Image Encryption using Discrete Radon Transformation and Non chaotic Substitution

K SHANKAR, NAVEED AHAMMED, M SHIVAKUMAR
Dept of EEE , MRIET

***Abstract*—In this paper, transformation and substitution based symmetric key encryption algorithm is proposed. Strong correlation between the adjacent pixels can be observed in the multimedia images. Encryption can be made effective by changing both position and value of each pixel in the image. In the proposed algorithm, each pixel position is scrambled using discrete radon transformation (DRT) and pixel value is varied using non chaotic substitution and permutation. The key length used is 64 bits. The secrete key is divided into eight separate keys each of length 8 bits and these are used to change the pixel position along with DRT. Simultaneously, the secret key is subjected for eight set of initial permutations and each set is used to change the pixel value of the image using exclusive-OR operation.**

Keywords— Symmetric key encryption; Correlation; Discrete Radon Transformation; Non chaotic substitution; Exclusive-OR

I. INTRODUCTION

A secured information transaction system is required for day to day multimedia communication. Hiding the original information by an apparent (cipher) is the major task for peer to peer data transaction. In cryptography and steganography, there are plenty of methods available for hiding the text as well as multimedia data. The encryption involves the conversion of original data into cipher data and the decryption is the inverse process of encryption. The encryption technique is widely classified into two classes: symmetric key encryption and asymmetric key encryption. The key used in the symmetric key encryption technique is same for both encryption as well as decryption and different keys are used for both encryption and decryption in asymmetric key encryption process.

Multimedia data are characterized with high redundancy. Each pixel value is strongly correlated with the neighboring pixels. The most popular encryption algorithms such as DES, AES, RSA and IDES are efficiently applicable for text data [1]. Image encryption involves two major processes: change in the pixel position and change in the pixel value. Both value transformation and position permutation are adopted in the proposed algorithm where value transformation is performed using DRT and position permutation is made using non chaotic substitution techniques.

II. RELATED WORK

Digital image encryption technique involves three major classes: position permutation, value transformation and visual transformation. Affine transformation based digital image encryption system has been described by Amitava Nag, Jyoti Prakash Singh, Srabani Khan and Saswati Ghosh [1]. The pixel position is shuffled by affine transformation and the pixel value is altered by XOR operation. The key length used is considerably less compared to other transformation algorithms.

Encryption of multimedia data based on discrete chaotic map has been proposed by Salwa K. Abd-El-Hafiz, Sherif H. AbdElHaleem and Ahmed G. Radwan [2]. In this paper, they explained three different permutation techniques to achieve shannon's confusion and diffusion properties.

In fractional Fourier transformation based image encryption algorithm, the image is divided into number of blocks and then each block is subjected for transformation [3]. Ahmed G. Radwana, Sherif H. AbdElHaleema and Salwa K. Abd-El-Hafiza presented non chaotic substitution and permutation method of image encryption. Fractal and chess based substitution and permutation methods has been adopted to change both pixel position and pixel value [4]. In hyper chaotic system based text and image encryption technique, the secret key is first subjected for hyper chaotic generator which performs permutation such that bruit force attack can be resisted for some extent [5]. Adrian-Viorel Diaconu, Valeriu Ionescu, Gabriel Iana and Jose Manuel Lopez-Guede has presented bit level permutation based image encryption technique. By this method, they achieved a considerable reduction of Fridrich's structure based image encryption scheme [6]. In quick Response (QR) code based image encryption, discrete wavelet transformation is used for embedding QR

code [7].

Image encryption can also be done using matrix transformation [8]. Self-invertible randomly generated matrix is used as encryption key. Ramtin Mojtahedi Saffari and Sattar Mirzakuchaki has explained image encryption based on discrete wavelet transformation and Haar transformation [9]. In this algorithm, two dimensional logistic map is used to generate private key. In Latin square and chaotic map based image encryption scheme, cellular neural network is used to generate chaotic sequence [10].

III. PROPOSED SCHEME

A 64 bit secret key is used in the proposed symmetric key encryption algorithm. In the first stage, the secret key is divided into 8 separate keys as $X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7$ each with 8 bits. Simultaneously the 64 bit input key is subjected for 8 separate group of initial permutations as P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7. In the next phase the 256x256 grayscale image is subjected for discrete radon transformation (DRT) in order to shuffle the pixel positions for 8 rounds along with X_0 to X_7. In the last phase, the pixel value of the image is changed by non-chaotic substitution and permutation using P_0 to P_7. Fig. 1 shows the flow chart of proposed encryption algorithm.

Algorithm 1: Encryption Algorithm
Input: A 256x256 gray scale image M. And 64 bits secret Key.
Step1: Split 64 bits secret key into X_0, X_1, X_2, X_3, X_4, X_5, X_6, and X_7 each with 8 bits.
Step2: Original image M(x,y) is transformed to cipher image $C^{l}(\rho,\theta)$ using Discrete Radon transformation along with key for 8 rounds.

$$C_0^{l}(\rho,\theta) = DRT(M(x,y))$$

$$C_1^{l}(\rho,\theta) = C_0^{l}(\rho,\theta) \text{ xor } X_0$$
$$C_2^{l}(\rho,\theta) = C_1^{l}(\rho,\theta) \text{ xor } X_1$$
$$C_3^{l}(\rho,\theta) = C_2^{l}(\rho,\theta) \text{ xor } X_2$$
$$C_4^{l}(\rho,\theta) = C_3^{l}(\rho,\theta) \text{ xor } X_3$$
$$C_5^{l}(\rho,\theta) = C_4^{l}(\rho,\theta) \text{ xor } X_4$$
$$C_6^{l}(\rho,\theta) = C_5^{l}(\rho,\theta) \text{ xor } X_5$$
$$C_7^{l}(\rho,\theta) = C_6^{l}(\rho,\theta) \text{ xor } X_6$$
$$C_8^{l}(\rho,\theta) = C_7^{l}(\rho,\theta) \text{ xor } X_7$$

Step3: The secret key is subjected for 8 set of initial permutations as P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7.
Step4: Non Chaotic substitution for each pixel value is performed using P_0 to P_7.

$$C_{i+9}^{l}(\rho,\theta) = C_8^{l}(\rho,\theta) \text{ xor } P_i \qquad 0 \le i \le 7$$

Output: Cipher image C

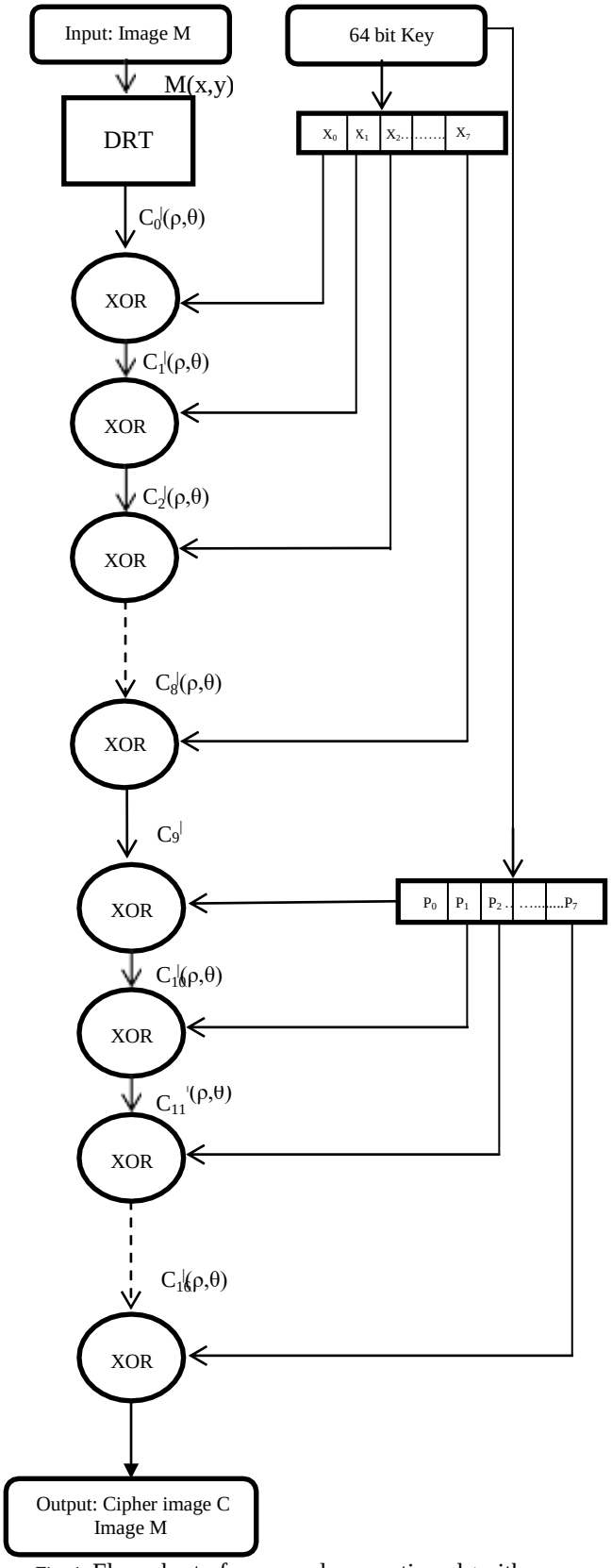

Fig. 1. Flow chart of proposed encryption algorithm.

Algorithm 2: Decryption Algorithm
Input: Cipher image C and 64 bits secret Key.
Step1: The secret key is subjected for 8 set of initial permutations as P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7.
Step2: Non Chaotic re-substitution for each pixel value of $C^{|}(\rho,\theta)$ is performed using P_0 to P_7.

$$C_8^{|}(\rho,\theta) = C_{i+9}^{|}(\rho,\theta) \text{ xor } P_i \qquad 0 \le i \le 7$$

Step3: Split 64 bits secret key into X_0, X_1, X_2, X_3, X_4, X_5, X_6, and X_7 each with 8 bits.
Step4: Cipher image $C^{|}(\rho,\theta)$ is subjected for Inverse Discrete Radon transformation for 8 rounds.

$$C_7^{|}(\rho,\theta) = C_8^{|}(\rho,\theta) \text{ xor } X_7$$
$$C_6^{|}(\rho,\theta) = C_7^{|}(\rho,\theta) \text{ xor } X_6$$
$$C_5^{|}(\rho,\theta) = C_6^{|}(\rho,\theta) \text{ xor } X_5$$
$$C_4^{|}(\rho,\theta) = C_5^{|}(\rho,\theta) \text{ xor } X_4$$
$$C_3^{|}(\rho,\theta) = C_4^{|}(\rho,\theta) \text{ xor } X_3$$
$$C_2^{|}(\rho,\theta) = C_3^{|}(\rho,\theta) \text{ xor } X_2$$

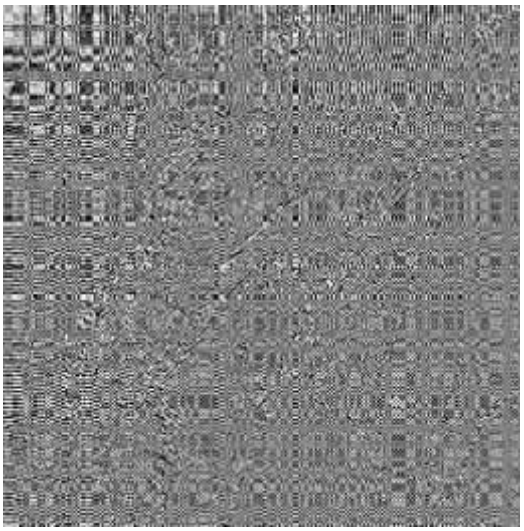

Fig. 2. 256x256 gray scale image of lena.

$$C_1^{|}(\rho,\theta) = C_2^{|}(\rho,\theta) \text{ xor } X_1$$
$$C_0^{|}(\rho,\theta) = C_1^{|}(\rho,\theta) \text{ xor } X_0$$

$$N(x,y) = IDRT(C_0^{|}(\rho,\theta))$$

Output: Decrypted image N which is same as M.

IV. EXPERIMENTAL RESULTS

The proposed algorithm is implemented in Matlab R2013a platform. Using this algorithm five 16 bit gray scale images of size 256 x 256 are subjected for encryption and the analysis is made on the 16 bit gray scale image of lena which is shown in the Fig. 2.

Fig. 3. Encrypted image after Radon Transformation and XOR operation

The radon transformed image with eight 8 bit secrete key X_0 to X_7 is shown in the Fig. 3. The final encrypted image using non chaotic substitution with P_0 to P_7 is shown in the Fig. 4.

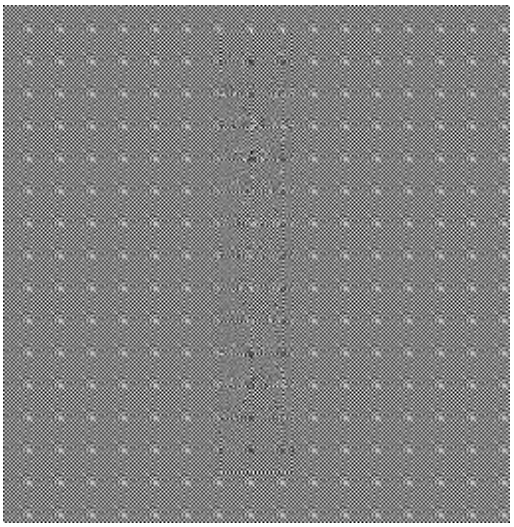

Fig. 4. Cipher image of lena.

The histograms of original image, radon transformed image and non chaotic substituted image are shown in the Fig.5, 6 and Fig. 7 respectively. Comparison between different encryption algorithms based on entropy is given in Table I. Average correlation between pixels values after transformation is given in Table II.

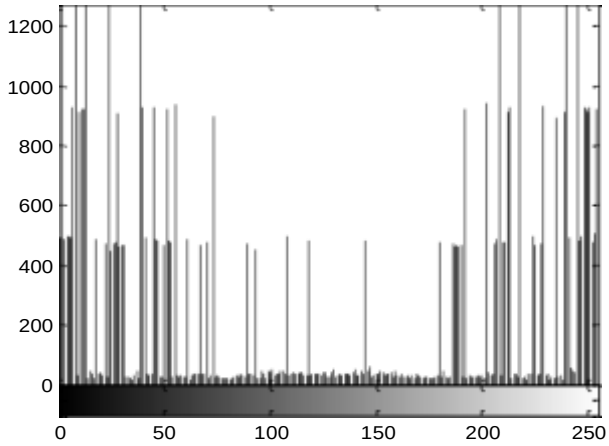

Fig. 5. Histogram of 256x256 original image of lena. .

Fig. 6.

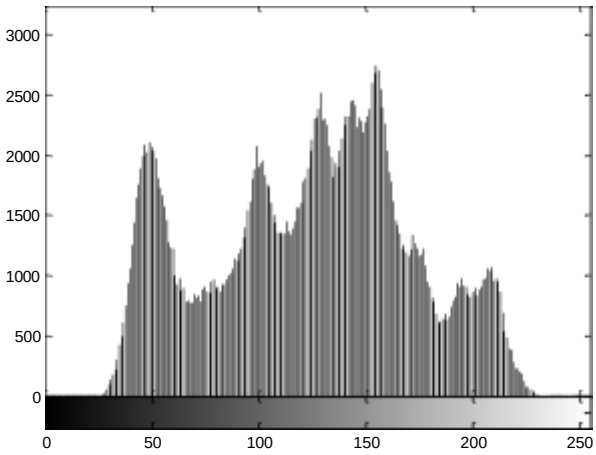

Fig. 7. Histogram of radon transformed image of Lena with X_0 to X_7 .

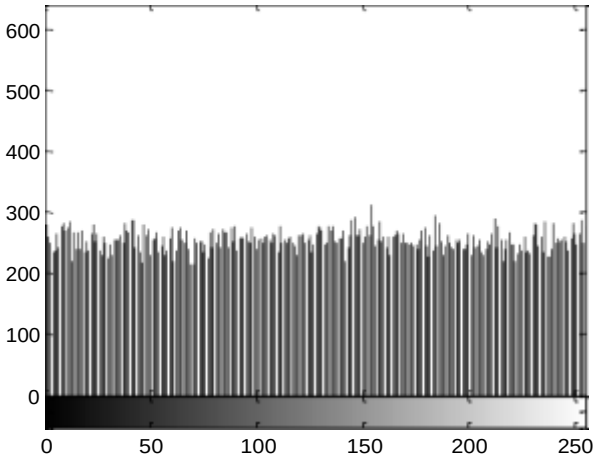

Fig. 8. Histogram of non chaotic substituted (cipher) image of Lena .

TABLE. I The comparision between standard algorithms and proposed algorithm based on entropy

Schemes	Entropy
Kamlesh Gupta[3]	5.5437
Blowfish[3]	5.5438
Twofish[3]	5.5438
Encryption using Radon transformation and chaotic substitution (proposed scheme)	7.9970

TABLE. II Average correlation between pixels values after encryption

Schemes	Correlation after transformation	Final Correlation coefficient
Image Encryption Using Affine Transform and XOR Operation [1]	0.9468	0.5088
Encryption using Radon transformation and chaotic substitution (proposed scheme)	0.0095	0.0021

V. CONCLUSION

In the proposed algorithm, transformation and substitution techniques have been adopted. The strong correlation between the neighboring pixels has been broken using discrete radon transformation and non chaotic substitution and permutation. The key length used is less compared to other encryption techniques and due to this, the algorithm requires less computation time. The key is subjected for eight set of initial permutations which makes the algorithm more effective against brute force attacks. The proposed algorithm is subjected to various analytical and differential analysis. It is observed that, very high level of information entropy and very minimum correlation between pixel values can be achieved in comparison with the existing algorithms. The security level can be further enhanced using non chaotic generators in the last stage of the algorithm.

REFERENCES

[1]. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar "Image Encryption Using Affine Transform and XOR Operation," Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), April 2011.

[2]. Salwa K. Abd-El-Hafiz, Sherif H. AbdElHaleem and Ahmed G. Radwan “Permutation Techniques Based on Discrete Chaos and their Utilization in Image Encryption,” 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), June 2016.

[3]. Delong Cui, Lei Shu, Yuanfang Chen and Xiaoling Wu, “Image Encryption Using Block Based Transformation With Fractional Fourier Transform,” 8th International Conference on Communications and Networking in China (CHINACOM), Aug 2013

[4]. Ahmed G. Radwan, Sherif H. AbdElHaleem and and Salwa K. Abd-El-Hafiz “ Image Encryption Algorithms Using Non-Chaotic Substitutions and Permutations, ” 13th International Conference On Electrical Engineering/Electronics, Computer, Telecommunications And Information Technology (Ecti-Con), June 2016

[5]. Seddik Hassene and Maalaoui Najm Eddine “A new hybrid encryption technique permuting text and image based on hyperchaotic system, ” 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP) in Tunisia, March 2016

[6]. Adrian-Viorel Diaconu, Valeriu Ionescu, Gabriel Iana and Jose Manuel Lopez-Guede. “A New Bit-Level Permutation” . International Conference on Communications (COMM), June 2016.

[7]. Vladimír Hajduk, Martin Broda, Ondrej Kováþ and Dušan Levický. “Image steganography with using QR code and cryptography,” 26th Conference Radioelektronika, April 2016.

[8]. Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda. “Image Encryption by Novel Cryptosystem Using Matrix Transformation,” First International Conference on Emerging Trends in Engineering and Technology, July 2008.

[9]. Ramtin Mojtahedi Saffari and Sattar Mirzakuchaki “A Novel Image Encryption Algorithm Based on Discrete Wavelet Transform Using Two dimensional Logistic Map ,” 24th Iranian Conference on Electrical Engineering (ICEE), May 2016.

[10]. Min Lin, Fei Long and Lu Guo “Grayscale image encryption based on Latin square and Cellular Neural Network ,” 28th Chinese Control and Decision Conference (CCDC), May 2016.

[11]. A. Zhang and N. Zhou, "Color image encryption algorithm combining compressive sensing with Arnold transform," Journal of Computers, vol. 8, pp. 2857-2863, 2013.

[12]. Z Li andX. Liu, "The image encryption algorithm based on the novel diffusion transformation," International Conference on Computer, Mechatronics , Control and Electronic Engineering (CMCE), pp. 345- 348, 2010.

[13]. N.K. Pareek, V. Patidar, and K.K. Sud, "Substitution-diffusion based image cipher," International Journal of Network Security & Its Applications (IJNSA), vol. 3, pp. 149-160, 2011.

[14]. S.H. AbdElHaleem, A.G. Radwan and S.K. Abd-El-Hafiz, "Design of pseudo random keystream generator using fractals," The IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 877-880, 2013.