Image Encryption Based on Pixel Permutation and Text Based Pixel Substitution

Pooja Hardiya[1] Ravindra Gupta[2]
[1]M.Tech. Student [2]Associate Professor
[1,2]Department of Computer Science & Engineering
[1,2] R.K.D.F. Institute of Science & Technology, Bhopal, Madhya Pradesh, India

Abstract— Digital image Encryption techniques play a very important role to prevent image from unauthorized access. There are many types of methods available that can do Image Encryption, and the majority of them are scrambling algorithms based on pixel shuffling, which cannot change the histogram of an image. Hence, their security performances are not good. The encryption method that combines the pixel exchanging and gray level changing can handles reach a good chaotic effect. In this paper we focus on an image encryption technique based on pixel wise shuffling with the help of skew tent map and text based pixel substitution. The PSNR, NPCR and CC obtained by our technique shows that the proposed technique gives better result than the existing techniques.

Keywords: Encryption, Scrambling, Pixel Shuffling, Information Security, Skew Tent Map

I. INTRODUCTION

Due to some inherent feature of image like low cost and high availability, usage of communication network has increased and it becomes a reason for rapid growth of the internet in the digital world today. In our society digital images play a more significant role than the traditional texts and it need serious protection of user's privacy for all applications. So the security of digital images has become more important and attracted much attention. The security of digital image can be achieved by digital image encryption technique. Basically Image Encryption means that convert the image into unreadable format so that third party cannot interpret them. Many digital services require reliable security in storage and transmission of digital images [1].

To prevent image from unauthorized access, Encryption techniques of digital images play a very important role .Since Digital images are exchanged over various types of networks and a large part of this digital information is either confidential or private. So Encryption is the preferred technique for protecting the transmitting information. There are various encryption systems to encrypt and decrypt image data. But, it can be said that there is no single encryption algorithm which satisfies the different image types [2].

In general, most of the available traditional encryption algorithms are used for text data. Although we can use the traditional encryption algorithm to encrypt images directly, this may not be a good idea for some reasons. First, image data have their special features such as high redundancy, and high correlation among pixels. Second, they are usually huge in size that makes traditional encryption methods difficult to apply and slow to process. third, the decrypted text must be equal to the original text but this requirement is not necessary for image data because characteristic of human insight, a decrypted image containing small distortion is usually acceptable .So the algorithms that are good for textual data may not be suitable for multimedia data, Even though triple data encryption standard (T-DES) and international data encryption algorithm (IDEA) can achieve high security, they may not be suitable for multimedia applications Therefore, well known encryption algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Standard (IDEA) were built for textual data not for multimedia data [3-4].

Now, there are many types of methods available that can do Image Encryption [5-8], and the majority of them are scrambling algorithms based on pixel shuffling. In 2011 Zhang et al. proposed an image encryption method based on total shuffling scheme [5]. This method is characterized in that the secret code stream used in encryption is not only associated with the key, but also related to the plain image. Because the random number used in the diffusion process is obtained by iterating the skew tent map, and the number of iterations is determined by the previous pixel value of cipher image which includes the information of previous pixel value of plain image, the next random number is indirectly related to the previous pixel value of plain image. This plain image related encryption method is strongly against chosen plaintext attacks [6]. However, the first secret code is not safe enough to resist the chosen plaintext attack, which is pointed out and crypt analyzed in [7].

In 2013, Eslami et al. suggested an improved algorithm [8] over these shortcomings described in [7]. Two major improvements, such as using previous cipher image pixels to execute "add modulus and xor" operations instead of plain image pixels, and enlarging the iteration times of chaotic system in every round, make the image encryption scheme proposed in [5] higher security against the chosen plaintext attacks with slower encryption speed as a trade off. Yong zhang [9] proposed a lookup table based encryption improvement on the schemes proposed in [5, 8] to improve the encryption speed.

Pixels shuffling based image encryption techniques have one problem that it cannot change the histogram of an image. Hence, their security performances are not good. The encryption method that combines the pixel exchanging and gray level changing can handles reach a good chaotic effect. Our proposed method does this job. The latter chapters are arranged as follows: In section 2 performance parameters are briefly introduced. Section 3 describes our proposed method based on the permutation and substitution. Section 4 presents some representative parameters to describe encryption quality. Section 5 shows the result of our method and the comparative performance analyses of our method with [5, 8, 9] .Section 6 concludes the paper

II. PERFORMANCE PARAMETERS

The performance of the encryption technique is measured by some of the basic parameters which are listed below: [10].

A. Visual Degradation (VD)

Visual degradation identifies the perceptual distortion of the image data with respect to the plain image.

B. Compression Friendliness (CF)

Compression Friendliness measures no or very little impact on data compression efficiency on the image. Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption.

C. Format Compliance (FC)

Format Compliance parameter is used to measures compliance the encrypted bit stream with the compressor. Standard decoder should be able to decode the encrypted bit stream without decryption.

D. Encryption Ratio (ER)

This measures the amount of data to be encrypted. Encryption ratio should be minimized so that the computational complexity can be reduced.

E. Speed (S)

This parameter measures how fast the encryption and decryption algorithms enough to meet real time requirements.

F. Cryptographic Security (CS)

Cryptographic security is used to identify whether encryption scheme is secure against different plaintext-cipher text attack.

III. PROPOSED METHODOLOGY

Suppose X is the original 8-bit gray-level cover-image of M×N pixels. It is denoted as:

$$X=\{x_{ij} \mid 1\le i\le M,\ 1\le j\le N,\ x_{ij}\in\{0,1,...,255\}\} \quad (1)$$

The proposed encryption scheme consists of two procedures, i.e. permutation and substitution. The pixel permutation procedure is shown as follows:

(1) Convert the 2-D 8-bit grayscale and of size M×N, into 1-D which is denoted by $X=\{x_0,x_1,...,x_{MN-1}\}$ using from top to bottom and then from left to right scanning method.

(2) Iterate eq.2 to obtain a pseudo random sequence of size M×N, denoted by $R=\{r_0,r_1,...,r_{MN-1}\}$.

$$F(x)=\begin{cases} x/p & x\in[0,p] \\ (1-x)/(1-p), & x\in(p,1] \end{cases} \quad (2)$$

(3) Sort R in ascending order to get $S=\{s_0,s_1,...,s_{MN-1}\}$.

(4) According to the relationship of R and S, a scrambling vector $T=\{t_0,t_1,...,t_{MN-1}\}$ is obtained such that $s_i=r_{t_i}$, i = 0, 1, …, MN-1.

(5) Permute the plain image X with T to get $Y=\{y_0,y_1,...,y_{MN-1}\}$ such that $y=x_{t_i}$, i = 0, 1, …, MN-1.

Then the substitution procedure is as follows:

(1) Convert the inserted text into binary form with the help of its ASCII code. And then determine the length of binary code .Let P is the n-bit binary text represented as:

$$P=\{p_i \mid 1\le i\le n,\ p_i\in\{0,1\}\}.$$

(2) Resize the *P* to same dimension as permuted image *Y* by using following pseudo code:

```
For i = 1 to M
    For j=1 to N
        K(i,j)=mod((P(next)* fact),255);
        next=next+1;
    end
end
```

Initially *next* and *fact* is set to 1. when *next* is reached to size of P (i.e. n) then again it's values is set to 1.but this time it is multiplied by new *fact*.

(3) Performs the bit wise operation X-OR operator to generate the encrypted image of length M*N pixels.

$$Z=Y\oplus K$$

Where

$$Z=\{z_{ij} \mid 1\le i\le M,1\le i\le N,c_i\in\{0\ to\ 255\}$$

$$\text{and } z_i=y_i\oplus k_i\}.$$

– Finally we get the encrypted image Z and this image is ready to transmit.

IV. EVALUATION METRICS

In this investigation, the set of criteria for comparing the selected algorithms are: the MSE, PSNR, UAIC NPCR and CC.

A. Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [11] can be defined as the measure of average of the squares of the difference between the intensities of the Encrypted image and the original image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-C'(i,j))^2$$

Where C (i, j) is the original image and C' (i, j) is the encrypted image. A large value for MSE means that the image is of poor quality.

B. Peak signal to noise ratio (PSNR)

The PSNR depicts the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover and encrypted image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR=20\log 255^2/MSE$$

A low value of PSNR shows that the constructed image is of poor quality.

C. UAIC and NPCR

Attacker tries to find out a relationship between the plain image and the cipher-image, with the help of studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. Attacker can observes the change of the plain-image by trying to make a slight change such as modifying one pixel of the encrypted image. Two common measures are used to test the influence of one pixel change on the whole encrypted image by the proposed algorithm [12]:

Number of Pixel Change Rate (NPCR)

$$NPCR=\frac{\sum_{i,j} D(i,j)}{W\times H}\times 100\%$$

Unified Average Change Intensity(UACI)

$$UACI=\frac{1}{W\times H}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right]\times 100\%$$

C1 and C2: two ciphered images, whose corresponding original images have only one-pixel difference. C1 and C2 have the same size.

C1 (i, j) and C2 (i, j): grey-scale values of the pixels at grid (i,j).

D(i, j): determined by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0.W and H: columns and rows of the image.

D. The Correlation Coefficient

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images [11]. This metric can be calculated as follows:

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where x and y are the gray-scale values of two pixels at the same indices in the plain and cipher images. In numerical computations, the following discrete formulas can be used:

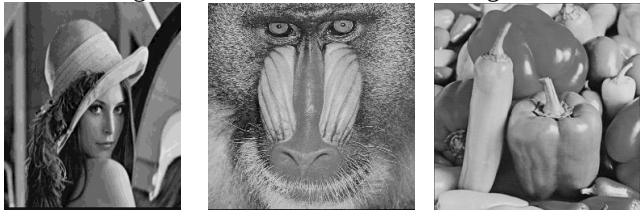
$$E(x)=\frac{1}{L}\sum_{l=1}^{L} X_l$$

$$D(x)=\frac{1}{L}\sum_{l=1}^{L}\left(x_l-E(x)\right)^2$$

$$\operatorname{cov}(x,y)=\frac{1}{L}\sum_{l=1}^{L}\left(x_1-E(x)\right)\left(y_1-E(y)\right)$$

V. Experimental Results

In the experiment, we do image encryption using permutation and substitution technique and we are taken different images of size 512× 512 shown in Figure 1.



(a)Lena (b) Baboon (c) Pepper

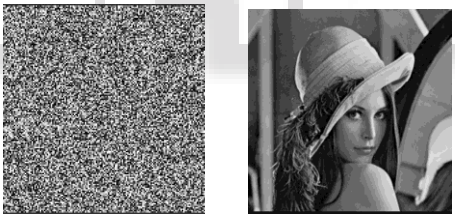
(d) Plane (e) Butterfly (f) Cat

Fig. 1: Test Images of size 512×512

To demonstrated our method we used the gray image Lena as Shown in Fig. 2(a), The results after permutation and text substitution with the help of secret key (r0=.123456789 and txt='abcdefgh') are shown as in Fig. 2(b) and 2(c) respectively. The pixel shuffling effect is very good and the encrypted image is very like the salt and paper noise. Figure 2(d) is the result of decryption, comparing with original image as shown in Figure 2(a), there is nothing to be lost.

Fig.3 (a) is the histogram of original image Lena. Figure 3(b) is the histogram of the encrypted image permuted by the proposed method .fig 3 shows that the histogram of the both image are not same so we can say that in encrypted image, the gray values of pixels are changed .

(a) original image (b) permuted image



(c)substituted permuted image (d) Decrypted image

Fig. 1: Results after image encryption and Decryption system for Lena.

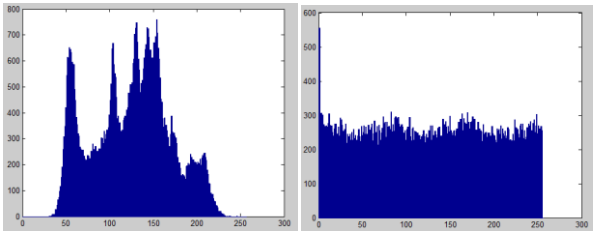


Fig. 1: Histograms of the image Encryption and Decryption system for Lena

The Average quality parameters between the corresponding pixels values of the six encrypted images Lena, Baboon, Papper, Airplane, Butterfly, and Cat are tabulated in Table I.

Images	PSNR (17.5735)	UACI (30.11)	NPCR (99.615)	CC (0.0035)
Lena	18.6664	28.4259	99.646	0.0041
Baboon	19.0249	27.8381	99.614	0.0044
Pepper	18.1665	28.9966	99.5728	0.0040
Plane	16.1514	32.0864	99.5278	0.0026
Butterfly	18.9072	27.992	99.688	0.0037
Cat	14.5249	35.3464	99.602	0.0024

Table 1: result of quality parameters on different image

We take the plain image Lena as an example to do 100 times of experiments, in each experiment randomly generate the secret key, and then calculate the NPCR and UACI and CC of produced cipher images. The average value of NPCR, UACI and CC are tabulated in Table II. From Table II, we can say that NPCR are better than that obtained using the other considered methods. We can see also from Tables II that the plain image is highly correlated in horizontal, vertical and diagonal directions, while the correlation coefficients of two adjacent pixels in proposed methods are close to zero, which demonstrate the proposed methods can well resist the statistical attacks. Fig 5 and Fig 6 shows the comparison graph of proposed method with other considered method with respect to NPCR and CC respectively.

Methods	NPCR	UACI	CC
Zhang et.al	99.6100	33.4613	0.0094
Eslami et.al.	99.6115	33.4622	0.0481
Yong Zhang	99.6094	**33.4635**	0.0172
Proposed	**99.6235**	32.4585	0.0036

Table 2: comparative analysis of proposed encryption technique

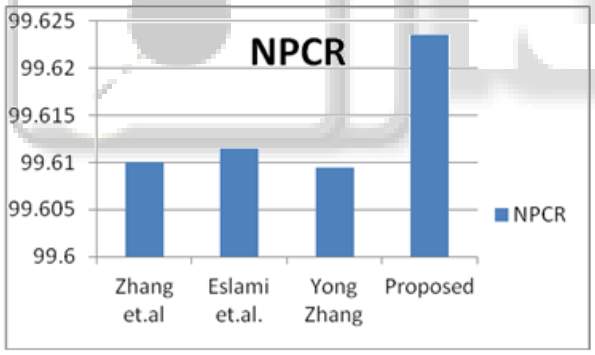


Fig. 1: Shows Average NPCR comparison with different image Encryption Methods.

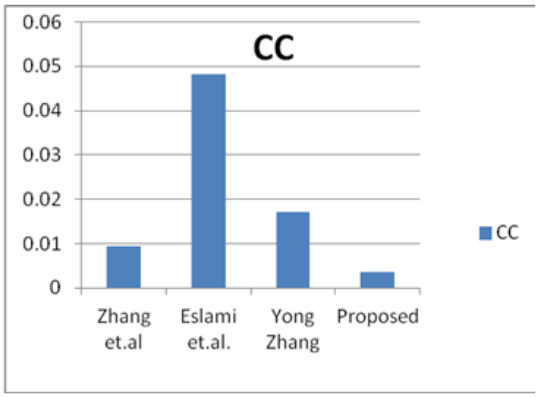


Fig. 1: Shows average Correlation between pixel values and compare different image Encryption Methods.

VI. Conclusion

In this paper we proposed a image encryption technique based on pixel wise shuffling with the help of skew tent map and text based pixel substitution. We have designed our image Encryption and Decryption System using MATLAB 7.8.0 to accomplish this research work. We have evaluated our proposed image Encryption and Decryption System on gray Scale image of 512*512. The experimental result proved that Correlation between pixel values is significantly decreased. The PSNR and NPCR obtained by our technique shows that the proposed technique gives better result than the existing techniques. We will future investigate in our proposed algorithm also can be applying to color image.

References

[1] Öztürk and I. Sogukpınar, "Analysis and comparison of image encryption algorithms," Transactions on Engineering, Computing and Technology, vol. 3, pp. 1305-5313, 2004.
[2] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature," Optics Communications, Vol-2 I 8 (2203), 229-234.
[3] V. Potdar and E. Chang, "Disguising text cryptography using image cryptography," International Network Conference in Plymouth, UK, 6 - 9 July, 2004.
[4] X. Li, J. Knipe, and H. Cheng, "Image Compression and Encryption Using Tree Structures," Pattern Recognition Letters, Vol. 18, No. 8, pp. 2439 2451, 1997.
[5] Zhang, and Q. Liu, "A novel image encryption method based on total shuffling scheme," Opt. Commun. vol. 284, pp. 2775-2780, 2011.
[6] X. Wang and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme," Opt. Commun. vol. 284, pp. 5804-5807, 2011.
[7] Yue Wu, Joseph P. Noonan, and Sos Agaian, NPCR and UACI Ran- domness "Tests for Image Encryption," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011.
[8] Y. Zhang, J. Xia, P. Cai, and B. Chen, "Plaintext related two-level secret key image encryption scheme," TELKOMNIKA. vol. 10, pp. 1254-1262, 2012.
[9] Payal Sharma, Manju Godara, Ramanpreet Singh, "Digital Image Encryption Techniques: A Review," International Journal of Computing & Business Research, 2012.
[10] Jawad Ahmad and Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes," International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04.
[11] Z. Eslami, and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," Opt. Commun. vol. 286, pp. 51-55, 2013.
[12] Yong Zhang, "Encryption Speed Improvement on Total Shuffling," International Conference on Sensor Network Security Technology and Privacy Communication System, 2013.

