Hybrid image encryption algorithm

Md Altaf Hussain
Dept. of Information Technology
National Institute of Technology Karnataka, Surathkal
Mangalore, India
md.altafhussain99@gmail.com

Sumit Gupta
Dept. of Information Technology
National Institute of Technology Karnataka, Surathkal
Mangalore, India
sumitankitg130@gmail.com

Sagar Choudhury
Dept. of Information Technology
National Institute of Technology Karnataka, Surathkal
Mangalore, India
sagarchoudhury.nitk@gmail.com

***Abstract*— The objective of this paper is to study different image encryption algorithms and generate a hybrid algorithm by combining the best components from each method. Three channels of a color image called red, green and blue is arranged into one dimensional vector and sort according to chaotic sequence generated by Piecewise Linear Chaotic Map. After that S-box generated by the usage of all 16 distinct degree 8 primitive irreducible polynomials is used to substitute the pixels of image. The final encrypted image can be obtained by a pixel transposition step.**

Keywords —Chaos theory, Galois field, Irreducible polynomials, S-Box, Image Encryption, cryptosystems, Lorenz System, Chen's hyper-system

I. Introduction

The rapid expansion of digital technologies has made the traffic of communication fast and informal. Though, due to the openness of wireless networks such as the internet, the confidentiality of secret information is a serious problem.

Cryptography is the study of sharing confidential information over the unsecured channel, which deals with encryption, decryption, and key distribution, etc. Cryptography distributes further into two classes, symmetric, and asymmetric key cryptography. This distribution is made based on the secret key.

In Symmetric Cryptography is an encryption system the sender and receiver of the message uses a single common key to encrypt and decrypt messages. They are faster and simpler, but the problem is that sender and receiver must secretly exchange key in a secure manner. The most popular algorithm is Data Encryption System (DES).

In Asymmetric system a pair of keys is used to encrypt and decrypt information. A public key is used for the encryption and a private key is used for the decryption. Public key and Private Key are different to each other. Even if the public key is known by everyone the genuine receiver can only decode it because he only knows the private key.

Image is a very sensitive information. Even a normal selfie can be misused in many ways. Due to the extensive use of digital images in different fields, the security of digital image data gain attention extensively in the field of cryptography, that's why we are proposing a new crypto algorithm for image encryption.

II. Literature Survey

An efficient version of image encryption using chaos theory is done in [14].

[15] tried to improve the S-box based image encryption algorithms by the usage of all 16 distinct degree 8 primitive irreducible polynomials.

In symmetric-key cryptography substitution box (S-box) is the only main component responsible to produce confusion among the key and the plaintext. Thus, a good quality S-box is essential to improve the nonlinearity of block ciphers. Recently many algorithms have been suggested for the construction of S-boxes [1, 2, 3].

Many algorithms for digital encryption based on chaos theory, have been presented in the last decade [4, 5, 6], subsequently, some of them are proved to be unsecured against different attacks, due to defect in their internal structure [8].

Li et al. examined the algorithm presented in [9] and established that encryption schemes based on only pixel position permutations and substitution can easily be broken over the chosen-plaintext attack. Zang et al. explored the weakness in the security of the image encryption scheme based on the perceptron model given in [7] and concluded that the secret key can be rebuilt easily if just one pair of plaintexts or ciphertext is known.

Norouzi et al. [10] devised an image encryption technique utilizing a hyperchaotic system that creates diffusion in a single round. Whereas Zong et al. [11] observed error in the technique; this technique is not secure against attacks like chosen plaintext.

A. PWLCM

In the proposed algorithm, three different chaotic systems of different dimension have been employed to add more complexity where each chaotic system has its own features. For PWLCM given in Eq. (1), the sensitivity to initial condition and control parameter are both considered as 10^{-12} [16],

$$a_{i+1} = \begin{cases} \frac{a_i}{p_0}, & 0 \le a_i < p_0 \\ \frac{a_i - p_0}{0.5 - p_0}, & p_0 \le a_i < 0.5 \\ 1 - a_i, & a_i \ge 0.5 \end{cases} \quad (1)$$

B. Chen's system

Chen's hyper-chaotic system is highly sensitive to initial values and control parameters; is described as Eq. (2) as in [17],

$$\begin{aligned} \dot{u} &= a(v - u) \\ \dot{v} &= -uw + \mathrm{d}u + cu - x \\ \dot{w} &= uv - bw \\ \dot{x} &= u + k \end{aligned} \quad (2)$$

In Eq. (2), a, b, c, d, k are the system parameters, when a = 36, b = 3, c = 28, d = 16 and $-0.7 \le k \le 0.7$, the Chen's hyper-chaotic system is in the chaotic state and can generate four chaotic sequences. In this paper, parameter k = 0.2 is used to generate Chen's chaotic sequence. Here, four-order Runge–Kutta method is applied to solve the equations and get the sequences U, V, W and X and then sequences are combined into one array.

C. Lorenz' system

Lorenz system is a mathematical model of weather forecasting, given as [18]:

$$\begin{aligned} \dot{y} &= -fy + fz \\ \dot{z} &= ry - z - yq \\ \dot{q} &= -gq + yz \end{aligned} \quad (3)$$

The above equation is a dynamical nonlinear system with two non-linearities yq, yz. The inputs f, g and r are constants physical characteristics of air flow, y represent amplitude of convective current in the air cell, z represents to the temperature difference between rising and falling currents, q to the deviation of temperature from normal temperature in the cell. No analytical solution exists for this nonlinear system, it first transformed into iterative form and numerical solution is then computed. The numerical solutions show that for 0 < r < 1, the overall system will have steady response, for 1 < r < 24the system will also be stable with periodic response, for r > 24, f = 10 and g = 8/3, the system yields chaotic response [18].

III. METHODOLOGY

Our encryption algorithm is based symmetric key cryptography. In symmetric-key cryptosystem, the interconnected parties use alike keys, while in an asymmetric key cryptosystem both parties use different keys namely public key and private key for secure communication.

A. Generate initial conditions and control parameters.

SHA-256 generates digest of 256 bits regardless the size of the input. If there is one-bit difference between two inputs, their message digest will be completely different [16]. So, this is used to generate digest of the color image to which encryption is to be done. The message digest is divided into two groups of hexadecimal values. The first group is divided into mj blocks of equal size where j = 1, 2, · · ·, 8. Each block contains seven hexadecimal digits and convert into a floating decimal number $m_j \in (0, 0.0156)$ using Eq. (4):

$$m_j = \text{hex2dec}(m_1, \ldots, m_8)/2^{34} \qquad (4)$$

The second group is directly converted into floating point valued (0, 0.0156)

$$d = \text{hex2dec}(d)/2^{42} \qquad (5)$$

$$\begin{cases} a_0' = a_0 + m_1 + CK \\ p_0' = p_0 + m_2 + CK \bmod 1 \end{cases} \qquad (6)$$

Suppose that seed values for Chen's are u_0 , v_0, w_0 and x_0 then new initial seed can be generated using Eq. (7) as follows,

$$\begin{cases} u_0' = u_0 + m_3 + Ck \\ v_0^1 = v_0 + m_4 + CK \\ w_0' = w_0 + m_5 + CK \bmod 1 \\ x_0' = x_0 + m_6 + CK \end{cases} \qquad (7)$$

Three more seeds are required for Lorenz chaotic system which is calculated as follows:

$$\begin{cases} y_0' = y_0 + m_7 + CK \\ z_0' = z_0 + m_8 + CK \bmod 1 \\ q_0' = q_0 + d + CK \end{cases} \qquad (8)$$

In above Equations, CK is the common key generated as follows,

$$CK = a_0 + p_0 + u_0 + v_0 + w_0 + x_0 + y_0 + z_0 + q_0 \bmod 1 \qquad (9)$$

The dependence of keys on plain image makes sure to change for every input, hence more secure [16].

S-box which is used in the proposed approach is based on the action of general linear group $G_L(2, F_{2^8})$ on finite field F_{2^8} of order 256.

w: $GL(2, F_{2^8}) \times F_{2^8} \rightarrow F_{2^8}$

$$w(M, y) = F_M(y) \qquad (10)$$

where $F_M(y) = \frac{\alpha(y)+\beta}{\gamma(y)+\delta}$ and α, β, γ and δ are the elements of F_{2^8}. F_M is a bijective mapping from F_{2^8} to F_{2^8}, and the resultant values of F_M are then converted into a 16x16 lookup table, which is the required S-box.

B. Encryption Process

a) Permutation Step – The proposed diffusion of color image is performed in two ways; first one is done by combining all three channels image I into 1-Dimensional array of size 1 × 3MN and then sort according to a chaotic sequence A. This chaotic sequence A is generated by iterating PWLCM up to 3MN times a_0 and p_0 and permute pixels of I as follows

$$\begin{gathered} A = \{a_i, a_{i+1}, \ldots, a_{3MN}\} \\ [valA, idxA] = sort(A) \\ I' = I(idx\, A) \end{gathered} \qquad (11)$$

After this, I' is split into three arrays of size 1 × MN called red, green and blue as follows,

$$\begin{gathered} R = [I'(1), I'(2), \ldots, I'(MN)] \\ G = [I'(MN+1), I'(MN+2), \ldots, I'(2MN)] \\ B = [I'(2MN+1), I'(2MN+2), \ldots, I'(3MN)] \end{gathered} \qquad (12)$$

The second permutation is performed on the above channels R, G and B independently. For this, Loren'z system of equation used to generate three pseudo-random sequences Y, Z, and Q of size t + MN using initial seed y_0', z_0' and q_0' to shuffle the pixels of three channels. The t values are discarded to avoid transient effect and sort three sequences as,

$$\begin{gathered} [valY, idxY] = sort(Y) \\ [valZ, idxZ] = sort(Z) \\ [valQ, idxQ] = sort(Q) \end{gathered} \qquad (13)$$

where idxY, idxZ and idxQ are index value of sorted Y, Z and Q and rearrange the elements of R, G and B according to idxY, idxZ and idxQ to get permuted image as shown in following equation,

$$\begin{cases} R_p(i) = R(idxY(i)) \\ G_p(i) = G(idxZ(i)) \\ B_p(i) = B(idxQ(i)) \end{cases} \qquad (14)$$

b) S-Box Substitution - In this step, we substitute the obtained permuted matrices using sixteen S-boxes to enhance the nonlinearity of the proposed scheme. For S-boxes generation, we chose the set of all degree 8 primitive irreducible polynomials over the field $\mathbb{Z}_2$;

$$\{h_j(y) \in \mathbb{Z}_2[y] : h_j(y) \text{ is irreducible}, 1 \le j \le 16\}$$

Thus for each j the quotient ring $\frac{\mathbb{Z}_2[y]}{\langle h_j(y) \rangle}$ form a field isomorphic to the Galois field $GF(2^8)$. Accordingly, the nonzero elements of each of these fields form a group known as the Galois cyclic group generated by the primitive element a_i, corresponding to the irreducible polynomial $h_j(y)$. The list of Galois fields against their primitive irreducible polynomials is given in Table 1. For S-boxes construction, we used the above degree 8 primitive irreducible polynomials and the action of the general linear group over a newly designed finite field is defined as;

Table 1: Primitive irreducible polynomials and their corresponding Galois fields

Irreducible Polynomial $h_i(y)$; Primitive element	Galois Field	Irreducible Polynomial $h_i(y)$ Primitive element	$\frac{\mathbb{Z}_2[y]}{<h_i(y)>}$
$h_1(y) = y^8 + y^4 + y^3 + y^2 + 1$	$\frac{\mathbb{Z}_2[y]}{<h_1(y)>}$	$h_9(y) = y^8 + y^7 + y^3 + y^2 + 1; a_9$	$\frac{\mathbb{Z}_2[y]}{<h_9(y)>}$
$h_2(y) = y^8 + y^5 + y^3 + y + 1; a_2$	$\frac{\mathbb{Z}_2[y]}{<h_2(y)>}$	$h_{10}(y) = y^8 + y^7 + y^5 + y^3 + 1; a_{10}$	$\frac{\mathbb{Z}_2[y]}{<h_{10}(y)>}$
$h_3(y) = y^8 + y^5 + y^3 + y^2 + 1; a_3$	$\frac{\mathbb{Z}_2[y]}{<h_3(y)>}$	$h_{11}(y) = y^8 + y^7 + y^2 + y + 1; a_{11}$	$\frac{\mathbb{Z}_2[y]}{<h_{11}(y)>}$
$h_4(y) = y^8 + y^6 + y^3 + y^2 + 1; a_4$	$\frac{\mathbb{Z}_2[y]}{<h_4(y)>}$	$h_{12}(y) = y^8 + y^7 + y^6 + y + 1; a_{12}$	$\frac{\mathbb{Z}_2[y]}{<h_{12}(y)>}$
$h_5(y) = y^8 + y^6 + y^4 + y^3 + y^2 + y + 1; a_5$	$\frac{\mathbb{Z}_2[y]}{<h_5(y)>}$	$h_{13}(y) = y^8 + y^7 + y^6 + y^5 + y^2 + y + 1; a_{13}$	$\frac{\mathbb{Z}_2[y]}{<h_{13}(y)>}$
$h_6(y) = y^8 + y^6 + y^5 + y + 1; a_6$	$\frac{\mathbb{Z}_2[y]}{<h_6(y)>}$	$h_{14}(y) = y^8 + y^7 + y^6 + y^3 + y^2 + y + 1; a_{14}$	$\frac{\mathbb{Z}_2[y]}{<h_{14}(y)>}$
$h_7(y) = y^8 + y^6 + y^5 + y^2 + 1; a_7$	$\frac{\mathbb{Z}_2[y]}{<h_7(y)>}$	$h_{15}(y) = y^8 + y^7 + y^6 + y^5 + y^4 + y^2 + 1; a_{15}$	$\frac{\mathbb{Z}_2[y]}{<h_{15}(y)>}$
$h_8(y) = y^8 + y^6 + y^5 + y^3 + 1; a_8$	$\frac{\mathbb{Z}_2[y]}{<h_8(y)>}$	$h_{16}(y) = y^8 + y^6 + y^5 + y^4 + 1; a_{16}$	$\frac{\mathbb{Z}_2[x]}{<h_{16}(x)>}$

$$w_j : GL\left(2, \frac{\mathbb{Z}_2[y]}{\langle h_j(y)\rangle}\right) \times \frac{\mathbb{Z}_2[y]}{\langle h_j(y)\rangle} \to \frac{\mathbb{Z}_2[y]}{\langle h_j(y)\rangle} \quad (15)$$

$$F_{jA}(y) = \frac{\alpha(y)+\beta}{\gamma(y)+\delta} \quad (16)$$

Where $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in GL\left(2, \frac{\mathbb{Z}_2[y]}{\langle h_j(y)\rangle}\right)$. For a M and for each j, $1 \le j \le 16$ F_{jA} give us sixteen S-boxes having diverse algebraic and statistical properties. Moreover, over the cryptographic properties of these S-boxes are closed to the standard S-box of AES and APA S-box, the justification is given [12]. Furthermore, we divide the permuted color components R_P, G_P and B_P into sixteen sub-blocks, and substitute each sunblock with a different S-box. At last, after the use of these newly generated sixteen S-boxes, we combine the substituted sub-blocks and obtained three substituted blocks R_S, G_S and B_S.

c) Pixel transposition step – For the pixels, transposition generate a sequence (x_n) from 1 up to$M \times N$ respectively. Then convert each element of the sequence into the range of $0 - 255$ using the following equation:

$$x_n' = \mathrm{mod}(x_n, 256) \quad (17)$$

In the next step by using the multiplicative operation of a group $\frac{\mathbb{Z}_2[y]}{\langle h_1(y)\rangle} \setminus \{0\}$ and generate a three random sequence from x' with the help of following equations;

$$x_R = a \times x_n' \bmod h_1(y) \quad (18)$$

$$x_G = b \times x_n' \bmod h_3(y) \quad (19)$$

$$x_B = c \times x_n' \bmod h_4(y) \quad (20)$$

Where a, b and c are the elements of the set $\frac{\mathbb{Z}_2[y]}{\langle h_1(y)\rangle} \setminus \{0,1\}$. After getting matrices x_R, x_G and x_B, permute each matrix.

For this, Chen's hyper system is iterated (t+ MN) times using initial secret key u_0', v_0', w_0' and x_0' to get four pseudo-random chaotic sequences U, V, W and X. The first t values are discarded to avoid transient effect and sort three sequences x_R, x_G and x_B as,

$$\begin{aligned} [valU, idxU] &= sort(U) \\ [valV, idxV] &= sort(V) \\ [valW, idxW] &= sort(W) \end{aligned} \quad (21)$$

where idxU, idxV and idxW are index value of sorted U, V and W and rearrange the elements of x_R, x_G and x_B according to idxY, idxZ and idxQ to get permuted image as shown in following equation,

$$\begin{cases} x_R'(i) = x_R(idxY(i)) \\ x_G'(i) = x_G(idxZ(i)) \\ x_B'(i) = x_B(idxQ(i)) \end{cases} \quad (22)$$

Then transpose the substituted blocks using the following formulas:

$$R_E = \mathrm{bitxor}(x_R', R_S) \quad (23)$$

$$G_E = \mathrm{bitxor}(x_G', G_S) \quad (24)$$

$$B_E = \mathrm{bitxor}(x_B', B_S) \quad (25)$$

Then combine R_E, G_E and B_E matrices and recover the encrypted RGB image.

C. Decryption Process

a) Pixel transposition step - The decryption process of the proposed scheme is the same as the encryption process, but it starts from the reverse side. Convert the encrypted image into three matrices R_E, G_E and B_E. The first round of the reverse processes is the same as the step which we have discussed in pixel transposition step, and get back the matrices R_S,G_S and B_S.

b) Inverse S-Box substitution - In this step, we generate the inverse S-box utilize degree 8 primitive irreducible polynomials given in the table, 1. The inverse sixteen S-boxes are generated using the following inverse map:

$$F_{jM}(y) = \frac{\delta(y)+\beta}{\gamma(y)+\alpha} \quad (26)$$

Then divided the matrices R_S, G_S and B_S into sixteen sub-blocks, substitute each sub-block with inverse S-box and then combine the sub-blocks to obtain the matrices R_P, G_P and B_P.

c) Inverse Permutation – We repeat the permutation step of the encryption process in reverse manner using pseudo-random sequences Y, Z, and Q generated from Loren'z System and chaotic sequence A generated from PWLCM. And after doing the permutation we get the original image .

IV. Results And Analysis

In this study, we perform image encryption experiments using JPEG images 'Lena', 'Baboon' and 'Pepper' shown in Fig. 1(a-c). Each encrypted image is also shown in Fig.1 (d-f).

Here the common initial values set for PWLCM maps are: a_0 = 0.123456789010 and p_0 = 0.234578900. The initial conditions for Chen's hyper chaotic system are u_0 = 0.3456789012, v_0 = 0.245789012, w_0 = 0.4567890124 and x_0 = 0.5678901234. The initial conditions for Lorenz system are y_0 = 0.6789012346, z_0 = 0.7890123456 and q_0 = 0.6890123450.

The control parameters of Chen's system are a = 36, b = 3, c = 28, d = 16 and k = 0.2 while for Lorenz system, control parameters are f = 10, g = 8/3 and r = 28.

The matrix elements for S-boxes generation (α, β, γ, δ) were chosen as (121,45,67,145). The elements a, b, c in pixel-transposition step were chosen to be 128,255 and 100.

A. Key-space Analysis

An efficient cryptosystem should have a large key-space to deal with threats like a brute force attack. The key-space is the set of all possible keys which are used during the process of encryption and decryption.

The floating-point precision of each input to chaotic system is dependent on the system which varies from 10^{10} to 10^{12} for the proposed technique. Here, three chaotic systems are used named PWLCM, Lorenz and Chen's system. The PWCLM uses two parameters a_0 and p_0 with precision 10^{12}, hence key space of

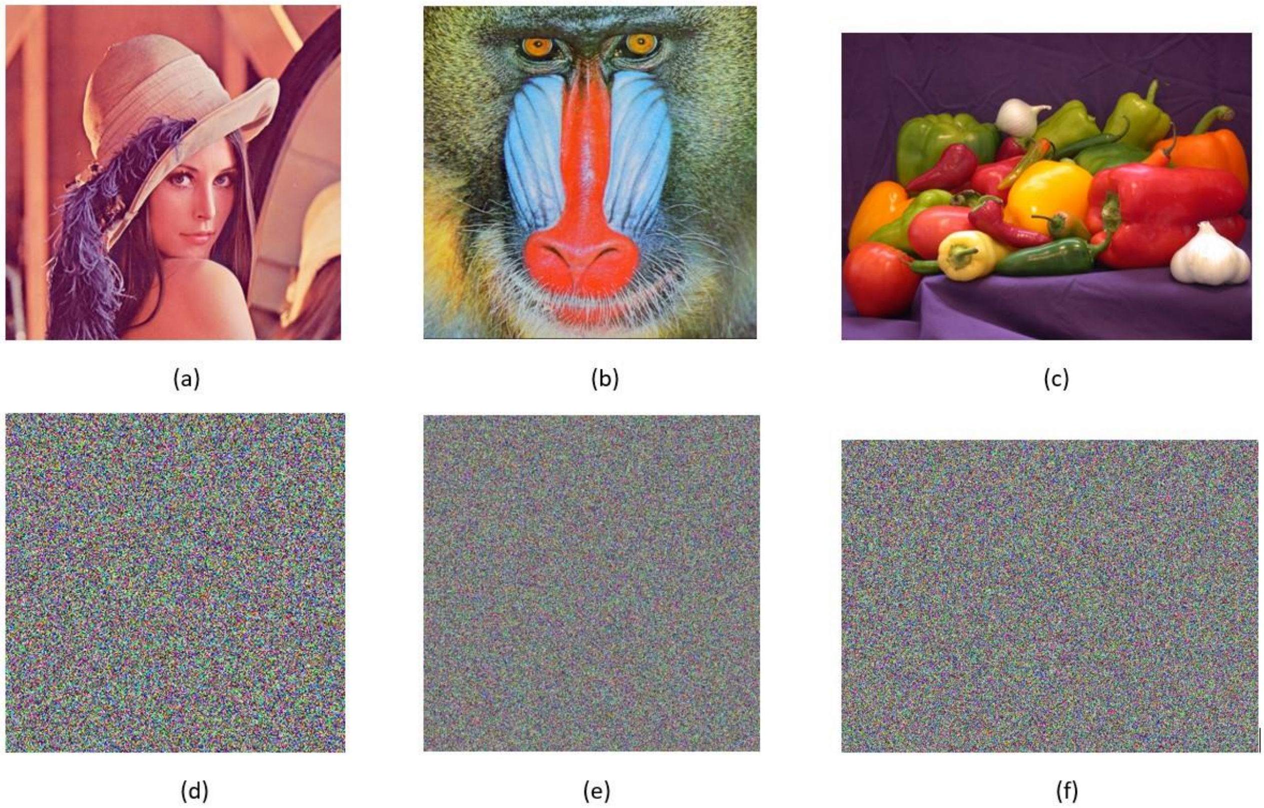

Figure 1: (a-c) shows the original three images; (d-f) represents corresponding encrypted three images

PWLCM is $S_{PWLCM} = S_{a0} * S_{p0} \cong 10^{24} \cong 2^{79.72}$. The second chaotic map is Chen's system of equations which require four inputs (0.3, −4, 1.2 and 1.0) in the interval (1, 3). The initial seed for Chen's system has precision of 10^{10} hence key space of Chen's system is $S_{Chen's} = S_{u0} \times S_{v0} \times S_{w0} \times S_{x0} \cong 10^{40} \cong 2^{132.87}$. The third system is known as Lorenz system that needs three initial seeds $S_{Loren'z} = S_{y0} \times S_{z0} \times S_{q0} = 10^{30} \sim= 2^{99.65}$.

The total number of different α, β, γ and δ which can be used as a part of the secret key in S-Box substitution is 4.2781×10^{9}, and the total number of a, b and c which can also be used as a part of a secret key 16194277. So, for a fixed key in PWLCM, Lorenz and Chen's, the key-space is 6.9281×10^{16} for substitution step.

Total key space of proposed system is $S_{Total} = S_{PWLCM} \times S_{Chen's} \times S_{Lorenz} \times S_{Substitution} \cong 10^{110} \cong 2^{365.41}$. The key space of proposed system is much larger than the minimum requirement 2^{128} to resist brute force attack [19].

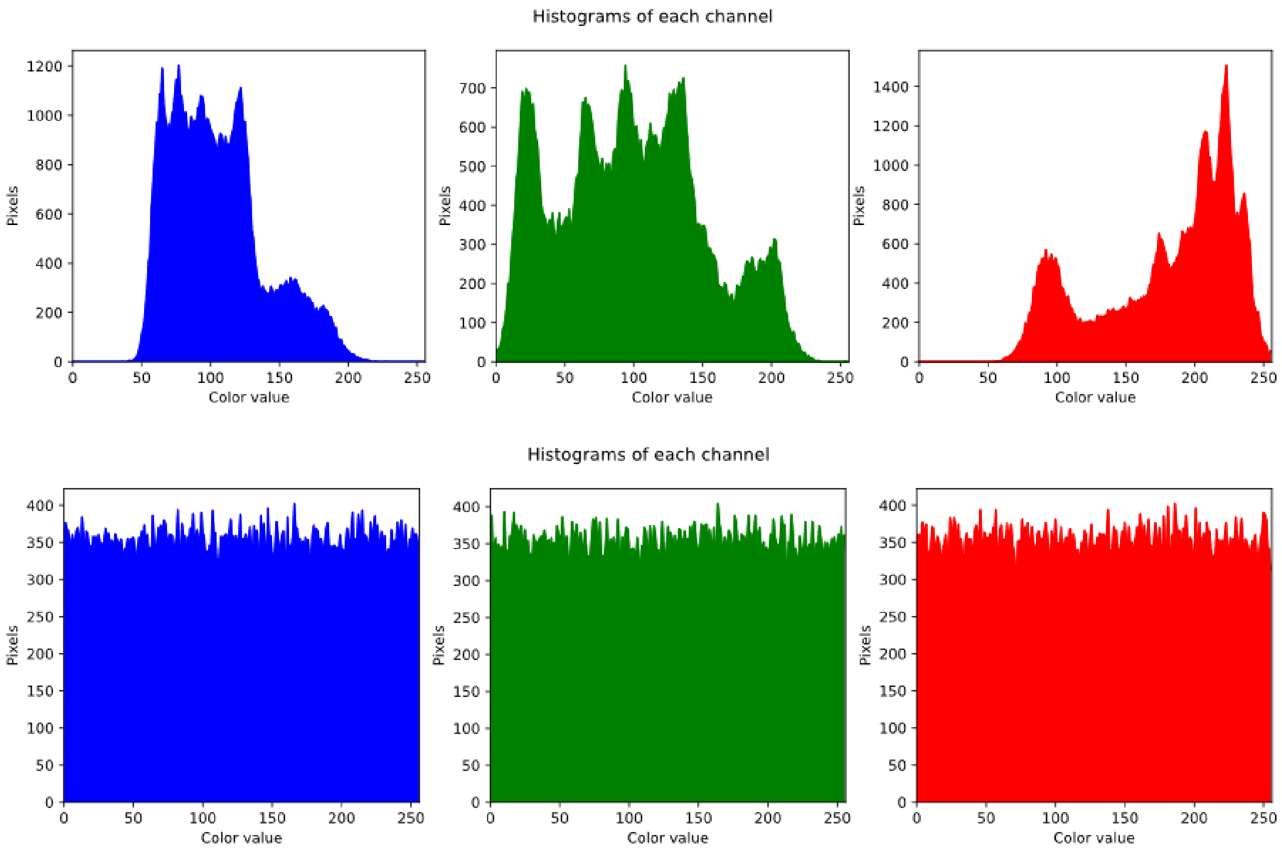

Figure 2: Histogram Analysis of Lena Image and their corresponding encrypted image

B. Histogram Analysis

In order to inspect the resisting capability of the proposed cryptosystem, we examined histograms of RGB images. Histogram of 'Lena' original image for RGB channels is shown in the Fig. 2, however Fig. 2 represents the histogram of the cipher 'Lena' image correspondingly. Histograms of the encrypted images have the uniform distribution that ensures the anticipated scheme is capable to resist against statistical attacks.

V. Conclusion And Future work

Substitution–permutation configuration is used in designing a new cryptosystem. Accordingly, confusion among the key streams and the cipher image is increased. In addition, the inclusion of the diffusion layer improved the security level of the proposed scheme.

For the futuristic perspective, we might extend this study for the different types of data, such as voice, signal, audio, and video.

VI. References

[1] Khan M, Shah T, Batool SI (2008) Construction of S-box based on chaotic boolean functions and its application in image encryption.

[2] Khan M, Shah T, Mahmood H, Gondal MA (2013) An efficient method for the construction of block cipher with multi-chaotic systems.

[3] Naseer Y et al (2019a) A Novel Algorithm of Constructing Highly Nonlinear Sp-boxes.

[4] Huang C-K, Nien H-H (2009) Multi chaotic systems-based pixel shuffle for image encryption.

[5] Huang Z-J et al (2020) Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform.

[6] Liao X, Li K, Yin J (2017a) Separable data hiding in encrypted image based on compressive sensing and discrete Fourier transform

[7] Zhang Y et al (2012a) Breaking a chaotic image encryption algorithm based on perceptron model.

[8] Khan M, Shah T (2015) An efficient chaotic image encryption scheme.

[9] Liao X, Zheng Q, Ding L (2017b) Data embedding in digital images using critical functions.

[10] Khan M, Waseem HM (2018) A novel image encryption scheme based on quantum dynamical spinning and rotations.

[11] Wang X, Lin T, Xue Q (2012) A novel colour image encryption algorithm based on ch

[12] Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR (2014) A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion proc

[13] Aqeel ur Rehman, Xiaofeng Liao, Rehan Ashraf, Saleem Ullah, Hueiwei Wang,
A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2

[14] Firdous, A., ur Rehman, A. & Saad Missen, M.M. A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2.

[15] Shah, D., Shah, T. A novel discrete image encryption algorithm based on finite algebraic structures.

[16] H. Liu, X. Wang, A. Kadir, Image encryption using DNA complementary rule and chaotic maps, Appl. Soft Comput. J.

[17] T. Gao, Z. Chen, Z. Yuan, G. Chen, A hyperchaos generated from chen's system, Int. J. Mod. Phys.

[18] A. Anees, An image encryption scheme based on lorenz system for low profile applications

[19] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Opt. Commun.