720	66,846,720	274.85	262.89	275.39	**271.04**
Ref. [16]	Black	NPCR	0	0	0	99.61	99.58	99.60	**99.60**
		UACI	-	-	-	33.45	33.39	33.40	**33.41**
		Variance	267,386,880	267,386,880	267,386,880	1089.4	1163.5	1076.2	**1109.73**
		Chi-Square	66,846,720	66,846,720	66,846,720	272.34	290.88	269.05	**277.42**
	White	NPCR	-	-	-	99.61	99.62	99.63	**99.61**
		UACI	-	-	-	33.37	33.47	33.42	**33.42**
		Variance	267,386,880	267,386,880	267,386,880	993.58	1085.4	1040.8	**1039.93**
		Chi-Square	66,846,720	66,846,720	66,846,720	248.39	271.33	260.18	**259.97**

Equalization change the intensity of each pixel and new image contains different gray levels with almost equal frequency. In this article, histogram Equalization is applied on Figure 5(f) that is displayed in Figure 12(a) and recovered image is presented in Figure 12(b). This technique is also applied to encrypted images of Lena, Panda, and

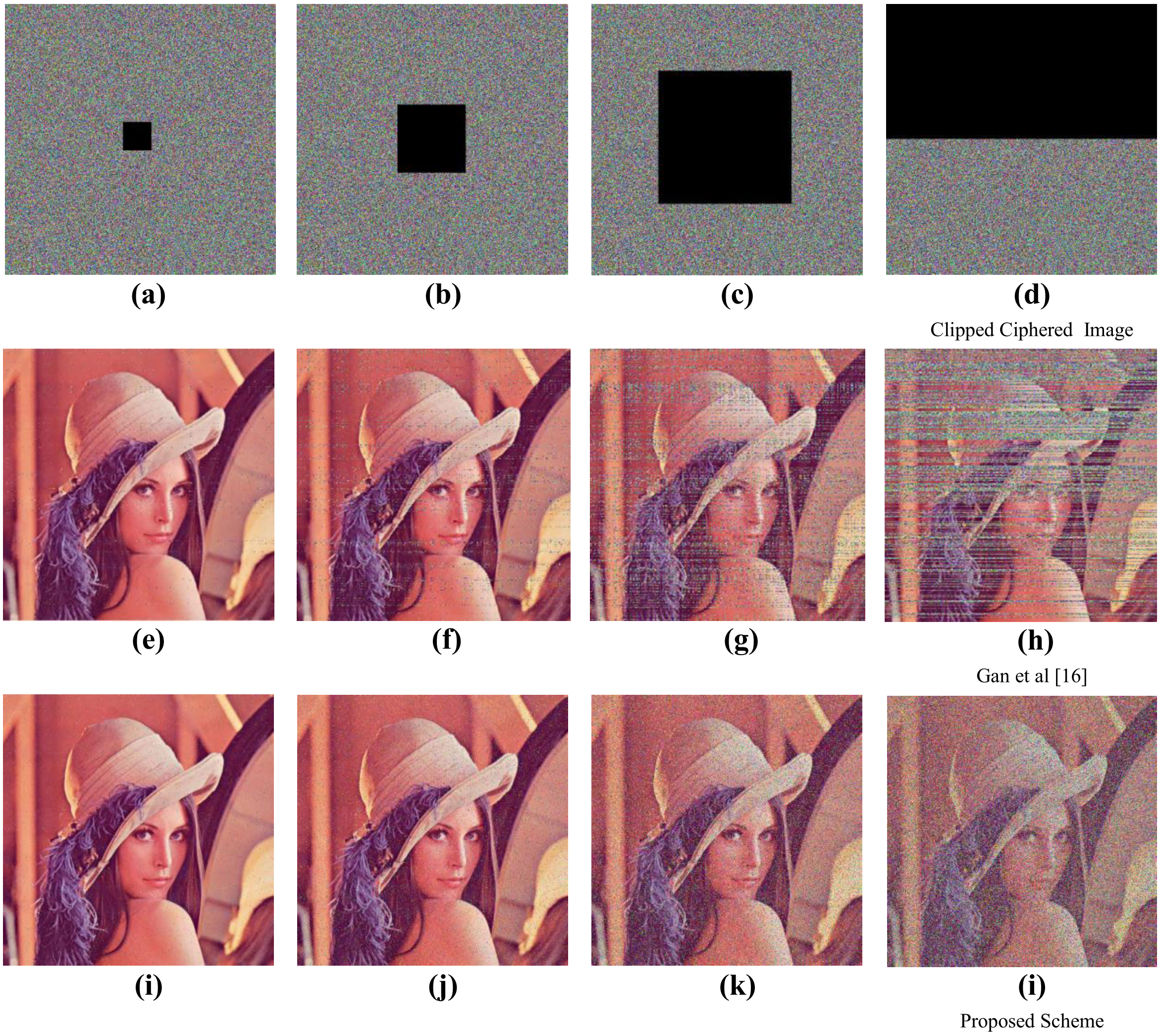

FIGURE 11. Robustness against cropping attack.

TABLE 21. PSNR values for Histogram Equalization attack for different number of rotations.

Images	β_1	β_2	β_3	β_4	β_5	β_6	**Avg.**	Ref. [14]
Lena	30.55	36.93	36.37	32.49	32.70	36.12	**34.19**	-
Vegetable	27.80	33.41	35.48	31.39	35.91	31.69	**32.61**	-
Panda	41.38	30.31	36.81	36.21	28.35	30.54	**33.93**	32.42
Avg. of all	33.24	33.55	36.22	33.36	32.32	32.78	**33.58**	-

Peppers under different value β shown in Table 21 with the average value for each image. The PSNR value in Figure 5(c) and 12(b) of Panda under $\beta = 3$ is 36.81dB as shown in Table 21 which is far better than Ref. [14]. The average PSNR of the image is 33.65 which is also better than Ref. [14]. Therefore, the result declare that the offered scheme can defend the histogram equalization attack.

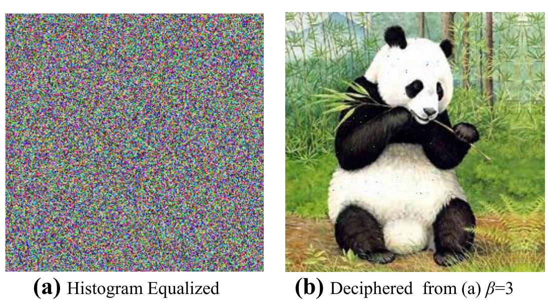

FIGURE 12. Histogram Equalization analysis: (a) Ciphered image histogram equalized; (b) Deciphered Panda image from (a).

C. NOISE ADDITION

In the real and the digital world scenario noise accumulation definitely occurs. This noise lowers the image quality and affect the visual information of digital images. In the simulation, the assumption is made that ciphered Panda image shown in Figure 5(f) is contaminated with the Gaussian noise under different variances of 0.002, 0.05 and 0.3. The recovered images under the Gaussian noise shown in Figure 13(a) to Figure 13(c) and have a strong visual effect and the

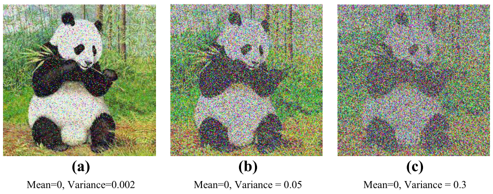

FIGURE 13. Recovered Panda images using Gaussian noise with different variances.

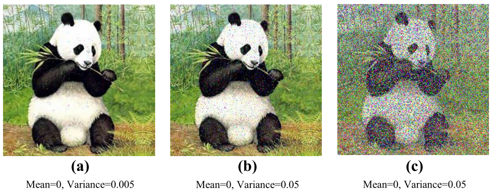

FIGURE 14. Ciphered and Deciphered Panda images under Salt & Pepper noise with different variances.

recovered image is still clearly visible. In the similar fashion, Salt & Pepper noise is used to disturb encrypted image given in Figure 5(f) with densities 0.005, 0.05 and 0.5. The recovered images under Salt & Pepper noise attack are demonstrated in Figure 14(a) to 14(c). In Table 22, the PSNR results

TABLE 22. comparison of noise robustness for Panda image.

Noise attacks	Parameters	Proposed	Ref. [10]	Ref. [14]
Salt & Pepper	0.005	31.023	30.87	30.50
	0.050	20.92	20.77	20.73
	0.500	10.98	10.79	10.75
Gaussian	[0, 0.002]	16.415	16.15	16.36
	[0, 0.050]	10.989	10.81	10.98
	[0, 0.300]	09.660	9.57	09.19
Contrast Adjustment	70%	14.948	13.97	14.39
	30%	12.423	11.25	11.51
Histogram Eq.	-	36.81	33.23	32.42

are listed that proves the robustness of proposed scheme as compared to Refs. [10], [14] for the Gaussian noise in terms of value comparison.

After this, Gaussian noise with mean=0 and variances 0.00001, lower 0.00003, 0.00005 and 0.0001 are added to image given in Figure 5(d). The visual results are displayed in Figure 15(a) to Figure 15(d). The corresponding deciphered images in comparison to Ref. [16] are shown in Figure 15(e) to Figure15(h). The deciphered images of the proposed scheme are displayed in Figure 15(i) to Figure 15(l).

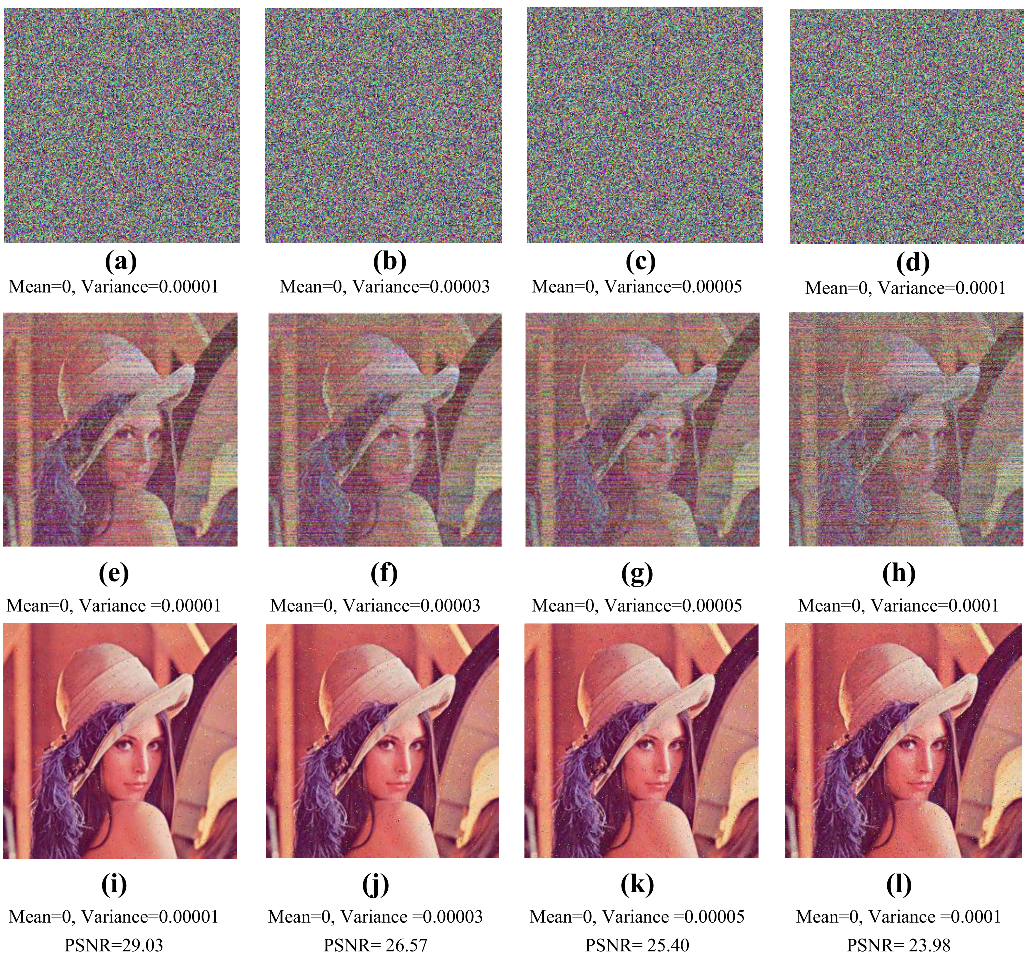

FIGURE 15. Comparison of robustness against Gaussian noise; (e)-(h) recovered images using Ref. [16]; (i)-(l)recovered images using Proposed method.

TABLE 23. Comparison of MSE, PSNR NPCR and UACI for Lena image.

Gaussian	Proposed System				Ref. [10]				Ref. [76]				Ref. [29]	
	MSE	PSNR	NPCR	UACI	MSE	PSNR	NPCR	UACI	MSE	PSNR	NPCR	UACI	NPCR	UACI
0.0001	261.35	23.98	84.27	2.45	399.16	22.13	86.90	3.3	81.26	29.03	87.7	17.3	99.20	28.44
0.0003	443.49	21.69	90.63	3.75	671.71	19.88	92.32	4.9	92.08	28.48	93.3	20.3	99.61	28.64
0.0005	578.82	20.54	92.60	4.51	843.97	18.88	94.09	5.9	95.70	28.32	94.9	21.5	99.74	28.84

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	Noise
		$H_{R,G,B}$	$V_{R,G,B}$	$D_{R,G,B}$					
Proposed (Chen)	10^{232}	-0.0238	-0.0013	0.0006	7.9976	99.6129	33.5623	1.07	Yes
Proposed (SSS)	10^{220}	-0.0005	-0.0111	-0.0013	7.9974	99.6037	33.5265	0.08	Yes
Ref. [10]	10^{94}	-0.0025	0.0023	-0.0002	7.9968	99.5999	33.3848	1.44	Yes
Ref. [11]	10^{230}	-0.0080	0.0136	-0.0370	7.9983	99.6231	33.6698	-	No
Ref. [12]	10^{70}	0.0422	0.0464	0.0056	7.9923	95.9730	31.3331	-	No
Ref. [14]	10^{90}	-0.0084	0.0004	0.0015	7.9864	99.6097	33.4819	-	Yes
Ref. [16]	$10^{148.41}$	-0.0097	-0.0087	0.0065	7.9970	99.60	33.44	5.35	Yes
Ref. [17]	4×10^{130}	0.0016	0.0017	0.0003	7.9975	99.6100	33.52	1.02	No
Ref. [18]	$10^{77.06}$	-0.0064	0.0107	0.0051	-	99.61	33.5133	0.82	No
Ref. [19]	$10^{38.53}$	0.0002	0.0006	0.0009	7.9973	99.6831	32.6602	0.17	No
Ref. [20]	$10^{38.53}$	0.0024	0.0029	0.0021	7.8679	99.6139	33.4412	0.76	No
Ref. [77]	10^{169}	-0.0065	0.0006	0.0054	7.9930	99.61	33.46	-	No
Ref. [78]	$10^{38.53}$	-0.0040	-0.0244	0.0072	7.9967	99.65	33.59	4.97	No
Ref. [79]	4×10^{118}	0.0024	0.0058	0.0170	7.9870	99.60	33.89	-	No
Ref. [85]	10^{240}	-0.0068	-	-	7.9973	99.61	33.49	1.44	Yes

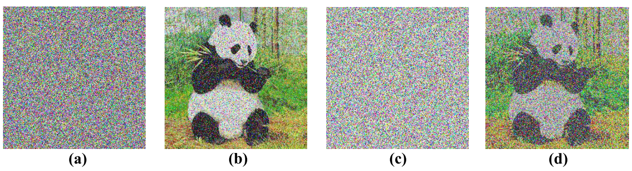

FIGURE 16. Robustness against contrast attack.

It is obvious from the results that the recovered images using the proposed scheme are far better in visual quality than that of the previous scheme in Ref. [16]. In Table 23, the MSE, PSNR, NPCR, UACI are computed between plain Lena and recovered image with Gaussian noises for densities 0.0001, 0.0003 and 0.0005. The proposed scheme is also better in NPCR and UACI as compared to other schemes [10], [29], [76] but it is lower in PSNR than that of Ref. [76].

D. CONTRAST ADJUSTMENT

The contrast adjustment is a basic image processing term to improve the level of viewing an image. This contrast enhancement is employed to the encrypted image of Panda shown in Figure 16(f) of two different levels, 70% and 30% where the substandard value shows the higher contrasts. These enhanced and encrypted images are displayed in Figure 16(a) and Figure 16(c) and corresponding decrypted images are shown in Figure 16(b) and Figure 16(d). After that the Peak Signal to Noise (PSNR) is also calculated for decrypted and original Panda images are 14.95dB and 12.42dB. For PSNR the proposed scheme is better than other the schemes in Refs. [10], [14], the comparison is given in Table 22. Therefore, the proposed system is robust against contrast adjustment attacks as well.

VI. EFFICIENT VERSION

A new chaotic map called Sine-Sine system proposed by C. Pak in [22] that is $x_{n+1} = F_{chaos}(\mu, x_n) \times 2^k - floor\,(F_{chaos}(\mu, x_n))$ in which $F_{chaos}(\mu, x_n)$ is the 1D logistic map. The new system is chaotic for $\mu \in (0, 10)$ and $k \in (8, 20)$ which produced the pseudo-random sequence $x_n \in (0-1)$. This chaotic map is highly efficient as compared to Chen system to generate values for the rotation of rotors. It has improved the efficiency greatly without compromising the results but to get angles between -360^0 to 360^0. A little modification is required to incorporate this in the proposed scheme. This modification is mentioned below, results are given in Table 24 with Chen and SSS system applied to Lena image. The comparison of results proves that the new system is better.

$$\begin{aligned}
&if\, x(n) > 0.5\\
&x(n) = \text{mod}\left(round\left(\left(x(n) - 1\right) \times 10^{14}\right)\right), 360\\
&else\\
&x(n) = \text{mod}\left(round\left(x(n) \times 10^{14}\right)\right), 360\\
&endif
\end{aligned} \tag{33}$$

VII. CONCLUSION

An innovative image encryption algorithm is proposed using the concept of rotor machines and chaotic maps. The rows and columns are combined to form rotors for each matrix of the color image and PWLCM used to build 2-dimensional matrices of pseudo-random numbers. These matrices are also transformed into rotors called pseudo rotors. A pseudo-rotor is rotated around an angle $+\theta$ or $-\theta$ and added to the rotor of plaintext. This process continue up to β times for the substitution of single rotor. The angle θ is obtained by Chen hyper chaotic system and one-time keys are generated using SHA-512 of the plain image that enables cryptosystem, to resist chosen plaintext attack. The experimental results show that the system is very strong against common attacks and quite better than some existing ciphers. It has higher NPCR, UACI,entropy and low Chi-Square scores. It has shown extreme resilient resistance against transmission impairments such as Gaussian, Salt & Pepper, clipping and histogram equalization that lacks in many existing systems. The replacement of Chen system with a 1-dimensional chaotic map called SSS which highly improves the efficiency without compromising the performance and security. The proposed scheme is also suitable for grey scale images.

REFERENCES

[1] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Process.*, vol. 93, no. 11, pp. 2986–3000, Nov. 2013.

[2] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena," *Signal Process.*, vol. 93, no. 5, pp. 1328–1340, May 2013.

[3] B. Schneier, "Applied cryptography: Protocols, algorithms, and source code in C," in *Network*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996, p. 631.

[4] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standar*. Berlin, Germany: Springer 2012.

[5] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "Discrete fractional wavelet transform and its application to multiple encryption," *Inf. Sci.*, vol. 223, pp. 297–316, Feb. 2013.

[6] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition," *Opt. Commun.*, vol. 285, no. 5, pp. 594–608, Mar. 2012.

[7] T.-H. Chen and C.-S. Wu, "Compression-unimpaired batch-image encryption combining vector quantization and index compression," *Inf. Sci.*, vol. 180, no. 9, pp. 1690–1701, May 2010.

[8] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-gray code for image systems," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 515–529, Apr. 2013.

[9] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "A hash-based image encryption algorithm," *Opt. Commun.*, vol. 283, no. 6, pp. 879–893, Mar. 2010.

[10] A. U. 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," *Int. J. Light Electron Opt.*, vol. 159, pp. 348–367, Jan. 2018.

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

[12] 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, Feb. 2012.

[13] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences," *Multimedia Tools Appl.*, vol. 75, no. 8, pp. 4363–4382, Apr. 2016.

[14] 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.

[15] M. Kumar and A. Vaish, "An efficient encryption-then-compression technique for encrypted images using SVD," *Digit. Signal Process.*, vol. 60, pp. 81–89, Jan. 2017.

[16] 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, Nov. 2019.

[17] 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, 2017.

[18] 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, Aug. 2018.

[19] 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.

[20] 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.

[21] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

[22] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26191–26217, Oct. 2018.

[23] 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.

[24] O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity," *Nonlinear Dyn.*, vol. 82, nos. 1–2, pp. 107–117, Oct. 2015.

[25] H.-I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Process.*, vol. 117, pp. 281–309, Dec. 2015.

[26] C. Jin and Z. Tu, "A novel color image encryption algorithm using chaotic map and improved RC4," in *Automation Control Theory Perspectives in Intelligent Systems. CSOC* (Advances in Intelligent Systems and Computing), vol. 466, R. Silhavy, R. Senkerik, Z. Oplatkova, P. Silhavy, and Z. Prokopova, Eds. Cham, Switzerland: Springer, 2016, doi: 10.1007/978-3-319-33389-2_1.

[27] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989.

[28] Z. Wang, X. Huang, N. Li, and X.-N. Song, "Image encryption based on a delayed fractional-order chaotic logistic system," *Chin. Phys. B*, vol. 21, no. 5, p. 50506, 2012.

[29] 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, May 2012.

[30] Y.-Q. Zhang and X.-Y. Wang, "Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice," *Phys. A, Stat. Mech. Appl.*, vol. 402, pp. 104–118, May 2014.

[31] 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.

[32] H. Liu, A. Kadir, and P. Gong, "A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise," *Opt. Commun.*, vol. 338, pp. 340–347, Mar. 2015.

[33] A. Firdous, A. ur Rehman, and M. M. Saad Missen, "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24809–24835, Sep. 2019.

[34] 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, May 2010.

[35] X. Wang, S. Wang, Y. Zhang, and C. Luo, "A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems," *Opt. Lasers Eng.*, vol. 103, pp. 1–8, Apr. 2018.

[36] I. Hussain, J. Ahmed, and A. Hussain, "An image encryption technique based on coupled map lattice and one-time S-Boxes based on complex chaotic system," *J. Intell. Fuzzy Syst.*, vol. 29, no. 4, pp. 1493–1500, Oct. 2015.

[37] A. V. Diaconu, V. Ionescu, and G. Iana, "A new bit-level permutation image encryption algorithm," in *Proc. Int. Conf. Commun.*, 2016, pp. 411–416.

[38] X. Chai, "An image encryption algorithm based on bit level Brownian motion and new chaotic systems," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1159–1175, Jan. 2017.

[39] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.

[40] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, "Substitution box generation using chaos: An image encryption application," *Appl. Math. Comput.*, vol. 332, pp. 123–135, Sep. 2018.

[41] U. Cavusoglu, S. Kacar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box, Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017.

[42] 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. 2017.

[43] I. Hussain, T. Shah, and M. A. Gondal, "Application of S-box and chaotic map for image encryption," *Math. Comput. Model.*, vol. 57, nos. 9–10, pp. 2576–2579, May 2013.
[44] I. Hussain, T. Shah, and M. A. Gondal, "Image encryption algorithm based on total shuffling scheme and chaotic S-box transformation," *J. Vib. Control*, vol. 20, no. 14, pp. 2133–2136, Oct. 2014.
[45] I. Hussain, "Optical image encryption based on S-box transformation and fractional Hartley transform," *J. Vib. Control*, vol. 22, no. 4, pp. 1143–1146, Mar. 2016.
[46] I. Hussain and M. A. Gondal, "An extended image encryption using chaotic coupled map and S-box transformation," *Nonlinear Dyn.*, vol. 76, no. 2, pp. 1355–1363, Apr. 2014.
[47] I. Hussain, T. Shah, and M. A. Gondal, "An efficient image encryption algorithm based on s8 S-box transformation and NCA map," *Opt. Commun.*, vol. 285, no. 24, pp. 4887–4890, Nov. 2012.
[48] Z. Liu, T. Xia, and J. Wang, "Image encryption technology based on fractional two-dimensional triangle function combination discrete chaotic map coupled with Menezes-Vanstone elliptic curve cryptosystem," *Discret. Dyn. Nat. Soc.*, vol. 2018, p. 24, Jan. 2018.
[49] A. A. A. El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools Appl.*, vol. 70, no. 3, pp. 1559–1584, Jun. 2014.
[50] A. A. Abd El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 136–143, Feb. 2013.
[51] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.
[52] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2943–2959, Jul. 2012.
[53] S.-J. Xu, X.-B. Chen, R. Zhang, Y.-X. Yang, and Y.-C. Guo, "An improved chaotic cryptosystem based on circular bit shift and XOR operations," *Phys. Lett. A*, vol. 376, nos. 10–11, pp. 1003–1010, Feb. 2012.
[54] 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.
[55] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognit. Lett.*, vol. 31, no. 5, pp. 347–354, Apr. 2010.
[56] D. Arroyo, J. Diaz, and F. B. Rodriguez, "Cryptanalysis of a one round chaos-based substitution permutation network," *Signal Process.*, vol. 93, no. 5, pp. 1358–1364, May 2013.
[57] M. I. Sobhy and A.-E.-R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, vol. 2, Jun. 2001, pp. 1001–1004.
[58] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3056–3075, 2009.
[59] Y. Liu, X. Tong, and J. Ma, "Image encryption algorithm based on hyper-chaotic system and dynamic S-box," *Multimedia Tools Appl.*, vol. 75, no. 13, pp. 7739–7759, Jul. 2016.
[60] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 38, pp. 5973–5978, Sep. 2008.
[61] X. Ge, F. Liu, B. Lu, and W. Wang, "Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version," *Phys. Lett. A*, vol. 375, no. 5, pp. 908–913, Jan. 2011.
[62] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 144, pp. 444–452, Mar. 2018.
[63] J. Chen, F. Han, W. Qian, Y.-D. Yao, and Z.-L. Zhu, "Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map," *Nonlinear Dyn.*, vol. 93, no. 4, pp. 2399–2413, Sep. 2018.
[64] H. Fan, M. Li, D. Liu, and E. Zhang, "Cryptanalysis of a colour image encryption using chaotic APFM nonlinear adaptive filter," *Signal Process.*, vol. 143, pp. 28–41, Feb. 2018.
[65] R. Rhouma, E. Solak, and S. Belghith, "Cryptanalysis of a new substitution–diffusion based image cipher," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 7, pp. 1887–1892, Jul. 2010.
[66] X. Zhang, W. Nie, Y. Ma, and Q. Tian, "Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box," *Multimedia Tools Appl.*, vol. 76, no. 14, pp. 15641–15659, Jul. 2017.
[67] K. de Leeuw, "The Dutch invention of the rotor machine, 1915–1923," *Cryptologia*, vol. 27, no. 1, pp. 73–94, Jan. 2003.
[68] A. D. Cipher and L. Kruh, *Machine Cryptography and Modern Cryptanalysis*. Norwood, MA, USA: Artech House, 1985.
[69] F. L. Bauer, "An error in the history of rotor encryption devices," *Cryptologia*, vol. 23, no. 3, pp. 206–210, Jul. 1999.
[70] H. Liu, X. Wang, and A. Kadir, "Color image encryption using choquet fuzzy integral and hyper chaotic system," *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 18, pp. 3527–3533, Sep. 2013.
[71] 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.
[72] A. U. Rehman and X. 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.
[73] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.
[74] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES BT," in *Proc. 12th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, E. F. Brickell, Ed. Berlin, Germany: Springer, 1993, pp. 487–496.
[75] A. ur 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.
[76] 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.
[77] 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.
[78] 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, Oct. 2016, Art. no. 100503.
[79] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Opt.-Int. J. Light Electron Opt.*, vol. 125, no. 5, pp. 1671–1675, Mar. 2014.
[80] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, Dec. 2018.
[81] J. Sun, Y. Wu, G. Cui, and Y. Wang, "Finite-time real combination synchronization of three complex-variable chaotic systems with unknown parameters via sliding mode control," *Nonlinear Dyn.*, vol. 88, no. 3, pp. 1677–1690, May 2017.
[82] J. Sun, G. Han, Z. Zeng, and Y. Wang, "Memristor-based neural network circuit of full-function Pavlov associative memory with time delay and variable learning rate," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 2935–2945, Jul. 2020.
[83] 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, p. e3966, May 2020.
[84] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on Julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, Feb. 2020.
[85] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.

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 Taxila (CASE campus) Islamabad, Pakistan, and the Ph.D. degree in computer science and technology from Chongqing University, China. He worked as an Assistant Professor with the Department Computer Sciences, COMSATS Institute of Information Technology, Vehari Campus, Pakistan. He is currently on Study Leave for working as a Senior Research Fellow with Southwest University, Chongqing China. He has published more than 12 research articles in Impact Factor journals. His primary areas of research are non-linear dynamics and cryptography. He is also a Reviewer of *Optics and Laser Technology*, *Optics and Lasers in Engineering*, and *International Journal Engineering Science and Technology*.

AMNAH FIRDOUS received the bachelor's and master's degrees in computer sciences (MSCS) from The Islamia University of Bahawalpur, Pakistan, where she is currently pursuing the Ph.D. degree in computer science. She worked as a Lecturer with the Computer Science Department, COMSATS Institute of Information Technology, Vehari, from 2018 to 2020.Her primary areas of research are image processing, petri nets, and cryptography.

SALMAN IQBAL received the M.S. degree in CS 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 serving as an Assistant Professor with COMSATS University Islamabad. He published more than eight research articles in high-impact ISI index journals. His research interests are in 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' degree in computer science from the Punjab University College of Information Technology (PUCIT), University of the Punjab, Lahore, Pakistan, in 2004, the M.S. degree in computer science from Uppsala University, Uppsala, Sweden, in 2008, and the Ph.D. degree in computer science from the Faculty of Computing, University Technology Malaysia (UTM), Malaysia, in 2017. 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 *Journal of Network and Computer Applications* and IEEE ACCESS and *IEEE Communications Magazine*.

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 worked with Behria University Islamabad from 2002 to 2004 and with Air University Islamabad 2004 to 2010. He is currently working with the Department of Computer Science, COMSATS University Islamabad, Vehari. His research interests are in software reliability engineering, software product line, and image-based encryption.

HUIWEI WANG received the B.S. degree in information and computing science and the M.E. degree in computer application from Chongqing Jiao Tong University, China, in 2008 and 2011, respectively, and the Ph.D. degree in computer science from Chongqing University, China, in 2014. 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, multi-agent networks, wireless sensor networks, and smart grids.

FARMAN ULLAH received the bachelor's degree in computer science from the Institute of Computing and Information Technology, Gomal University Dera Ismail Khan, Pakistan, in 2012, and the M.Phil. degree in computer science from NCBA&E Lahore, in 2016. He is currently working as a Lecturer with the Department of Computer Science, COMSATS University Islamabad, and also has additional charge as a Web Administrator. His research interest includes cryptography, image processing, computer graphics, and programming languages.