Chapter 64
A Symmetric Key-Based Image Encryption Scheme

Jaydeb Bahumik and Supriyo De

Abstract In this information age, secure transmission and storage of digital image are an important requirement. Due to its better performance, symmetric key algorithms are popularly employed to provide confidentiality of digital information. In this paper, a new symmetric key-based image encryption technique has been introduced. In proposed scheme, firstly, a plain image is divided into blocks of 16 pixels and then each block is permutated by an invertible linear transformation. After that, permutated image pixel values are XOR-ed with expanded key bytes. The scheme is implemented and analyzed against statistical analysis and cryptanalysis. It is shown that proposed scheme is secure and easy for implementation.

Keywords Image security · Symmetric key · Linear transformation · Cipher image · Histogram · Correlation · Entropy · Differential attack

Introduction

Cryptography is a tool to transform readable information into a meaningless one. It plays a vital role when the secure information is transmitted through a non-secure channel. This scenario makes it more complex and significant for digital image. Encryption plays an important role which makes the image meaningless to the attacker. Although there exists several well-established encryption [1, 2] techniques such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RSA, and Advanced Encryption Standard (AES) but with respect to robustness and complexity, they are not suitable for image encryption.

J. Bahumik (✉)
Department of ECE, Haldia Institute of Technology, Haldia, WB, India
e-mail: I.bahumik.jaydeb@gmail.com

S. De
Department of ECE, Saroj Mohan Institute of Technology, Guptipara, WB, India
e-mail: II.supriyo.tech@gmail.com

J. K. Mandal et al. (eds.), *Proceedings of the International Conference on Computing and Communication Systems*, Lecture Notes in Networks and Systems 24, https://doi.org/10.1007/978-981-10-6890-4_64

In last few years, researchers developed several image encryption schemes. But till date, it is becoming a challenge to develop an efficient image encryption scheme due to large size, redundancy, and strong correlation between pixel values of plain image. In [3], skew tent chaotic map and permutation–diffusion architecture have been proposed. But with respect to differential cryptanalysis, it does not provide satisfactory result in round one and the paper concluded that more than two times iteration of the algorithm can resist the differential attack. Bhowmik et al. [4] developed their work with the help of genetic algorithm (GA). Here, GA has been applied to generate encryption key with the combination of well known Blowfish encryption technique. Using GA, a new approach of image encryption has been developed in [5]. Beside GA-based scheme, several researchers focused their work on AES and modified AES for image encryption [6, 7]. In [8, 9], image encryption schemes based on AES in Electronic Code Book (ECB) mode have been presented. In these schemes, two different linear operations are performed before applying AES. Most of the existing image encryption schemes either do not satisfy all cryptographic parameters or they are costly for implementation in real-time application.

In this paper, a new image encryption scheme has been introduced. The scheme consists of three parts: image permutation, key expansion, and the final one is key XOR-ing with the permutated image. The correlation between adjacent pixels of cipher image significantly reduced by the proposed scheme, and it is observed that linear transformation with optimum number of iterations makes the algorithm lighter and faster.

The rest of the paper is organized as follows. In section "Proposed Scheme," proposed image encryption scheme is described. Section "Experimental Results" elaborately represents the experimental outcomes. In section "Security Analysis," security analysis of the proposed scheme is discussed and finally conclusions are drawn in section "Conclusion."

Proposed Scheme

The said scheme consists of three functional blocks: linear transformation for plain image, key expansion, and the last one is encryption by XOR operation with expanded key and outcome of the permutation block. The details of the each block are explained below.

Linear Transformation for Plain Image (LT_PI)

LT_PI is a linear transformation, and it is a 128×128 binary matrix. The matrix is a tri-diagonal matrix where upper and lower diagonal elements are all ones and main diagonal elements are as follows:
01001000100010000010111110111101011001110000001110011110010111 10

01011110010110001100000011100110101111011111010000010001000100010
In *LT_PI*, at a time, 16 bytes data are XOR-ed with 16 bytes output of *LT_PI*. Then, XOR-ed output is passed through the linear transformation.

Key Expansion

In key expansion algorithm, cipher key is expanded to produce key of size equal to image size. Key is expanded by employing linear transformation for key and nonlinear mixing function *Nmix*.

Linear Transformation for key (*LT_Key*) It takes 16 bytes input (initially 16 bytes cipher key) and produces a 16 bytes output by employing the matrix T_{key} shown in Eq. 64.1(a) and the 16 bytes previously permutated output. T matrix (Eq. 64.1(b)) is a (8×8) binary non-singular matrix and $T^L = I$, where I is a (8×8) identity matrix and $L = 255$. T matrix is as follows:

$$T_{key} = \begin{pmatrix} T^1 & T^2 & T^3 & .... & T^{15} & T^{16} \\ T^2 & T^4 & T^6 & & T^{30} & T^{32} \\ T^3 & T^6 & T^9 & & T^{45} & T^{48} \\ ... & & & & & \\ ... & & & & & \\ T^{15} & T^{30} & T^{45} & & T^{225} & T^{240} \\ T^{16} & T^{32} & T^{48} & & T^{240} & T^1 \end{pmatrix} ..(a) \; and \; T = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} ..(b) \quad (64.1)$$

The characteristic polynomial associated with T matrix is $(T + I.x)$, and it is also a primitive polynomial of degree 8. Input 128-bits cipher key is first passed through *LT_Key*. Then, output of *LT_Key* is mixed with input of *LT_Key* using *Nmix* function. For even/odd key generation, *Nmix* is operated from left to right/right to left, respectively. After 16th iteration, 16th 128-bits key is loaded as an input of *LT_Key* and it repeats until it expands the key size at par with size of plain image. Process has been presented in Fig. 64.1.

Nmix, the nonlinear key mixing function [10], is applied here for the key expansion from the permuted keys. Two different directions of operation of *Nmix* in key expansion algorithm are considered here to produce odd and even 128-bit keys. For an odd set of 128 bits output (obtained from *LT_Key*), the *Nmix* operation is done from the right to left (LSB to MSB). On the other hand, in an even set of key generation, the *Nmix* operation is done from the left to right (MSB to LSB) direction. The detailed equations for right to left *Nmix* operation are expressed in Eqs. 64.2 and 64.3. Similarly, left to right operation is performed starting from MSB.

$$y_i = x_i \oplus k_i \oplus c_{i-1} \quad (64.2)$$

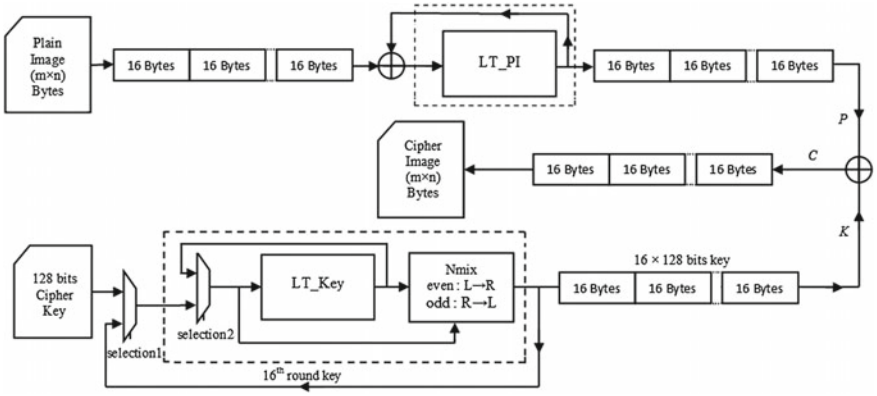

Fig. 64.1 Block diagram of proposed image encryption scheme

$$c_i = \oplus_{j=0}^{i} x_j k_j \oplus x_{i-1} x_i \oplus k_{i-1} k_i \tag{64.3}$$

where *X, K*, and *Y* are n-bit variables, c_i is the carry term propagating from the *i*th bit position to $(i + 1)$th bit position; $0 \leq i \leq n - 1$ and $0 \leq j \leq n - 1$.

Encryption

Image encryption part is done by bitwise XOR operation of permutated image with expanded keys. Here, the cipher image is obtained from the XOR operation between expanded keys(K) and permuted image(P).

$$C = P \oplus K \tag{64.4}$$

where P: permuted image, K: expanded key, C: cipher image

Decryption

Image decryption is done using following steps.
Step 1: Expand cipher key
Step 2: XOR between cipher image and expanded key
Step 3: Reverse image permutation

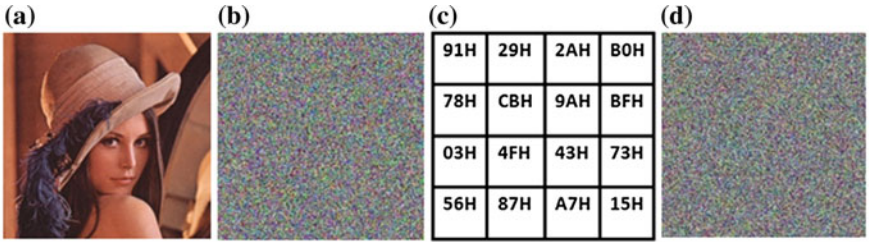

Fig. 64.2 **a** Lena image; **b** Permuted Lena; **c** 128 bits key; **d** Expanded key(256×256)

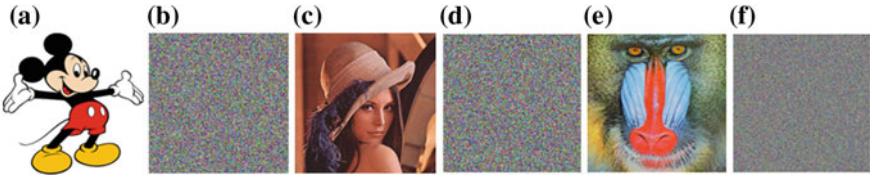

Fig. 64.3 **a** Micky image; **b** Encrypted Micky; **c** Lena image; **d** Encrypted Lena; **e** Baboon image; **f** Encrypted Baboon

Experimental Results

Proposed scheme is tested by using several plain images. The plain image "Lena" and result of the permutation block are shown in Figs. 64.2(a) and 64.2(b), respectively. On the other hand, initial 128 bits key and expanded keys for encryption are shown in Figs. 64.2(c) and 64.2(d), respectively. Figure 64.3 represents the plain images and corresponding cipher images obtained by applying the proposed scheme.

Security Analysis

In the following section, security analysis of proposed scheme is discussed.

Key Space Analysis

Key space indicates the all possible set of keys which can be used for encryption. Security level is proportional to the key space size. In proposed scheme, key length is 128 bits, i.e., the key space size is 2^{128}. As the key space size is larger than 2^{104} [11, 12], it can be stated that the proposed scheme can prevent the brute force attack.

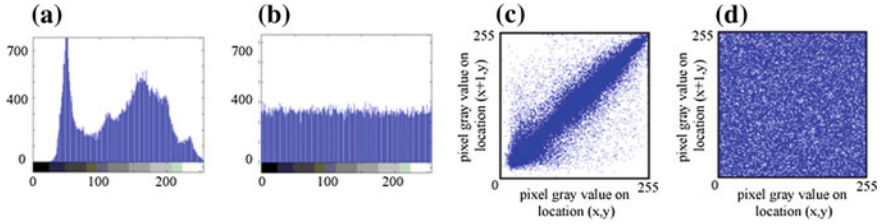

Fig. 64.4 **a** Histogram of Lena; **b** Histogram of encrypted Lena; **c** Correlations of two horizontally adjacent pixels of Lena; **d** Correlations of two horizontally adjacent pixels of encrypted Lena

Statistical Analysis

Statistical analysis is absolutely necessary to verify the encryption scheme. Robustness of the algorithm and the random distribution of the cipher images can be categorized by this analysis.

Histogram Analysis An image histogram illustrates how the pixel values are distributed throughout the image. The uniform distribution of histogram indicates to have equal probability of all color intensity level which is highly required for the cipher images. Plot of histograms for "Lena" image and corresponding cipher image are shown in Figs. 64.4(a) and 64.4(b), respectively. Here, the histogram analysis is justifying the proposed scheme.

Correlation Analysis Correlation analysis is used to find out the relation between two adjacent pixels of an image in all possible direction. High correlation is an intrinsic nature of general digital image. On the other hand, for an encryption scheme, it is the primary target to break the correlation between two adjacent pixels of the image. Correlation analysis has been done for plain image and cipher image produced by proposed scheme. The equation to compute correlation may be found in [3]. Comparison of correlation with other existing methods of image encryption schemes are provided in Table 64.1. Figure 64.4c, d shows the correlation of two horizontally adjacent pixels of "Lena" image and corresponding cipher image, respectively.

Entropy Analysis

Entropy is a mathematical tool which is basically used for checking the uncertainty of a signal or sequence. For an image encryption scheme having maximum values of entropy implies that it is more significant encryption. The column 5 of the Table 64.2 represents the entropy value of cipher images obtained by employing proposed scheme which is nearly closed to ideal 8-bits random sequences. Table 64.2 shows that the proposed scheme is competent enough with other existing image encryption schemes.

Table 64.1 Correlation coefficient of two adjacent pixels in the plain image and the cipher images

Image	Direction	Plain image	Cipher image [3]	Cipher image [7]	Cipher image-proposed
Micky	Horizontal	0.9350	–	−0.0112	−0.0024
	Diagonal	0.8891	–	0.0009	−0.0019
	Vertical	0.9244	–	−0.0813	0.0012
Lena	Horizontal	0.9327	−0.0008	–	0.0031
	Diagonal	0.9288	−0.0001	–	−0.0049
	Vertical	0.9468	0.0037	–	−0.0019
Baboon	Horizontal	0.9210	–	–	−0.0025
	Diagonal	0.8287	–	–	0.0033
	Vertical	0.8550	–	–	−0.0018

Table 64.2 Entropy value for the cipher images

Image	Cipher image [3]	Cipher image [7]	Cipher image [8]	Cipher image-proposed
Micky	–	7.9992	7.9973	7.9971
Lena	7.9974	–	–	7.9972
Baboon	7.9993	–	–	7.9993

Table 64.3 NPCR and UACI of cipher images with respect to key sensitivity

Image	NPCR		UACI	
	Reference [3]	Proposed	Reference [3]	Proposed
Micky	–	99.6332	–	33.5005
Lena	–	99.6332	–	33.5629
Baboon	99.6052	99.6187	33.4132	33.4645

Sensitivity Analysis

Block cipher-based cryptosystem can be analyzed by sensitivity analysis. It is a technique to check how the encryption scheme reacts with respect to one-bit change of key and/or plaintext. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) [13, 14] are measured for this analysis. Mathematical expressions to compute NPCR and UACI may be found in [14].

Key Sensitivity In this test, one-bit difference between two 128 bits keys is employed for encrypting a plain image and then from the two different cipher images, NPCR and UACI values are computed and comparative study is shown in Table 64.3.

Plaintext Sensitivity The sensitivity is measured by finding out the NPCR and UACI from two cipher images(using same key) obtaining from two plain images with one-bit difference. The Table 64.4 shows the result of this study.

Table 64.4 NPCR and UACI of cipher images with respect to plaintext sensitivity

Image	NPCR				UACI			
	Reference [3] 1st round	Reference [3] 2nd round	Reference [7]	Proposed	Reference [3] 1st round	Reference [3] 2nd round	Reference [7]	Proposed
Micky	–	–	99.58	97.5631	–	–	29.63	32.6957
Lena	37.6389	99.6063	–	97.7071	12.7034	33.4758	–	32.8327
Baboon	84.1255	99.6048	–	98.7178	28.1799	33.4554	–	33.1385

From Table 64.3, it is observed that NPCR and UACI values with respect to key sensitivity are better compared to existing scheme. On the other hand, in Table 64.4 the NPCR values with respect to plaintext are slightly lesser than existing scheme in [3, 7], whereas in Table 64.4, UACI values of proposed scheme is better than existing scheme in [3, 7].

Conclusion

In this paper, a new image encryption scheme is introduced. The scheme consists of three functional blocks. In permutation step, the scheme generates same size of image from plain images using *LT_PI*. Next step, the key expansion module expands the key with same size of plain image using *LT_Key* and *Nmix* function. Third block performs XOR-ing of permutated image with the expanded same size key. The experimental results show that the scheme is able to break the correlation and provides the random outcome as a cipher image. Proposed scheme is able to prevent the brute force attack, statistical attack as well as differential attack.

References

1. Stallings, W.: Cryptography and Network Security: Principles and Practice. Prentice-Hall, Upper Saddle River, NJ. (1999)
2. Daemen, J., Rijmen, V.: The Design of Rijndael- AES, The Advanced Encryption Standard. Springer-Verlag. (2002)
3. Zhang, G., Liu, Q.: A Novel Image Encryption Method Based on Total Shuffling scheme. Journal of Optics Communications, Elsevier, vol. 284, Issue 12, 2775–2780 (2011)
4. Bhowmik, S., Acharyya, S.: Image Cryptography: The Genetic Algorithm Approach. IEEE International Conference on Computer Science and Automation Engineering, vol. 2, 223–227 (2011)
5. Kumar, J., Nirmala, S.: Encryption of Images Based on Genetic Algorithm A New Approach. Advances in Computer Science, Engineering & Applications, vol. 167 of the series Advances in Intelligent Systems and Computing, 783–791 (2012)
6. Huang, C. W., Tu, Y. H., Yeh, H. C., Liu, S. H., Chang, C. J.: Image observation on the modified ECB operations in Advanced Encryption Standard. Proc. of Int. Conf. on Information Society (i-Society), London, 264–269 (2011)
7. Shtewi, A. A., Hasan, B. E. M., Hegazy, A. E. F. A.: An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. International Journal of Computer Science and Network Security, vol. 10, 226–232 (2010)
8. De, S., Bhaumik, J.: TBLT-AES: A Robust Image Encryption Scheme. Journal of Discrete Mathematical Sciences & Cryptography, (Taylor & Francis, Co-published with TARU Publications) vol. 17, no. 3, 273–288 (2014)
9. De, S., Bhaumik, J.: An AES-based Robust Image Encryption Scheme. Int. Journal of Computer Applications, vol. 109, no. 12, 29–34 (2015)
10. Bhaumik, J., Chowdhury, D. R.: Nmix: An Ideal Candidate for Key Mixing. Proc. of Int. Conf. on Security and Cryptography (Secrypt), Milan, Italy, 285–288 (2009)
11. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. Journal of Bifurcation and Chaos, vol. 16, no. 8, 2129–2151 (2006)

12. Stinson, D.: Cryptography: Theory and Practice. Second ed. CRC/C&H
13. Wu, Y., Noonan, J. P., Agaian, S.: NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 31–38 (2011)
14. El-Wahed, M. A., Mesbah, S.,Shoukry, A.: Efficiency and Security of Some Image Encryption Algorithms. Proc. of the World Congress on Engineering, vol. 1. (1982)