Encryption Speed Improvement on "An Improvement over An Image Encryption Method Based on Total Shuffling"

Yong Zhang
School of Software and Communication Engineering
Jiangxi University of Finance and Economics
Nanchang, P. R. China
E-mail: zhangyong@jxufe.edu.cn

***Abstract*—Encryption security and encryption speed are two important aspects of image encryption algorithm. Recently, Zhang et al. proposed a plaintext related image encryption method based on chaos and permutation-diffusion architecture [G. Zhang, Q. Liu, Opt. Commun. 284 (2011) 2775-2780]. In the same year Wang et al. pointed out that Zhang's scheme cannot resist chosen plaintext attacks [X. Wang, G. He, Opt. Commun. 284 (2011) 5804-5807]. Most recently, Eslami et al suggested an improvement over Zhang's method with slower encryption speed [Z. Eslami, A. Bakhshandeh, Opt. Commun. 286 (2013) 51-55]. This paper presented another improvement over Eslami's scheme using a lookup table to enhance the speed of encryption algorithm without loss of security, which makes it more feasible in practical communication.**

Keywords-image encryption; encryption speed; cryptosystem; chaotic system

I. INTRODUCTION

Some of the inherent characteristics of the chaotic system, for example, the initial value sensitivity, parameter sensitivity and long-term evolution unpredictability, are corresponding to those of image encryption system, for example, plaintext sensitivity, key sensitivity, and noise-like cipher-text. In addition, chaotic system can be obtained by the deterministic equations and can generate pseudo-random numbers with excellent features. Therefore, chaotic system is widely employed in image encryption researches [1-6].

Recently, Zhang et al. proposed an image encryption method based on total shuffling scheme [7]. 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, 8]. However, the first secret code in [7] is not safe enough to resist the chosen plaintext attack, which is pointed out and crypt analyzed in [9].

In 2013, Eslami et al. suggested an improved algorithm [10] over these shortcomings described in [9]. 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 [7] higher security against the chosen plaintext attacks with slower encryption speed as a trade off. In this paper, we proposed a lookup table based encryption improvement on the schemes proposed in [7, 10] to improve the encryption speed. The latter chapters are arranged as follows: The algorithms of Zhang et al.'s and Eslami et al.'s are briefly introduced in Section 2. Section 3 describes our proposed improvement based on the lookup table. Section 4 shows some representative simulation results of our method. Section 5 tabulates the encryption speed of our method and those of [7, 10]. The comparative performance analyses of our method and [7, 10] are made in Section 6 to demonstrate the feasibility of our proposed. Section 7 concludes the paper.

II. ENCRYPTION ALGORITHM PROPOSED IN [7,10]

A. Original Encrption Algorithm [7]

The skew tent map is used in [7] and formulated as (1).

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

Assume the plain image is of 8-bit grayscale and of size $M\times N$, which is denoted by $\mathbf{P}=\{p_0, p_1, \ldots, p_{MN-1}\}$ using from top to bottom and then from left to right scanning method. The encryption scheme in [7] consists of two procedures, i.e. permutation and diffusion. The pixel permutation procedure is shown as follows:

Step 1. Iterate (1) to obtain a pseudo random sequence of size $M\times N$, denoted by $\mathbf{X}=\{x_0, x_1, \ldots, x_{MN-1}\}$(excluding the transient states of the first L iterations).

Step 2. Sort X in ascending order to get $\mathbf{Y}=\{y_0, y_1, \ldots y_{MN-1}\}$.

Step 3. According to the relationship of **X** and **Y**, a scrambling vector $\mathbf{T} = \{t_0, t_1, \ldots, t_{MN-1}\}$ is obtained such that $y_i = x_{t_i}$, $i = 0, 1, \ldots, MN-1$.

Step 4. Permute the plain image **P** with **T** to get $\mathbf{P}' = \{p'_0, p'_1, \cdots, p'_{MN-1}\}$ such that $p'_i = p_{t_i}$, $i = 0, 1, \ldots, MN-1$.

Then the diffusion procedure is as follows:

Step 1. Let $i = 0$.

Step 2. Get an 8-bit pseudo random integer d_i from the current state value x, i.e. d_i=mod(floor($x\times 2^{48}$), 256).

Step 3. Calculate the current pixel value c_i of cipher image according to the current pixel value p'_i and the previous pixel value p'_{i-1} of the plain image as well as d_i, i.e. $c_i = p'_i \oplus \mathrm{mod}(p'_{i-1} + d_i, 256)$, where $\oplus$ means bitwise XOR operator.

Step 4. Calculate k using c_i, i.e. $k = 1 + \mathrm{mod}(c_i, 2)$. Then continue to iterate (1) for k times to obtain a new state value x.

Step 5. Let $i = i + 1$, and return to Step 2 until i reaches MN.

B. *Some Improvements in [10]*

The improvements in [10] over [7] are in Steps 3-4 of the diffusion procedure. In Step 3, use the formula $c_i = p'_i \oplus \mathrm{mod}(c_{i-1} + d_i, 256)$ instead. In Step 4, use the formula $k = 1 + \mathrm{mod}(c_i, 4)$ instead, which means the average iteration times are 2.5.

III. Proposed Improvement Algorithm

From the Step 4 of the diffusion procedure in [7], it can be seen that the average iteration times (k) are 1.5, while the average iteration times (k) reach up to 2.5 in the improvement in [10]. The more the average number of iterations, the better the randomness of security stream code, but the slower the encryption speed.

The scrambling algorithm is employed in both [7] and [10], which simply changed the location of each pixel without changing the value of each pixel. The actual security of scrambling is under suspicion [11], and furthermore, the workload of sort operation is huge when the plain image is of large size, which must be done in the preprocessing. Therefore, the scrambling process is omitted in our scheme.

Based on [10], our proposed method has the following improvements:

1) The scrambling process is omitted. We add one process of iterating (1) to get a lookup table of size 256, denoted by LT: $\{e_0, e_1, \ldots, e_{255}\}$.

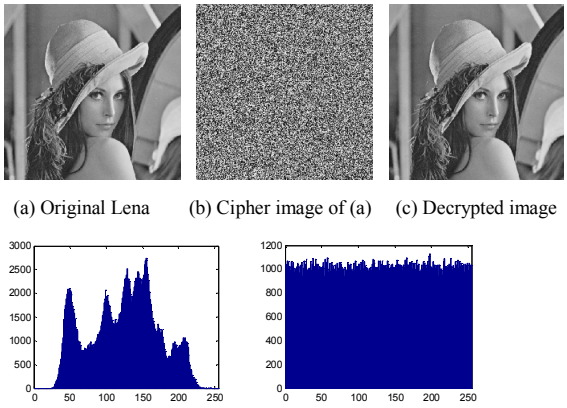
2) In the Step 3 of diffusion procedure, we use $c_i = \mathrm{mod}(p_i + c_{i-1} + d_i, 256)$ instead of $c_i = p'_i \oplus \mathrm{mod}(c_{i-1} + d_i, 256)$, i.e. XOR operator is changed to "addition and modulo". The reason is that the high significant bits (e.g. the 7th and 6th bits) of one pixel value in the 8-bit grayscale image contain the great visual image information. When using XOR operator, the 7th and 6th bits are changed with the probability of only 75%, and the 7th bit is changed in probability of only 50%. However, while using "addition and modulo" operator, the 7th and 6th bits' change rate is higher than that of XOR, up to 2023/2056≈98.3949%, and the 7th bit's change rate is up to 963/1028≈93.6770%.

3) The Step 4 of diffusion in [10] is modified totally as follows: Let $k = \mathrm{mod}(c_i + d_i, 256)$. Then employ the entry e_k of LT to do the operation of $x' = \mathrm{mod}(e_k + \text{original state } x, 1)$. Use the x' as initial value of (1) to iterate once to get a new state value x.

4) The decryption process is the inverse of the encryption process, e.g. in Step 3 of the diffusion, $p_i = \mathrm{mod}(c_i + 256 - c_{i-1} - d_i, 256)$.

IV. Simulation Results

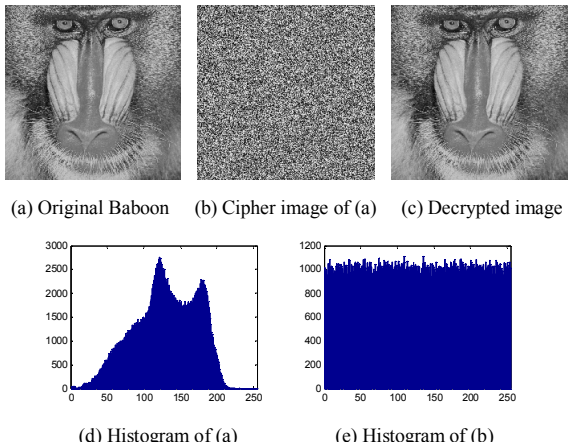
Take the plain images "Lena" and "Baboon" as examples by means of our proposed method for encryption and decryption with the secret key $\{x_0$=0.123456789, p=0.234$\}$. The results obtained are illustrated in Figs. 1-2, which show that the noise-like cipher images have flat histograms without any visual information, and the decrypted images are identical to the plain images.



(a) Original Lena (b) Cipher image of (a) (c) Decrypted image

(d) Histogram of (a) (e) Histogram of (b)

Figure 1. Plain image Lena and its cipher image.



(a) Original Baboon (b) Cipher image of (a) (c) Decrypted image

(d) Histogram of (a) (e) Histogram of (b)

Figure 2. Plain image Baboon and its cipher image.

V. ENCRYPTION SPEED COMPARISON

Encryption/Decryption speed is tested with the same computer of Intel Core i5 460M and 2GB memory under the MATLAB 7. Lena/Baboon (of size 512×512) is employed to do 1000 times experiments of encryption and decryption using random secret keys each time. The mean comparative results of encrypting one cycle and two cycles are tabulated in Table 1.

From Table 1 it can be seen that Eslami et al.'s method is slower than that of Zhang et al, and our improvement is about 8 times faster than their methods. The reason is that in Step 4 of diffusion Zhang et al.'s method needs 1.5 times of average iterations, and Eslami et al.'s method needs 2.5 times of average iterations, whereas our improvement only needs one time of iteration.

VI. SECURITY ANALYSIS

A. Key Space

The key space size of our method is identical to the size of Zhang et al.'s and Eslami et al.'s, i.e. $2^{52}\times2^{52}=2^{104}$. If p'_{-1} is considered as part of the key, the binary length of key is 112. If x_0, p and p'_{-1} for the second encryption cycle are also regarded as part of the key, the total binary key length is 224 bits, which is large enough to resist the brute-force attacks.

B. Key Sensitivity

Take the plain image Lena as an example. Firstly, do 1000 times of experiments, in each experiment randomly generate the secret key, and then make x_0 change 2^{-52} to calculate the NPCR and UACI [5, 12] of two produced cipher images. The average value of NPCR and UACI are tabulated in Table 2. Secondly, be similar to the first situation except that in each experiment the p is changed 2^{-52} instead of x_0. The results are listed in Table 3. Thirdly, also be similar to the first situation except that in each experiment the p'_{-1} is changed the least significant bit instead of x_0. The results are tabulated in Table 4. Note that the values in the parentheses in the Tables 2-4 are the theoretical values of NPCR and UACI.

From Tables 2-4 we can see that all the methods have the strong sensitivity to the x_0 and p regardless of the encryption cycles, but only our method and Eslami et al.'s have strong sensitivity to the p'_{-1}. That means the p'_{-1} cannot be regarded as part of key in [7].

TABLE I. COMPARATIVE ANALYSIS OF ENCRYPTION AND DECRYPTION TIME

Cycle Times	One Cycle (s)		Two Cycles (s)	
	Encryption	*Decryption*	*Encryption*	*Decryption*
Zhang et al [7]	0.419285	0.413744	0.840932	0.829475
Eslami et al [10]	0.483756	0.478631	0.841317	0.851974
Our proposed	0.051520	0.050980	0.102913	0.102569

TABLE II. KEY SENSITIVITY ANALYSIS OF x_0

Cycle Times	One Cycle (%)		Two Cycles (%)	
	NPCR (99.6094)	*UACI (33.4635)*	*NPCR (99.6094)*	*UACI (33.4635)*
Zhang et al [7]	99.6100	33.4613	99.6107	33.4628
Eslami et al [10]	99.6115	33.4622	99.6113	33.4656
Our proposed	99.6090	33.4614	99.6107	33.4688

TABLE III. KEY SENSITIVITY ANALYSIS OF p

Cycle Times	One Cycle (%)		Two Cycles (%)	
	NPCR (99.6094)	*UACI (33.4635)*	*NPCR (99.6094)*	*UACI (33.4635)*
Zhang et al [7]	99.6100	33.4657	99.6100	33.4704
Eslami et al [10]	99.6089	33.4620	99.6103	33.4628
Our proposed	99.6108	33.4687	99.6104	33.4619

TABLE IV. KEY SENSITIVITY ANALYSIS OF p'_{-1}

Cycle Times	One Cycle (%)		Two Cycles (%)	
	NPCR (99.6094)	*UACI (33.4635)*	*NPCR (99.6094)*	*UACI (33.4635)*
Zhang et al [7]	0.1181	0.0400	3.0127	1.0116
Eslami et al [10]	99.6083	33.4621	99.6084	33.4610
Our proposed	99.6088	33.4692	99.6072	33.4599

C. Information Entropy

Information entropy reflects the similarity degree of the visual image and the noise image. For the 8-bit grayscale noise image, the information entropy value is 8.

Take Lena and Baboon as examples, whose information entropies are 7.4451 and 7.3583, respectively. Do 100 times of experiments for each method of Zhang et al., Eslami et al. and our proposed with randomly selected secret keys to get 600 cipher images of Lena and Baboon. Then calculate the average information entropies of the cipher images of Lena and Baboon for each method, whose values are all 7.9993. That means the information leakage is negligible for all the methods.

D. Statistical Properties of Cihper Image

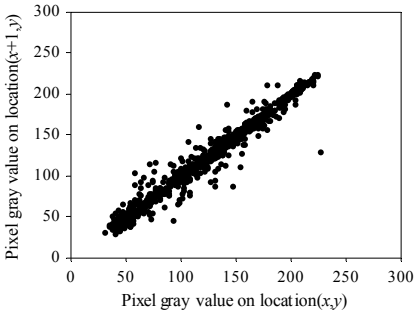
Take Lena as an example. We randomly selected 1000 pairs of two adjacent pixels in horizontal, vertical and diagonal directions from Lena and its cipher images produced by Zhang et al.'s, Eslami et al.'s and our proposed with the same key $\{x_0=0.123456789,\ p=0.234\}$, and calculated their correlation coefficients [13] which are tabulated in Table 5-6. The representative correlations of horizontal direction are illustrated in Fig. 3.

TABLE V. CORRELATION COEFFICIENTS OF PLAIN IMAGE LENA

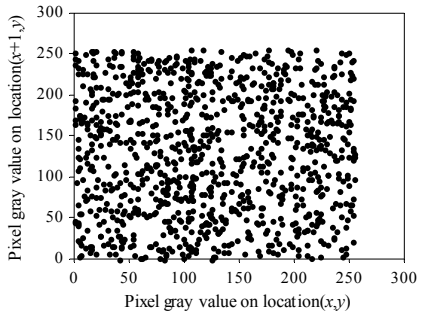
Direction	Horizontal	Vertical	Diagonal
Lena	0.9690	0.9853	0.9655

TABLE VI. COMPARATIVE ANALYSIS OF CORRELATION COEFFICIENTS

Cycle Times	One Cycle			Two Cycles		
	Hori.	*Vert.*	*Diag.*	*Hori.*	*Vert.*	*Diag.*
Zhang et al [7]	-0.0094	-0.0294	-0.0140	-0.0047	0.0189	0.0408
Eslami et al [10]	-0.0481	0.0043	-0.0042	0.0445	0.0283	0.0064
Our proposed	0.0172	0.0021	0.0316	0.0032	0.0437	0.0079



(a) Horizontal correlation of Lena



(b) Horizontal correlation of the cipher image

Figure 3. Horizontal Correlations of Lena and its cipher image produced by our proposed method with the key {0.123456789, 0.234}.

We can see from Tables 5-6 and Fig. 3 that the plain image is highly correlated in horizontal, vertical and diagonal directions, while the correlation coefficients of two adjacent pixels in horizontal, vertical and diagonal directions in all the methods are close to zero, which demonstrate the three methods can well resist the statistical attacks.

E. Plain Image Sensitivity

We do 100 times of experiments for each plain image of Lena and Baboon with the constant key {0.135792468, 0.864}.

TABLE VII. PLAIN IMAGE SENSITIVITY ANALYSIS OF LENA

Cycle Times	One Cycle (%)		Two Cycles (%)	
	NPCR (99.6094)	*UACI (33.4635)*	*NPCR (99.6094)*	*UACI (33.4635)*
Zhang et al [7]	0.6213	0.2085	3.1441	1.0570
Eslami et al [10]	44.1703	14.8344	99.6096	33.4615
Our proposed	54.2103	18.2095	99.6085	33.4602

TABLE VIII. PLAINTEXT SENSITIVITY ANALYSIS OF BABOON

Cycle Times	One Cycle (%)		Two Cycles (%)	
	NPCR (99.6094)	*UACI (33.4635)*	*NPCR (99.6094)*	*UACI (33.4635)*
Zhang et al [7]	0.0528	0.0176	3.4661	1.1628
Eslami et al [10]	50.9354	17.1109	99.6103	33.4645
Our proposed	53.1850	17.8625	99.6083	33.4623

In each of experiments, one pixel of the plain image is randomly selected and its value adds 1, and then the original plain image and the slightly changed plain image are encrypted to obtain two cipher images. Finally calculate the average values of NPCR and UACI, which are tabulated in Tables 7-8.

Tables 7-8 show that Zhang et al.'s method is not sensitive to plain image, which is weak against chosen plaintext attacks, demonstrated in [9]. Eslami et al.'s and our proposed with only one encryption cycle are not very sensitive to the plain image, but with two encryption cycles the NPCRs and UACIs of our proposed and Eslami et al.'s are perfectly close to the theoretical values of 99.6094% and 33.4635%, and furthermore the secret stream code is related with the plain image, which demonstrates that both our proposed and Eslami et al.'s methods can effectively resist the chosen plaintext attacks.

VII. CONCLUSION

In this paper, we proposed a lookup table based method to improve the encryption/decryption speed of the image encryption scheme presented in [7, 11], and employed "addition and modulo" operator instead of "XOR" in diffusion procedure. We compared our proposed and the methods in [7, 11] in the aspects of encryption/decryption speed, key space, key sensitivity, information entropy, cipher image statistical properties and plain image sensitivity analysis, and the results fully demonstrated that the speed of our proposed method is about 8 times faster than those of [7, 11] without loss of security. Therefore, the proposed method is more feasible in the practical communications.

ACKNOWLEDGMENT

This work was fully supported by the Natural Science Foundations of Jiangxi Province (Grant Nos. 20122BAB201036 and 20114BAB211011).

REFERENCES

[1] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," Cryptologia. vol. 13, pp. 29-42, 1989.

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurc. Chaos. vol. 8, pp. 1259-1284, 1998.

[3] S. Lian, J. Sun, Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," Chaos. Solitons. Fractals. vol. 26, pp. 117-129, 2005.

[4] K. Wong, B. S. H. Kwok, and W. S. Law, "A fast image encryption scheme based on chaotic standard map," Phys. Lett. A. vol. 372, pp. 2645-2652, 2008.

[5] G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos. Solitons. Fractals. vol. 21, pp. 749-761, 2004.

[6] A. A. Adb El-Latif, L. Li, T. Zhang, N. Wang, X. Song, and X. Niu, "Digital image encryption scheme based on multiple chaotic systems," Sensing. Imaging. An Int. J. vol. 13, pp. 67-88, 2012.

[7] G. Zhang, and Q. Liu, "A novel image encryption method based on total shuffling scheme," Opt. Commun. vol. 284, pp. 2775-2780, 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] 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.

[10] Z. Eslami, and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," Opt. Commun. vol. 286, pp. 51-55, 2013.

[11] S. Li, C. Li, G. Chen, N. Bourbakis, and K. Lo, "A general quantitative cryptanalysis of permutation only multimedia ciphers against plaintext attacks," Signal Proc. Image Commun. vol. 23, pp. 212-223, 2008.

[12] Y. Mao, G. Chen, S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," Int. J. Bifur. Chaos. vol. 14, pp. 3613-3624, 2004.

[13] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," Opt. Commun. vol. 283, pp. 3259-3266, 2010.