IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

# Color Image Encryption using Single Layer Artificial Neural Network and Buffer Shuffling

**Dipankar Dey[1*], Soumen Paul[2]**

[1]Global Institute of Science and Technology, Haldia-721657, India
[2]Haldia Institute of Technology, Haldia-721657, India

[*]*Corresponding Author: deydipankar2014@gmail.com, Tel.: 943242218*

DOI: https://doi.org/10.26438/ijcse/v7i3.202211 | Available online at: www.ijcseonline.org

Accepted: 11/Mar/2019, Published: 31/Mar/2019

***Abstract***— An image encryption is a traditional way to hide original image to an adversary in the case of secure image transmission. In this regard, the Artificial Neural Network (ANN) can be used in digital communication systems (digital image transmission) to achieve a secure and reliable data transmission. However, we have designed a new scheme that encrypts a color image, which can be used in secure image transmission. This proposed scheme is divided into three steps, (a) we subdivide the color image into $R$ (red), $G$ (green) and $B$ (blue) factors, and using the chaotic map, we randomly shuffle these RGB factors to get first encrypted image; (b) we process the first encrypted image through the single-layer artificial neural network to get the second encrypted image; and (c) pixels of the second encrypted image are shuffled using exclusive-or (XOR) operation to get the final encrypted image, which can be transmitted over insecure channel. Furthermore, we have examined the proposed scheme on some standard color images each of size $512 \times 512$. The several security study and experimental outcomes indicate that the proposed scheme can protect from several statistical attacks like Plaintext Attack, Cipher text Attacks, Brute Force Attack, and Birthday Attack etc.

***Keywords***—Encryption, RGB buffer shuffle, Artificial Neural Network, Attacks.

## I. INTRODUCTION

In the 4G and 5G technology era, we protect our confidential and sensitive information (in case of image), while transmitted over the Internet. The different fields of the Image encryption scheme are online data communication, multimedia systems, telemedicine biomedical imaging and military secret data transmission. Hence, the security of digital information processing plays an important role nowadays. However, the digital information processing can be implemented through an artificial neural network [4, 5]. Therefore, with the help of the artificial neural network and cryptographic technique, based on encryption technique of color image, which can apply in secure image transmission. Cryptography defines several important services that can protect our confidential information, where Color Image encryption [12, 13, 20] is one of the parts of the secure image transmission.

In the recent era, image encryption plays an important role to protect an original image from authorized access. However, there are different methods [15, 23, 25, 26], proposed by different researchers to encrypt images and to make the images secure. We also try to change the original image into the encrypted image with the help of the secret key.

In this paper, we present a color image cryptography technique using the artificial neural network and buffer shuffling. This scheme is implemented in three stages. In the first stage, we read a color image and then we separate RGB factors [1, 14] from the image. After that, we randomly shuffle these red, green and blue components using the chaotic map and we get our first encrypted image. Then we go for the second stage. In the second stage, we process our first encrypted image using Artificial Neural Network. The weight of the neural network is implemented using the Galois Field, GF (2) and these weights are multiplied separately with the RGB factors and each of the final output of the RGB factors are exclusive-or (XOR) with each other and a random number, where random numbers are produced using the LFSR (Linear Feedback Shift Register). Then, we go for the third stage and it is the last stage of this scheme, where the pixels of the encrypted image are exclusive - or (XOR) using two secret keys. These secret keys are generated using the logistic map and the modular arithmetic. We then show our encryption procedure is secure against differential statistical attacks. We also simulate our scheme

 

and measure the UACI, the NPCR, and histogram analysis and information entropy.

The outline of this paper as follows: Section 2 focuses on the literature review of some existing schemes; preliminaries of this study are explained in Section 3. Section 4 illustrates the proposed scheme in details. The different security analysis of the proposed scheme is describing in Section 5. Section 6 explains the performance of the proposed scheme and we com-pares our scheme with some existing scheme. Section 7 gives the conclusion of this paper.

## II. RELATED WORK

Wang et al. [1] proposed a scheme, where color images are used. For better statistical and diffusion properties, scheme in [1] used 4 - pixel Feistal structure and functions that is based on two 3 D chaotic maps. The proposed scheme in [1] is divided into 3 levels: 1st level is the basic level based on chaotic maps that are used to create round function, the 2nd level is the intermediate level define the block operation using rounding function and the 3rd level is the final level, where a key is used to encrypt the color image. However, with different security analysis, authors claimed that scheme in [1] is highly secure.

Xiao et al. present a scheme in [2]. For the high level of security, the authors designed an algorithm using perturbed high - dimensional Chaos technique. Using the Henon map [2], the image is perturbed. For implementing Confusion - diffusion process, the authors generated a separate new cat map. For this purpose, they divided the image into several parts, which can overlap with each other. For each part, the separate cat map is used to permute. The control parameters of the cat map are increased to enlarge the key space and to improve the security. The confusion process is applied using separate cat map algorithm and then the diffusion method is applied to this confusion image. At last, the round functions are used to encrypt the image.

Rhouma et al. [10] proposed a color image encryption scheme. This scheme based on high-dimensional chaos function OCML (one-way coupled-map lattices) by which they encrypt the color image. Here, 192 bits long external key is defined as the parameter of the OCML function. To enhance the sensitivity of this scheme, the authors used the OCML function and some algebraic transformation. In a coupling fashion, the three color components (RGB) are encrypted to achieve the security of the scheme in [10].

Yang et al. [21] presented a scheme, where they encrypted the image using chaotic coupled map lattices with time-varying delays. To shuffle the pixel's position of the image, they used the desecrate Tent map. After that, the authors used a coupled chaotic map to puzzle the relationship between the original image and the cipher image. The different control parameters are used in the shuffling stage and secret keys are used in diffusing stage. All the keys and the control parameters are generated from the chaotic map. Therefore, for good confusion - diffusion architecture, the proposed scheme [21] is secure from different attacks.

Liu et al. [22] introduced a new color image encryption scheme. To implement the high security, they used one time keys and piecewise linear chaotic map. Here, the chaotic map is used to generate the pseudo random key sequence. These random numbers are used to generate the secret keys by the Message-Digest algorithm 5 (MD5) [22] of the mouse positions. In the key stream, every item is generated by different initial condition from perturbation map, parameter and different number of iteration times.

Wen et al. [23] proposed an optical color image encryption scheme. In this scheme, an optical asymmetric cryptosystem has been implemented to encrypt the color images. To implement the security system, a phase-truncated strategy is developed in the Fresnel domain, and multiple wavelengths and indexed image methods. In this scheme [23], different numerical analysis has been proposed to demonstrate the feasibility and effectiveness of this encryption.

## III. METHODOLOGY

This section describes the different features, which are used to implement our proposed scheme. The different symbols used in this paper are given in Table 1.

Table 1: NOMENCLATURE

| Term | Usage |
|---|---|
| $\mu$ | a Threshold value i.e., $3.57 \leq \mu \leq 4$ |
| $\lfloor \rfloor$ | Floor function |
| $\oplus$ | Bitwise xor operation |
| $dx$ | Change in the value of x |
| $dx$ | Change in the value of y |
| $W$ | Column of the image |
| $H$ | Row of the image |
| $X_0$ | Initial value of the chaotic map |
| $X_i$ | i-th value of the chaotic map |
| $P_i$ | i-th pixel's intensity value of the plain image |
| $P_i^{'}$ | i-th pixel's modified intensity value |
| $C_i$ | i-th pixel's intensity value of the cipher image |
| $H(S)$ | Entropy |
| $L$ | Total number of pixels |
| $k_1, k_2, k_3$ | Secret keys |
| $r$ | Correlation coefficient |
| $\phi(h)$ | Random shared secret key |
| $\|\|$ | Concatenation operator |
| $R, G, B$ | Red, Blue and Green Components |
| $R_i, G_i, B_i$ | i-th pixels Red, Blue and Green Components |
| $w_{i,j}$ | Weight of the $ANN$ |

 

3.1. **LFSR**

A Linear Feedback Shift Registers [6] are mostly used for generating pseudo random numbers. The LFSR is represented by the polynomial equation. A maximum length of the polynomial of degree n will have $2^{n-1}$ different states. It means that the random numbers repeat after $2^{n-1}$ clock cycle. The 8 degree linear feedback shift register is defined using the following polynomial:

$$P(x) = x^8 + x^6 + x^5 + x^4 + 1 \qquad (3.1)$$

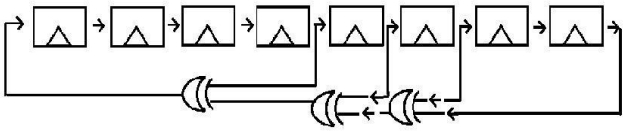

Figure 1: 8 degree Linear Feedback Shift Registers

The Figure 1 describes 8 degree LFSR. The basic value of the LFSR is called seed. The operation in LFSR is over modulo 2 and thus the coefficients of the LFSR must be either 0 or 1. Another name of LFSR is feedback polynomial or reciprocal character polynomial for modulo 2 operations. The maximum number of pseudo random numbers is generated if we use an irreducible polynomial.

3.2. **Logistic Map**

In mathematics, a chaotic map [1, 18] is expressed as an evolution function, which has some sort of chaotic nature. The chaotic map may have some discrete / continuous time parameters. It is often used in the study of the dynamic system. The Logistic map is one type of chaotic map that can be defined as:

$$X_{i+1} = \left(\mu + \frac{X_i}{2}\right) \cdot X_i \cdot (1 - X_i) \qquad (3.2)$$

Where $3.57 \leq \mu \leq 4$ and $0 < X_i < 1$, and $X_0 \in (0,1)$ is considered as a boundary value. Here, logistic maps are also used to generate a random sequence. These random values are used to modify the pixels values of an image.

3.3. **Galois field**

Galois field [7, 17] is one of the important parts of the mathematics invented by Evariste Galois. It is a finite field that contains a finite number of elements. The finite numbers of elements are called order. The Galois field is defined by the integer mod p and p is defined as a prime number. GF(2) is one of the most important part of Galois field, which defines only one irreducible polynomial of degree 2. The irreducible polynomial of degree two over GF(2) is given below:

$$X^2 + X + 1 \qquad (3.3)$$

Using GF (2), we can design a matrix as

$$w_{i,j} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

The Figure 2 and the Equations 3.4 describe the procedure of GF (2) matrix creation.

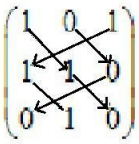

Figure 2: GF(2) Matrix

$$w_{21} = w_{13}, w_{22} = w_{11} \oplus 0, w_{23} = w_{12} \oplus 0$$
$$w_{31} = w_{23}, w_{32} = w_{21} \oplus 0, w_{33} = w_{11} \oplus w_{22} \qquad (3.4)$$

Here, each element of this matrix (see Figure 2) is used as the weight of the Artificial Neural Network (ANN). Here ANN is used for image encryption. We can also easily find the inverse of this matrix as follows:

$$w'_{i,j} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

For image decryption, we use the inverse matrix as the weight of ANN.

3.4. **ANN**

An ANN [4, 5] is an arithmetical form based on the functions of biological neural structure. ANN is considered as a statistical data of nonlinear type, where the complex association among the inputs and outputs are determined. ANN is used as a random number generator. ANN takes data samples to reach at solutions that minimize time complexity.

The ANN is combined with multiple nodes that are called neurons. The nodes are connected by links and each link has a specified weight. Each of the nodes is assigned some input value. These input values are multiplied by the weight of the links. Then these input values are exclusive-or (XOR) with other input values and produce the desired outputs. The Figure 3 shows the schematic diagram of ANN: Here $r_i$, $g_i$ and $b_i$ are

 

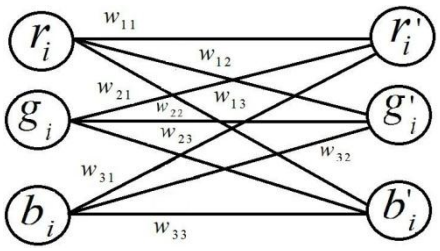


Figure 3: Artificial Neural Network Implementation

the RGB factors of the color image. The weight of the ANN has implemented with GF (2) matrix. Here $w_{i,j}(i,j = 1,2,\cdots,3 \times 3)$ is the elements of the GF (2) matrix and $r_i'$, $g_i'$ and $b_i'$ are the updated RGB factors of the image.

## IV. OUR PROPOSED SCHEME

This section describes our proposed image encryption scheme, which contains three steps: (a) buffer shuffling, (b) image encryption using Artificial Neural Network, and (c) alter pixel intensity value. Figure 4 shows the block diagram of our proposed scheme.

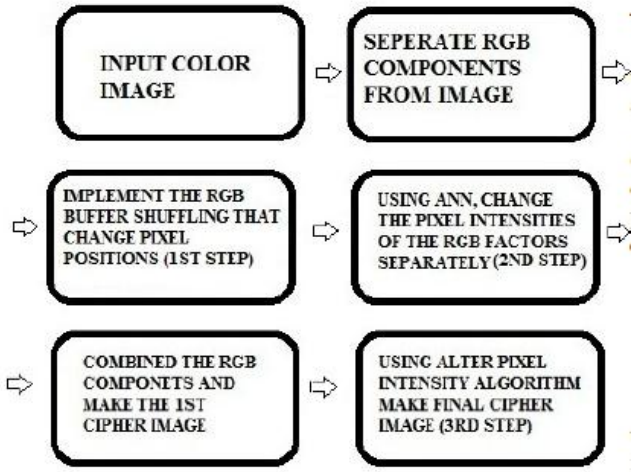


Figure 4: Block diagram of the proposed scheme

### 4.1. **Buffer Shuffling**

The first step of the image encryption is buffer shuffling [8]. We first separate the RGB factors from the images. Then, we have implemented the buffer shuffling using the 6 separated values of d (Here d defines the decision parameter corresponding to RGB factors). The values of d can be 1 to 6. The selection of the value of d is control by chaotic map. The values of d are determined using following formula:

$$Q = \lfloor (k \cdot 2 \cdot X_j) \rfloor \cdot (Q+1) mod\ 6 + 1, where\ 0 < X_j < 1, \quad d = Q \tag{4.1}$$

where the initial value of $Q$ is 4 and with respect to other iteration the value of $Q$ is changed, $k = 1001$ and $X_j$ is the value that found from the chaotic system. Here $Q$ and $X_j$ are considered as a secret information.

The following steps describe the buffer shuffling procedure:

$$\begin{aligned}
&Case\ 1{:}\ If\ d = 1,\ then\quad r_i' = r_i;\quad g_i' = g_i;\quad b_i' = b_i;\\
&Case\ 2{:}\ If\ d = 2,\ then\quad r_i' = r_i;\quad g_i' = b_i;\quad b_i' = g_i;\\
&Case\ 3{:}\ If\ d = 3,\ then\quad r_i' = b_i;\quad g_i' = r_i;\quad b_i' = g_i;\\
&Case\ 4{:}\ If\ d = 4,\ then\quad r_i' = b_i;\quad g_i' = g_i;\quad b_i' = r_i;\\
&Case\ 5{:}\ If\ d = 5,\ then\quad r_i' = g_i;\quad g_i' = r_i;\quad b_i' = b_i;\\
&Case\ 6{:}\ If\ d = 6,\ then\quad r_i' = b_i;\quad g_i' = b_i;\quad b_i' = r_i;
\end{aligned}$$

Where $i,j = 1,2,3\cdots,512 \times 512$ and $r_i, g_i\ and\ b_i$ are corresponding to the RGB factors of the image and also $r_i', g_i'\ and\ b_i'$ are the updated RGB factors after changing buffer. Figure 5 describes buffer shuffling method:

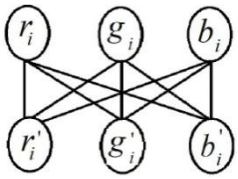


Figure 5: Shuffle RGB factors of the original color image

### 4.2. **Image encryption using Artificial Neural Network**

After successful completion of the first step of image encryption, we have designed the second step. In the second step, we apply the concept of Artificial Neural Network.

Here, the inputs values of ANN are implemented using Red ($r_i$), Green ($g_i$) and Blue ($b_i$) (where $i,j = 1,2,3\cdots,512 \times 512$ ) components of the color image. The weight of the links is implemented using GF(2) matrix. The ANN networks are also expressed using the following mathematical operations:

$$\begin{aligned}
r_i' &= r_i \cdot w_{11} \oplus g_i \cdot w_{12} \oplus b_i \cdot w_{13}\\
g_i' &= r_i \cdot w_{21} \oplus g_i \cdot w_{22} \oplus b_i \cdot w_{23}\\
b_i' &= r_i \cdot w_{31} \oplus g_i \cdot w_{32} \oplus b_i \cdot w_{33}
\end{aligned} \tag{4.2}$$

 

The values of $r_i', g_i' \text{ and } b_i'$ are then exclusive-or (XOR) with the random number $l_1$ and this random number is generated using LFSR. Using the following process, we get the modified RGB value.

$$\begin{aligned} r_i'' &= r_i' \oplus l_1, \\ g_i'' &= g_i' \oplus l_1, \\ b_i'' &= b_i' \oplus l_1 \end{aligned} \tag{4.3}$$

Here $r_i'', g_i'' \text{ and } b_i''$ are the modified values of the RGB pixels.

4.3. **Alter pixel intensity value**

At this step, we have changed the pixel intensity value of Red $(r_i'')$, Green $(g_i'')$ and Blue $(b_i'')$ (where $i = 1,2,3,\cdots,512 \times 512$) components of the second encrypted image using following two steps:

Step1:

$$\begin{aligned} R_i &= (r_i'' \,||\, r_{i+1}''||r_{i+2}''||r_{i+3}'') \oplus k_1 \\ G_i &= (g_i''||g_{i+1}''||g_{i+2}''||g_{i+3}'') \oplus k_2 \\ B_i &= \left(b_i''||b_{i+1}''||b_{i+2}''||b_{i+3}''\right) \oplus k_3 \end{aligned} \tag{4.4}$$

Where $i = 1,2,3,\cdots,512 \times 512$ and $k_1, k_2 \text{ and } k_3$ are 32 bits random numbers which are determined by the following ways:

$$\begin{aligned} k_1 &= (k_1 \cdot X_i' \cdot 2^{16}) mod\ K \ \oplus k_1 \\ k_2 &= (k_2 \cdot X_i'' \cdot 2^{16}) mod\ K \oplus k_2 \\ k_3 &= (k_3 \cdot X_i''' \cdot 2^{16}) mod\ K \oplus k_3 \end{aligned}$$

Here $X_i', X_i'' \text{ and } X_i'''$ are the values that found from the chaotic system. The initial value of

$$k_1 = 4294967291, \quad k_2 = 4294967279,$$
$$k_3 = 4093082899, \quad K = 4294967295.$$

Step 2:

a)

$$\begin{aligned} R_2' &= R_2 \oplus R_1' \oplus \emptyset(h_1) \\ G_2' &= G_2 \oplus G_i' \oplus \emptyset(h_2) \\ B_2' &= B_2 \oplus B_i' \oplus \emptyset(h_3) \end{aligned}$$

where we consider the initial values of $R_i' = 11, G_1' = 19, B_1' = 23$ and the initial values of $\emptyset(h_1) = 11, \emptyset(h_2) = 29, \ \emptyset(h_3) = 17$

b)

$$\begin{aligned} R_i' &= \emptyset(h_1) \oplus \left((R_i + \emptyset(h_1)) mod\ 253\right) \oplus R_{i-1}' \oplus R_{i-2}' \\ G_i' &= \emptyset(h_2) \oplus \left((G_i + \emptyset(h_2)) mod\ 253\right) \oplus G_{i-1}' \oplus G_{i-2}' \\ B_i' &= \emptyset(h_3) \oplus \left((B_i + \emptyset(h_3)) \ mod\ 253\right) \oplus B_{i-1}' \oplus B_{i-2}' \end{aligned} \tag{4.5}$$

$$C_i = cat(3, R_i', G_i', B_i') \tag{4.6}$$

where $i = 3,4,\cdots,512 \times 512$. The values of $\emptyset(h_1), \emptyset(h_2) \text{ and } \emptyset(h_3)$ are calculated as

$$\begin{aligned} \emptyset(h_1) &= \emptyset(h_1) \oplus R_{i-1}' \oplus G_{i-1}' \oplus B_{i-1}' \oplus R_{i-2}' \\ \emptyset(h_2) &= \emptyset(h_2) \oplus R_{i-1}' \oplus G_{i-1}' \oplus B_{i-1}' \oplus G_{i-2}' \\ \emptyset(h_3) &= \emptyset(h_3) \oplus R_{i-1}' \oplus G_{i-1}' \oplus B_{i-1}' \oplus B_{i-2}' \end{aligned}$$

where $i = 3,4,\cdots,512 \times 512$. Using the above equations we get our final encrypted image $C_i$. In Figure 6, we show the some examples of Image Encryption and Decryption of Lena, Baboon and Peppers image.

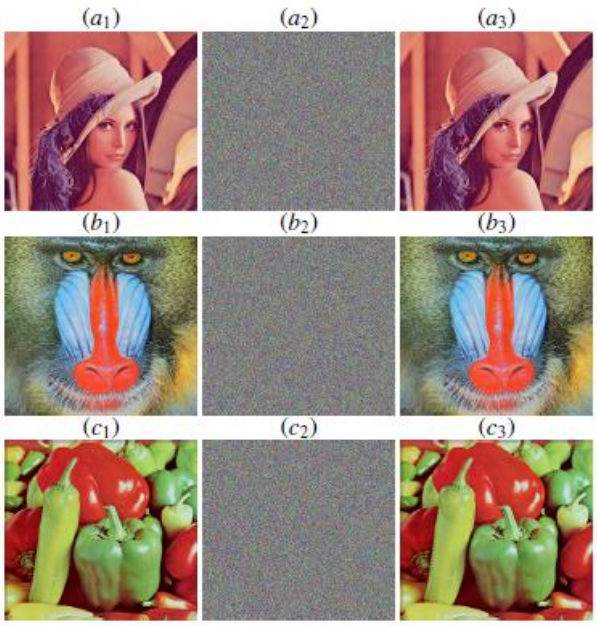


Figure 6: Experimental result of test image:

Lena Image: $(a_1)$ Original, $(a_2)$ Encryption, $(a_3)$ Decryption, Baboon Image: $(b_1)$ Original, $(b_2)$ Encryption, $(b_3)$ Decryption, Peppers Image: $(c_1)$ Original, $(c_2)$ Encryption, $(c_3)$ Decryption

 

## V. STATISTICAL AND SECURITY ANALYSIS OF OUR SCHEME

An encryption scheme has to convert the encrypted image confusing properly so that an unauthorized user cannot access the meaningful information. In the following, we show the histogram analysis, coefficient correlations of two neighbourhood pixels and information entropy.

In our experiment on multiple images, namely Lena, Baboon, and Peppers each of size $512 \times 512$, we have used Matlab 2010a (64 bit) and the configuration of our experimental machine is Microsoft Windows 7 operation system, Intel Core 2 Duo 2 GHz CPU, 3GB memory.

### 5.1. **Histogram Analysis**

The histogram [1, 19] is one of the major parts of the statistical analysis. In Figure 7, we separately represent the histogram of the red component, the green component and the blue component of the color image Lena. The histogram of each component of the encrypted image is distinct from the meaningful image and the values are uniformly distributed in each component of the encrypted image. It can be concluded that the cipher image of all color images has the similar histogram. Thus, the proposed scheme meets the diffusion features very well and also the proposed scheme is protected from any attack with respect to the statistical viewpoint.

### 5.2. **Information entropy**

Information Entropy [1, 10, 11] evaluates the randomness value and the unpredictability of the color images. The information entropy first proposed by Shannon in 1949. We can found the information entropy using the following equation:

$$H(S) = \sum_{i=0}^{2^L-1} P(S_i) log_2 \frac{1}{P(S_i)} \qquad (5.1)$$

where $P(S_i)$ represents the probability of source $S_i$, $L$ is the total amount of pixels represents the source $S_i$ and $H(x)$ is the in-formation entropy. The entropy of the encrypted image should be close to the perfect value that protects the color image from entropy attack. The perfect value of the entropy is 8 and from this perfect value, we can represent 256 gray levels. In Table 2, we represent the entropy of the color images of Lena, Baboon, Peppers and the size of each image is $512 \times 512$ and most of the results are closer to the perfect entropy value. The outcome shows the randomness of the encrypted images and accordingly, indicates the security performance of the proposed cipher.

Table 2: Entropy test of the different cipher images

| | | Red Channel | Green Channel | Blue Channel |
|---|---|---|---|---|
| Lena | Plain Image | 7.2477 | 7.5779 | 6.9559 |
| | Cipher Image | 7.9994 | 7.9994 | 7.9993 |
| Baboon | Plain Image | 7.7067 | 7.4744 | 7.7522 |
| | Cipher Image | 7.9993 | 7.9994 | 7.9993 |
| Peppers | Plain Image | 7.3388 | 7.4963 | 7.0583 |
| | Cipher Image | 7.9993 | 7.9994 | 7.9993 |

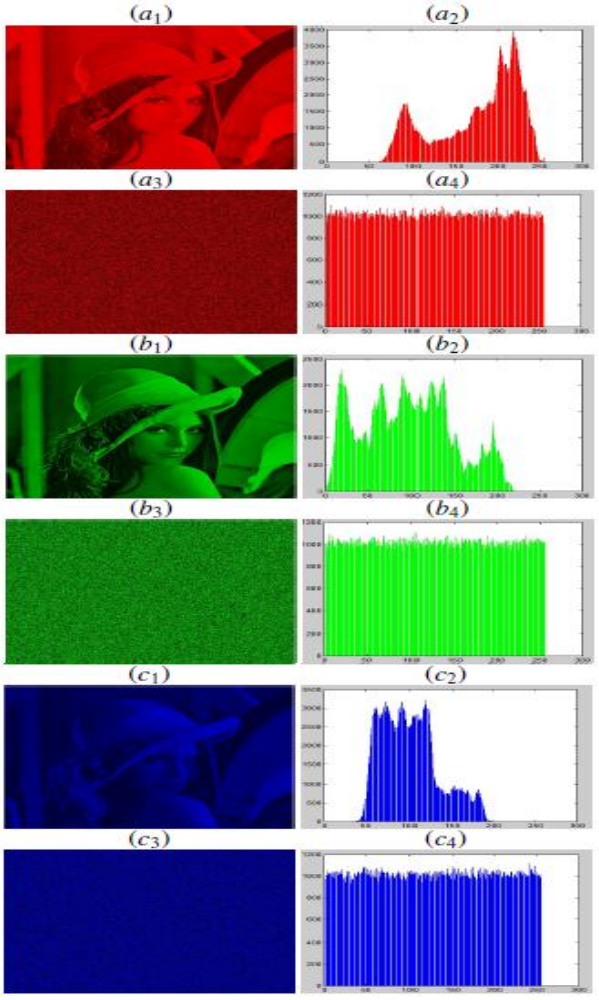


Figure 7: Experimental result of test image:

Lena Red Component ($a_1$) Original Image, ($a_2$) Histogram of Original image, ($a_3$) Encrypted image, ($a_4$) Histogram of Encrypted image,

 

Lena Green Component ($b_1$) Original Image, ($b_2$) Histogram of Original image, ($b_3$) Encrypted image, ($b_4$) Histogram of Encrypted image,

Lena Blue Component ($c_1$) Original Image, ($c_2$) Histogram of Original Image, ($c_3$) Encrypted image, ($c_4$) Histogram of Encrypted image

5.3. Sensitivity analysis

In cryptanalysis [9], an attacker tries to find some clues to crack the protection of the sensitive information. He/she can do it by changing the key or other important information of the cipher text. If the attacker makes the small change to crack our algorithm and he/she might not be succeeded.

5.3.1. Key Sensitivity

This is one of the most important parts of the sensitivity analysis. For decryption, we subdivided the cipher image $C_i$ into Red ($r_i'''$), Green ($g_i'''$) and Blue ($b_i'''$) (where $i = 1,2,3\cdots,512 \times 512$) components. Using the following steps, we implement the decryption algorithm:

Step1:

$$\begin{aligned} R_i' &= (r_i'''||\, r_{i+1}'''||\, r_{i+2}'''||\, r_{i+3}''') \oplus k_1 \\ G_i' &= (g_i'''||\, g_{i+1}'''||\, g_{i+2}'''||\, g_{i+3}''') \oplus k_2 \\ B_i' &= (b_i'''||\, b_{i+1}'''||\, b_{i+2}'''||\, b_{i+3}''') \oplus k_3 \end{aligned} \qquad (5.2)$$

where $i = 1,2,3,\cdots,512 \times 512$ and $k_1, k_2\ and\ k_3$ are 32 bits random numbers.

Step 2:

a)

$$\begin{aligned} R_2 &= R_2' \oplus R_1' \oplus \Phi(h_1) \\ G_2 &= G_2' \oplus G_1' \oplus \Phi(h_2) \\ B_2 &= B_2' \oplus B_1' \oplus \Phi(h_3) \end{aligned}$$

where we consider the initial values of $R_1 = R_1',\ G_1 = G_1',\ B_1 = B_1'$.

b)

$$\begin{aligned} R_i &= \left(\Phi(h_1) \oplus R_i' \oplus R_{i-1}' \oplus R_{i-2}' + 256 - \phi(h_1)\right) mod\ 256 \\ G_i &= \left(\Phi(h_2) \oplus G_i' \oplus G_{i-1}' \oplus G_{i-2}' + 256 - \phi(h_2)\right) mod\ 256 \\ B_i &= \left(\Phi(h_3) \oplus B_i' \oplus B_{i-1}' \oplus B_{i-2}' + 256 - \phi(h_3)\right) mod\ 256 \end{aligned} \qquad (5.3)$$

$$P_i = cat(3, R_i, G_i, B_i) \qquad (5.4)$$

where $i = 3,4,\cdots,512 \times 512$. Using the above equations we get the decrypted image $P_i$.

The values of $\emptyset(h_1)$, $\emptyset(h_2)\ and\ \emptyset(h_3)$ are calculated as

$$\begin{aligned} \Phi(h_1) &= \Phi(h_1) \oplus R_{i-1} \oplus G_{i-1} \oplus B_{i-1} \oplus R_{i-2} \\ \Phi(h_2) &= \Phi(h_2) \oplus R_{i-1} \oplus G_{i-1} \oplus B_{i-1} \oplus G_{i-2} \\ \Phi(h_3) &= \Phi(h_3) \oplus R_{i-1} \oplus G_{i-1} \oplus B_{i-1} \oplus B_{i-2} \end{aligned}$$

where $i = 3,4,\cdots,512 \times 512$.

Here the secret keys are

$$k_1 = 4294967291,\quad k_2 = 4294967279,$$
$$k_3 = 4093082899,\quad \mathrm{K} = 4294967295$$

and ($R_1' = 11,\ G_1' = 19,\ B_1' = 23$) and ($\emptyset(h_1) = 11,\ \emptyset(h_2) = 29,\ \emptyset(h_3) = 17$). These secret keys are used to decrypt the cipher image into original form. But, if any small change is made on these secret information that is

$$k_1 = 4294967292,\quad k_2 = 3294967279,$$
$$k_3 = 4193082899,\quad \mathrm{K} = 4294967295$$

and ($R_1' = 12,\ G_1' = 29,\ B_1' = 34$) and ($\emptyset(h_1) = 22,\ \emptyset(h_2) = 39,\ \emptyset(h_3) = 18$), the attacker unable to decrypt the original image (see Figure 8).


Figure 8: Experimental result of test image

(a1) Decrypted with the appropriate key of Lena image, (a2) Decrypted with the incorrect key of Lena image

5.3.2. **Plain image sensitivity**

The unified average changing intensity (UACI) and the number of pixels change rate (NPCR) are the two methods to de-scribe the plain text sensitivity. NPCR defines that only one pixel of the meaningful image is altered and UACI defines the average intensity of the dissimilarities between the meaningful image and cipher image. These two approaches describe that a slight altering of the plain image, cipher image should alter extremely so that an attacker unable to crack the original information. The NPCR gets closer to 100 percents, and UACI gets closer to 33.50 percentages. These two approaches are more useful for the

 

cryptosystem to protect the plaintext attack. The following equations describe the NPCR and UACI [1, 2, 4] methods:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \cdot H} \cdot (100) \qquad (5.5)$$

$$UACI = \left| \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{L} \right| \cdot \frac{(100)}{W \cdot H} \qquad (5.6)$$

where $C_1$ and $C_2$ are two cipher images with the equal size $W \times H$ ($W$ is column and $H$ is row) and $L$ is the maximum intensity of the image. If $C_1(i,j) = C_2(i,j)$, then $D(i,j) = 1$; otherwise, $D(i,j) = 0$. After encryption, most of the pixels of the cypher images have altered. It is clearly understandable that the disparity between the neighborhood pixels became larger. Therefore, the proposed scheme is sensitive to the plain image. Table 3, Table 4 and Table 5 show the result of NPCR and UACI of different ciphered images when there is a single pixel distinction between the plain images. It shows that NPCR is near the rate 100, but UACI varies for Lena, Baboon and Pappers images.

Table 3: Outcome of NPCR and UACI of "Lena"

| | Red Channel | Green Channel | Blue Channel |
|---|---|---|---|
| NPCR | 99.6155 | 99.6223 | 99.6120 |
| UACI | 33.5277 | 33.5046 | 33.4465 |

Table 4: Outcome of NPCR and UACI of "Baboon"

| | Red Channel | Green Channel | Blue Channel |
|---|---|---|---|
| NPCR | 99.5953 | 99.6109 | 99.5930 |
| UACI | 33.4108 | 33.4707 | 33.5075 |

Table 5: Outcome of NPCR and UACI of "Pappers"

| | Red Channel | Green Channel | Blue Channel |
|---|---|---|---|
| NPCR | 99.5876 | 99.6006 | 99.5979 |
| UACI | 33.4572 | 33.4229 | 33.4862 |

### 5.4. **Correlations of two adjacent pixels**

The statistical analysis is done on the different encrypted images and determines the initial relationship between two adjacent pixels by calculating the correlation [1, 2] of pixels in $x$-direction (horizontal), $y$-direction (vertical) and $z$-direction (diagonal). There can have a high correlation among the pixels of the original images as their values are close to each other. Thus, in the cipher image, these correlations should be weakened. We calculate correlation separately in $x$-direction (horizontal), $y$-direction (vertical) and $z$-direction (diagonal) from the color images such as Lena, Baboon, and Peppers. The correlation coefficient of each image is calculated using the following equation:

$$r = \frac{\sum dx \cdot dy}{\sqrt{\sum dx^2 \cdot \sum dy^2}} \qquad (5.7)$$

where $dx = (x - \bar{x})$, $dy = (y - \bar{y})$, $\bar{x} = \frac{\sum dx}{n}$, $\bar{y} = \frac{\sum dy}{n}$ and $n$ is the number of values.

Table 6 shows the coefficients correlation of two neighbor-hood pixels in $x, y$ and $z$ directions.

Table 6: Correlations of two adjacent pixels

| | | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| Lena | Plain Image | 0.9646 | 0.9768 | 0.9265 |
| | Cipher Image | 0.1830 | 0.1648 | 0.0233 |
| Baboon | Plain Image | 0.9141 | 0.9172 | 0.8957 |
| | Cipher Image | 0.1565 | 0.1917 | 0.0438 |
| Peppers | Plain Image | 0.9701 | 0.9683 | 0.9382 |
| | Cipher Image | 0.1675 | 0.2329 | 0.0313 |

## V. COMPARISON

We compare our proposed scheme with several existing schemes in [1],[2] and [10], where we use the same data set of the color image. For the fair comparison, the proposed scheme considers the image Lena as a standard image. The NPCR, UACI, and entropy of the encrypted images are calculated and the results are furnished in the Table 7 and Table 8.

Table 7: NPCR of "Lena" cipher image

| Image encryption algorithm | Red Channel | Green Channel | Blue Channel |
|---|---|---|---|
| Our scheme | 99.6155 | 99.6223 | 99.6120 |
| Wang et al.'s scheme [1] | 99.6010 | 99.6120 | 99.6109 |
| Xiao et al.'s scheme [2] | 99.57123 | 99.61872 | 99.69223 |
| Rhouma et al.'s scheme [10] | 99.5660 | 99.5860 | 99.5880 |

 

Table 8: Information Entropy of "Lena" cipher image

| Image encryption algorithm | Red Chan-nel | Green Chan-nel | Blue Chan-nel |
|---|---|---|---|
| Our scheme | 7.9994 | 7.9994 | 7.9993 |
| Wang et al.'s scheme [1] | 7.999369 | 7.999299 | 7.999319 |
| Lahieb et al.'s scheme [11] | 7.9993 | 7.9992 | 7.9991 |
| Rhouma et al.'s scheme [10] | 7.9732 | 7.9750 | 7.9715 |

## VII. CONCLUSION

In this article, we have proposed a color image encryption scheme using a Single Layer Artificial Neural Network and Buffer Shuffling. Using RGB buffer shuffling, we have scram-bled the red components, green components and blue components of the pixels based on the chaotic map and using the artificial neural network. We have modified the intensity value of each pixel. Then using pixel alternation method, we get the cipher image. Different experimental outcomes and analysis have shown that our scheme is good. We have shown that our scheme is able to protect common known attacks.

## REFERENCES


[1] W. Yao, X. Zhang, Z. Zheng and W. Qiu, "A color image encryption algorithm using 4-pixel Feistel structure and multiple chaotic systems", Non-linear Dynamics, Vol. 81, pp. 151-168, 2015.

[2] X. J. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu and J. Ma, "An image encryption algorithm based on the perturbed high-dimensional chaotic map", Nonlinear Dynamics, Vol. 80, pp. 1493-1508, 2015.

[3] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications", Commun Nonlinear Sci Numer Simulat, Vol. 24, pp. 98-116, 2015.

[4] M. Chauhan and R. Prajapati, "Image encryption using chaotic based artificial neural network", International Journal of Scientific Engineering Research, Vol. 5, pp. 2229-5518, 2014.

[5] Dr. S. Ramakrishnan, R. R. Rakshitha, V.Gayathiri and P.Kalaiyarasi, "Neural network based image encryption and authentication using chaotic maps", International Journal of Current Trends in Engineering Research, Vol. 3, pp. 29-37, 2017.

[6] P. Alfke, "Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators", XAPP 052, (Version 1.1), July 7,1996.

[7] H. Bahjat and M. A. Salih, "Speed Image Encryption Scheme using Dynamic Galois Field GF(P) Matrices", International Journal of Computer Applications, Vol. 89, pp. 0975-8887, 2014.

[8] Q. A. Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling", I. J. Computer Network and Information Security, Vol. 7, pp. 43-50, 2013.

[9] W. S. Yap, R. C. W. Phan, W. C. Yau, S. H. Heng "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map", Nonlinear Dynamics, Vol. 80, pp. 483-1491, 2015.

[10] R. Rhouma, S. Meherzi and S. Belghith "OCML-based colour image encryption", Science Direct, Vol. 40, pp. 309-318, 2009.

[11] L. M. Jawad and G. Sulong "Chaotic map-embedded Blowfish algorithm for security enhancement of color image encryption", Nonlinear Dynamics, Vol. 81, pp. 2079-2093, 2015.

[12] D. Arroyo, S. Li, J. M. Amigoc, G. Alvarez and R. Rhouma "Comment on - Image encryption with chaotically coupled chaotic maps", Science Direct, Vol. 239, pp. 1002-1006, 2010.

[13] C. K. Huang and H. H. Nien "Multi chaotic systems based pixel shuffle for image encryption", Science Direct, Vol. 282, pp. 2123-2127, 2009.

[14] L. Hongjun and W. Xingyuan "Color image encryption based on one-time keys and robust chaotic maps", Science Direct, Vol. 59, pp. 3320-3327, 2010.

[15] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez and G. Chen "On the security defects of an image encryption scheme", Science Direct, Vol. 27, pp. 1371-1381, 2009.

[16] W. Chen and X. Chen "Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain", Science Direct, Vol. 284, pp. 3913-3917, 2011.

[17] N. R. Kumar , G. Manikandan , R. B. Krishnan , N. R. Raajan and N. Sairam "A reversible visual cryptography technique for color images using Galois field arithmetic", Biomedical Research, Vol. 28 (5), pp. 2036-2039, 2017.

[18] S. N. Lagmiri , N. E. Alami and J. E. Alami "Color and gray images encryption algorithm using chaotic systems of different dimensions ", IJC-SNS International Journal of Computer Science and Network Security, Vol. 18, pp. 1, 2018.

[19] S. Banerjee, L. Rondoni, S. Mukhopadhyay and A. P. Misra "Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption ", Optics Communications, Vol. 284, pp. 2278-2291, 2011.

[20] M. Joshi, C. Shakher and K. Singh "Fractional Fourier transform based image multiplexing and encryption technique for four-color images using input images as keys ", Optics Communications, Vol. 283, pp. 2496-2505, 2001.

[21] Y. Tang, Z. Wanga and J. A. Fang, "Image encryption using chaotic coupled map lattices with time-varying delays", Commun Nonlinear Sci Nu-mer Simulat, Vol. 15, pp. 2456-2468, 2010.

[22] L. Hongjun and W. Xingyuan, "Color image encryption based on one-time keys and robust chaotic maps", Computers and Mathematics with Applications, Vol. 59, pp. 3320-3327, 2010.

[23] W. Chen and X. Chen, "Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain", Optics Communications, Vol. 284, pp. 3913-3917, 2011.

[24] Jyotsna, A. Papola, "An Image Encryption Using Chaos Algorithm Based on GLCM and PCA", International Journal of Computer Sciences and Engineering, Vol. 6(3), pp. 76-81, 2018.

[25] M. Dasgupta, J. K. Mandal, "Bit-plane Oriented Image Encryption through Prime-Nonprime based Positional Substitution (BPIEPNPS)", International Journal of Computer Sciences and Engineering, Vol. 4(6), pp. 65-70, 2016.


 

**Authors Profile**

*Dipankar Dey* pursed B.Sc. Math Honours from Burdwan University, West Bengal in 2001 and MCA Maulana Abul Kalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology), in 2005. He is currently pursuing Ph.D. from University of Mysore, Karnataka and currently working as an Assistant Professor in Global Institute of Science and Technology, Haldia, West Bengal, in Computer Science Technology Department, since 2006. His main research work focuses on Image encryption using chaotic map. He has 12 years of teaching experience.

*Dr. Soumen Paul* pursued M.Stat from Indian Statistical Institute; Kolkata on the year of 1990 and completed M.Tech in Information Technology from Punjabi University on the year of 2003. He got Ph.D award from Jadavpur University on the year of 2014. Currently he is working at Haldia Institute of Technology as a professor and head of the Department of Information Technology. He has sixteen years teaching and ten years industrial experience.

 