A Multiple Tent Maps Based Image Encryption Scheme with Plain-image Dependent Permutation and Diffusion

Ruisong YE[1,a], Yuting XI[1], Ming YE[1], Xiaoyun SHI[1], Wenhao YE[1]

[1]Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China

[a]rsye@stu.edu.cn

Keywords: Tent map; Permutation; Diffusion; Plain-image dependent; Image encryption

Abstract. A novel multiple tent maps based image encryption scheme with plain-image content dependent permutation-diffusion mechanism is proposed. The permutation is realized by swapping the gray values at different part of the considered image; it is performed with the help of pseudo-random sequence yielded by tent map, which is different from conventional permutation within the whole plain-image, and therefore improves the permutation efficiency. The diffusion is performed over the permuted image by bitxoring operations with pseudo-random gray value sequences generated by two other tent maps. The key streams for the two processes are both related to the image contents, and consequently the proposed image encryption scheme is strongly sensitive to cipher keys as well as plain-images. One round of permutation and one round of diffusion achieve perfect security effect. The security and performance of the proposed scheme have been analyzed thoroughly in details.

Introduction

Chaos-based image encryption schemes have been extensively investigated in the last decades since Fridrich firstly proposed the typical permutation-diffusion mechanism in 1998 [1]. It is well-known that chaotic dynamical systems possess some perfect features, such as high sensitivity to initial conditions and control parameters, ergodicity, pseudo-randomness etc. Furthermore, these good chaotic features are line with the fundamental requirements of cryptography like confusion and diffusion, and consequently chaotic systems provide potential candidates for constructing cryptosystems [2][3][4][5][6][7]. Unfortunately, Most of the existing chaos-based image encryption schemes with typical permutation-diffusion architecture have been proved to be weak resisting cryptanalysis due to one fatal drawback, that is, the key steams in both the permutation phase and the diffusion phase are all fixed for different plain-images. The two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value [8]. As a matter of fact, some image encryption algorithms with typical permutation-diffusion architecture have been attacked successfully by chosen-plaintext or known-plaintext attacks [9][10][11]. Therefore how to construct image encryption schemes resisting cryptanalysis attracts much attention recently, for example, see [12][13][14].

In this paper, we present a novel image encryption scheme with revised permutation-diffusion mechanism. The image encryption scheme proposed is plain-image content dependent, which can resist cryptanalysis efficiently. The permutation is performed between two separate parts of the plain-image by sorting-based permutation. Sorting-based permutation has been widely applied in the chaos-based image encryption schemes. The conventional sorting-based permutation is implemented within one whole image, while the permutation in this paper is realized between two separate parts of the plain-image. The pseudo-random sequence generated by the chaotic map is just $H \times W / 2$ at length as the plain-image is of width W and height H, while in conventional sorting-based permutation, the key stream needs $H \times W$ pseudo-random numbers. As a result, the proposed image encryption scheme can improve the encryption/decryption rate. The permutation stage depends on the plain-image as well, and therefore the permutation process resists chosen-plaintext and know-plaintext attacks effectively. Regarding the diffusion process, we also design image content

dependent diffusion bitxoring operations. The pseudo-random gray value sequence is generated by two tent maps instead of one tent map in conventional diffusion functions to improve the security of the proposed scheme. The previous pixel gray value is applied to determine which tent map is used to generate the current pseudo-random numbers. The merit of such a compound pseudo-random sequence is related to the image content, and therefore robustly resists the cryptanalysis. The security and performance analysis of the proposed image encryption are carried out thoroughly, including histogram analysis, correlation coefficient analysis, entropy analysis, differential attack analysis, key space analysis, key sensitivity analysis, etc. All the experimental results show that the proposed image encryption scheme is highly secure and demonstrates excellent performance.

The Proposed Image Encryption Scheme

Skew Tent Map. Skew tent map is defined as Eq. (1) . It is chaotic for all the control parameters $a \in (0,1)$ with Lyapunov exponent $\sigma = -a\log_2 a - (1-a)\log_2(1-a) \geq \log 2 > 1$.

$$x_i = T_a(x_{i-1}) = \begin{cases} x_{i-1}/a, & \text{if } x_{i-1} \in [0,a], \\ (1-x_{i-1})/(1-a), & \text{if } x_{i-1} \in (a,1], \end{cases} \quad (1)$$

In this paper, we use three skew tent maps, one map is for the permutation process, the other two maps are applied in the diffusion process. The control parameters and initial condition values are respectively denoted as $a_i, x_0^i, i = 1,2,3$. The processed gray image is expressed as one 2D matrix I of size $H \times W$. Throughout the context, we set $L = H \times W / 2$; $floor(x)$ means the nearest integers less than or equal to x.

Permutation Process. For a 256 gray-scale image with height H and width W, it is an integer matrix of H rows and W columns, in which the values range from 0 to 255. Its data can be converted to a one-dimensional vector $P = \{p_1, p_2, \cdots, p_{H\times W}\}$, where p_i stands for the gray value of the image pixel in the row $\text{mod}(i-1, H)+1$ and column $floor((i-1)/H)+1$. We then split P into two equal parts $P_1 = \{p_1, p_2, \cdots, p_L\}$ and $P_2 = \{p_{L+1}, p_{L+2}, \cdots, p_{H\times W}\}$. The permutation process is depicted as follows.

Step 1. The sum of all gray values of matrix I is calculated and processed to get one integer number by $S = \text{mod}(\sum_{i=1}^{H}\sum_{j=1}^{W} I(i,j), 60) + 20$. The first skew tent map $T_a(x)$ with $a = a_1$ and initial value x_0^1 is iterated for S times and discard the iterated points so that the generated pseudo-random sequence later on will be related to the plain-image content. For simplicity, we also denote x_S as x_0^1 in the sequel. A minor change in the plain-image will cause the change of S. Therefore the corresponding cipher-images of two plain-images with minor difference will be dramatically different. Then proposed image encryption scheme will then resist differential attack analysis.

Step 2. Continue to iterate the skew tent map $T_a(x)$ with $a = a_1$ and initial value x_0^1 for L times and get the pseudo-random sequence $\{x_1^1, x_2^1, \cdots, x_L^1\}$.

Step 3. Sort $\{x_1^1, x_2^1, \cdots, x_L^1\}$ in ascendant order and get $\{\overline{x}_1^{-1}, \overline{x}_2^{-1}, \cdots, \overline{x}_L^{-1}\}$. Find the position of values $\{\overline{x}_1^{-1}, \overline{x}_2^{-1}, \cdots, \overline{x}_L^{-1}\}$ in $\{x_1^1, x_2^1, \cdots, x_L^1\}$ and mark down the corresponding position indices $S = \{s_1, s_2, \cdots, s_L\}$ such that $\overline{x}_i^{-1} = x_{s_i}^1$.

Step 4. Exchange the gray values of pixel pairs between P_1 and P_2 according to the yilded permutation S by $P_1(i) \leftrightarrow P_2(s_i),\ i = 1,2,\cdots,L.$

Step 5. Integrate the exchanged P_1 and P_2 together to be one permuted vector $B = [P_1, P_2]$ with length $H \times W$. It is used for the diffusion process.

Diffusion Process. We write B as $B=\{b_1,b_2,\cdots,b_{H\times W}\}$. The diffusion process is outlined as follows.

Step 1. Set the values of the control parameters a_2,a_3, the initial condition values x_0^2,x_0^3 and seed $c(0)$. For $i=1$ to $H\times W$, we execute Step 2 to Step 4.

Step 2. Calculate $t=\mathrm{mod}(c(i-1),2)$. If t is zero, then iterate the skew tent map with control parameter a_2 and current state x_{i-1}^2 to get the next state x_i^2 and get the next pseudo-random number $u(i)=x_i^2$. If t is one, then iterate the skew tent map with control parameter a_3 and current state x_{i-1}^3 to get next orbit point x_i^3 and get the next pseudo-random number $u(i)=x_i^3$.

Step 3. The key stream element $k(i)$ is calculated by $k(i)=floor(u(i)\times 256)$.

Step 4. The current pixel value of the cipher-image is modified according to Eq. (2), where $b(i)$, $k(i)$, $c(i)$, $c(i-1)$ are the current operated pixel in the permuted image, key stream element, output cipher pixel, previous cipher pixel, respectively.

$$c(i)=b(i)\oplus k(i)\oplus c(i-1). \tag{2}$$

Step5. Convert the yielded vector $(c(1),c(2),\cdots,c(H\times W))$ be one 2D matrix and the final cipher-image is then obtained. Encrypt the plain-image Lena one round with cipher key $a_1=0.761, a_2=0.371, a_3=0.839$, $x_0^1=0.321, x_0^2=0.41, x_0^3=0.83$ and seed $c(0)$=132, the resulted cipher-image is shown in Figure 1 (b).

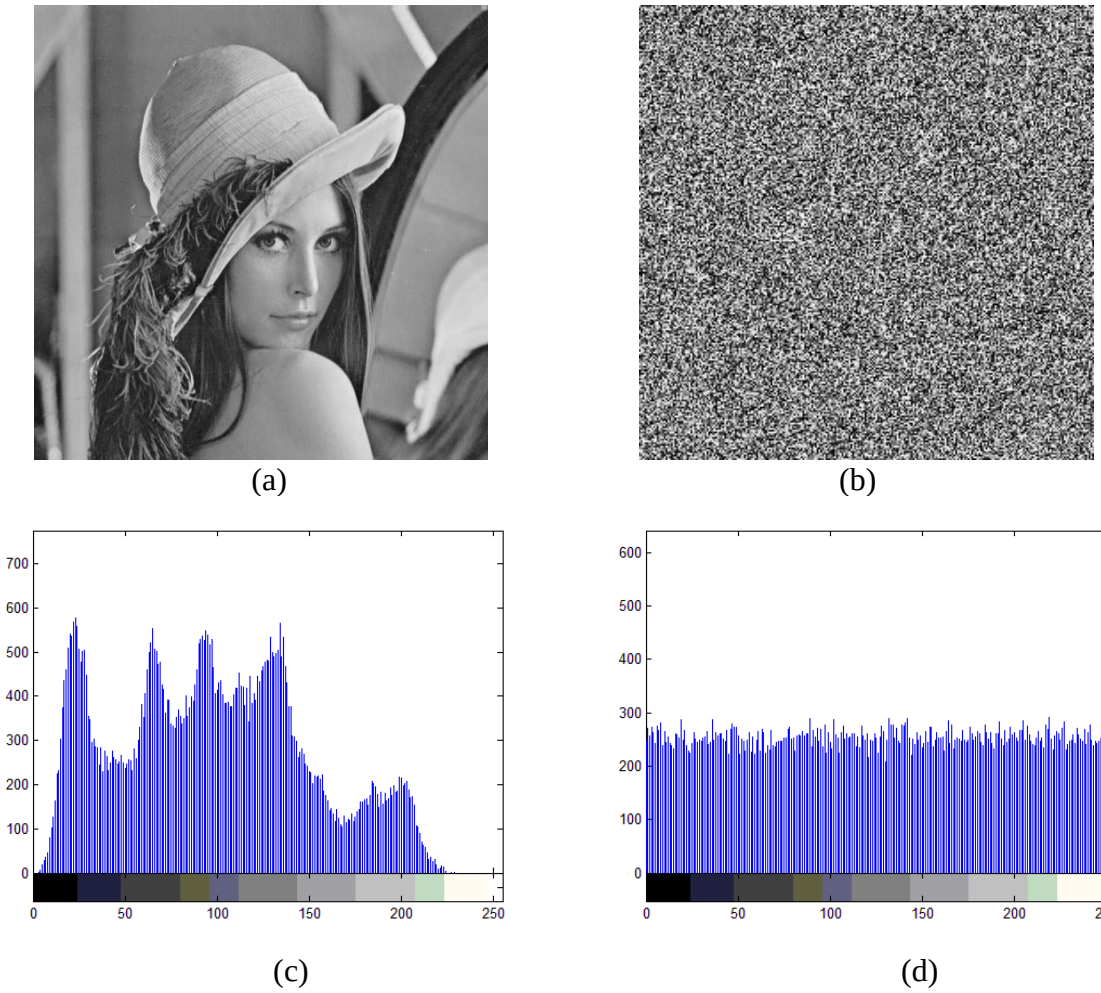


Fig.1. The encrypted results: (a) plain-image Lena, (b) cipher-image, (c) histogram of Lena, (d) histogram of cipher-image.

Performance Analysis

It is common sense that an ideal cryptosystem requires strong sensitivity to cipher keys as well as plaintexts, i.e., the cipher-texts should have strong correlation with cipher keys and plaintexts [15]. An ideal encryption scheme should have a large key space to make brute-force attack infeasible; it should also effectively resist various kinds of attacks like statistical analysis attack, differential attack, chosen plaintext attack and known plaintext attack, etc. In this section, the security and performance analyses have been carried out with details for the proposed image encryption scheme, including statistical analysis (histograms, correlation coefficients, information entropy), key space analysis, key sensitivity analysis, differential analysis, etc. Experimental results demonstrate that the proposed image encryption technique is highly secure and can be used for the secure image and video communication applications.

Histogram Analysis. Histogram analysis visually reveals the distribution information of pixel gray values of considered image, showing the number of pixels at each different intensity value existing in the considered image. A good encrypted image should have a uniform and completely different histogram in comparison with that of the plain-image. The histograms of plain-image Lean and its cipher-image are shown in Figures 1(c)-(d). It follows from the histogram of the cipher-image that it is fairly uniform and significantly different from the histogram of plain-image. Hence the proposed image encryption scheme does not provide any useful information for the opponents to perform any effective statistical analysis on the cipher-image.

Correlation Coefficient Analysis. As we know, the adjacent pixels' gray values for one meaningful and nature image vary gradually, implying that each pixel is highly correlated with its adjacent pixels. An ideal image encryption scheme should generate cipher-images with less correlation in the adjacent pixels. We calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels in plain and cipher image respectively. The correlation coefficient of the pairs is calculated by the following formulae:

$$Cr = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},\ cov(x,y) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y)),\ E(x) = \frac{1}{T}\sum_{i=1}^{T}x_i,\ D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2,$$

where x_i, y_i form the ith pair of horizontally, vertically or diagonally adjacent pixels, T is the total number of chosed adjacient pixel pairs. For a gray image of size $W \times H$, the values of T for horizontally, vertically and diagonally adjacent pixels pairs are $W \times (H-1)$, $(W-1) \times H$ and $(W-1) \times (H-1)$ respectively. The correlation coefficients of horizontally, vertically, diagonally adjacent pixels for plain-images Lena and cameraman, their corresponding cipher-images are given in Table 1. It is clear from Table 1 that the proposed image encryption technique significantly reduces the correlation between the adjacent pixels of the plain image.

Tab. 1. Correlation coefficients between adjacent pixels.

Test image	Direction	Plain-image	Cipher-image
Lena	Horizontal	0.9401	0.0011
	Vertical	0.9695	0.0032
	Diagonal	0.9180	-0.0092
Cameraman	Horizontal	0.9335	0.0029
	Vertical	0.9592	-0.0033
	Diagonal	0.9087	0.0017

Information Entropy Analysis. Information entropy measures the uncertainty of a random variable and therefore is usually used to measure disorder and randomness. Two extremely cases are:

a long sequence of repeating characters and a truly random sequence. The former has entropy of 0 since every character is predictable, and the latter has maximum entropy since there is no way to predict the next character in the sequence. As for image, it can be applied to measure the uniformity of image histograms as well. The entropy $H(m)$ of a gray image I can be measured by $H(I)=-\sum_{i=0}^{L-1} p(r_i)\log_2(p(r_i))$ (bits), where L is the gray levels of image, $p(r_i)$ stands for the probability of occurrence of gray r_i. For a random gray image with 256 gray scale levels, its entropy is $H(I)=8$ bits. We calculate the information entropy for plain-image Lena and its cipher-image. The results are 7.5683 and 7.9972 respectively. The value of information entropy for the cipher-image is very close to the expected value 8 of truly random image. Therefore the proposed encryption scheme is extremely robust against entropy attacks. Some other plain-images are tested to calculate the information entropies as shown in Table 2.

Tab. 2.Information entropy test.

Test image	Information entropy
Lena	7.9972
Cameraman	7.9975
Rice	7.9970
Aerial	7.9974

Key Sensitivity Analysis and Key Space Analysis. An ideal cipher should be extremely sensitive to cipher keys, which is an essential feature for any good cryptosystem in the sense that it can effectively make brute-force attacks infeasible if the key space is large enough. The key sensitivity of a cryptosystem can be observed from two aspects. (i) the cipher-images derived from the cryptosystem should be extraordinarily sensitive to cipher keys, i.e., if one uses two slightly different cipher keys to encrypt the same plain-image, then two produced cipher-images should be almost different and possess negligible correlation; (ii) the cipher-images cannot be decrypted correctly with a large percentage (e. g. near 100%) difference from the original plain-images although there is a slight difference between the encryption and decryption keys. In the proposed scheme, the key space is composed of all possible choices of a_1, a_2, a_3, x_0^1, x_0^2, x_0^3, $c(0)$.

To test the sensitivity of cipher key k, the original plain-image is encrypted with k, $k-\Delta\delta$, $k+\Delta\delta$ respectively while keeping the other cipher keys unchanged. The key sensitivity coefficient p_s is calculated by

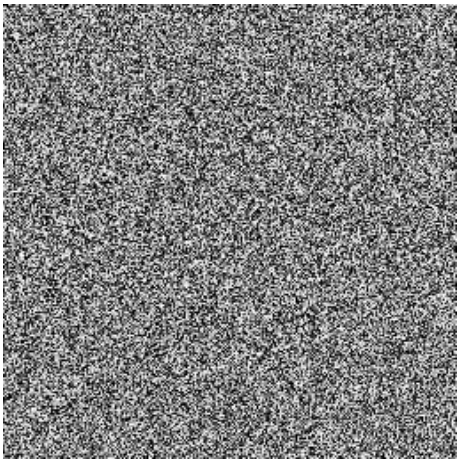
$$p'_s=\sum_{i=1}^{H}\sum_{j=1}^{W}[N_s(I_1(i,j),I_2(i,j))+N_s(I_1(i,j),I_3(i,j))],\ p_s=\frac{p'_s}{2\times M\times N}\times 100\%,\ N_s(x,y)=\begin{cases}1, x\neq y,\\ 0, x=y,\end{cases}$$

where I_1, I_2, I_3 are the encrypted images respectively, and $\Delta\delta$ is the perturbing value which can be used to calculate possible choices for the considered cipher key k. The test results are shown in Table 3. The experimental results show that all the cipher keys are all strongly sensitive. The key space is therefore calculated by $(10^{16})^6\times 256=256\times 10^{96}\approx 2^{327}$. Such a key space is large enough to stand brute-force attacks.

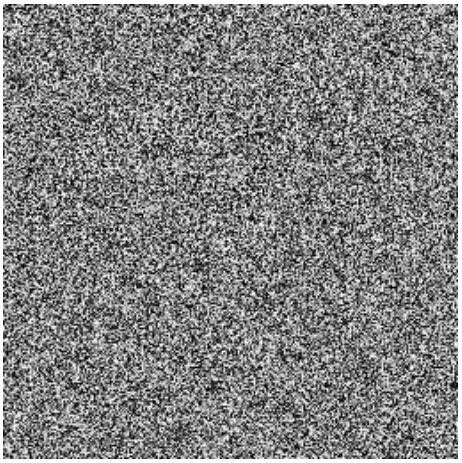
Tab. 3. Key sensitiviy test.

k	a_1	a_2	a_3	x_0^1	x_0^2	x_0^3	$c(0)$
p_s	99.61	99.56	99.50	99.59	99.56	99.48	99.62

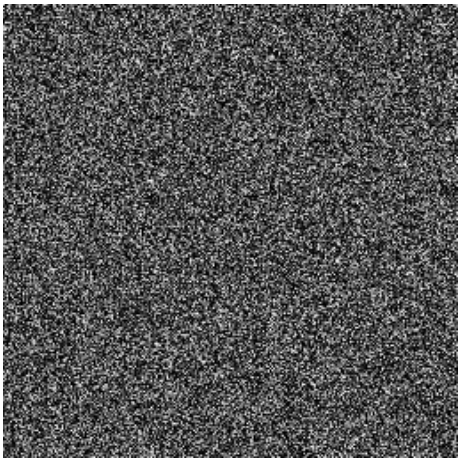
The sensitivity test can also be demonstrated visually. (i) Influence of minor change for cipher keys over encryption. We perform two simulations. The plain-image Lena is encrypted by the cipher keys $a_1 = 0.761, a_2 = 0.371, a_3 = 0.839$, $x_0^1 = 0.321, x_0^2 = 0.41, x_0^3 = 0.83$ and $c(0)$ =132, the cipher-image is shown in Figure 1(c). Replace a_1, x_0^2 by a_1=0.761+10^{-16}, $x_0^2 = 0.41+10^{-16}$ respectively, and keep the other cipher keys unchanged, the cipher-images are shown in Figures 2(a)-(b) respectively. The difference images between Figures 2(a)-(b) and Figure 1(b) are demenstrated in Figures 3(c)-(d) respectively. (ii) Influence of minor change for cipher keys over decryption. Replace a_2 by a_2=0.761+10^{-16} and keep the other cipher keys unchanged, the decrypted image is shown in Figure 3(a), which has a difference 99.61% from the plain-image Lena. Replace x_0^3 by x_0^3=0.83+10^{-16} and keep the other cipher keys unchanged, the decrypted image is shown in Figure 3(b), which has a difference 99.59% from Lena.



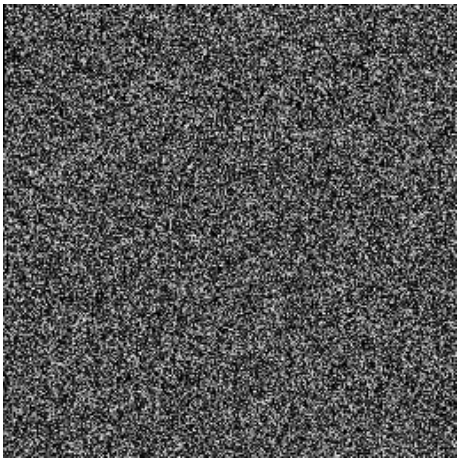
(a) Cipher-image by a_1=0.761+10^{-16}



(b) Cipher-image by $a = 0.41+10^{-16}$

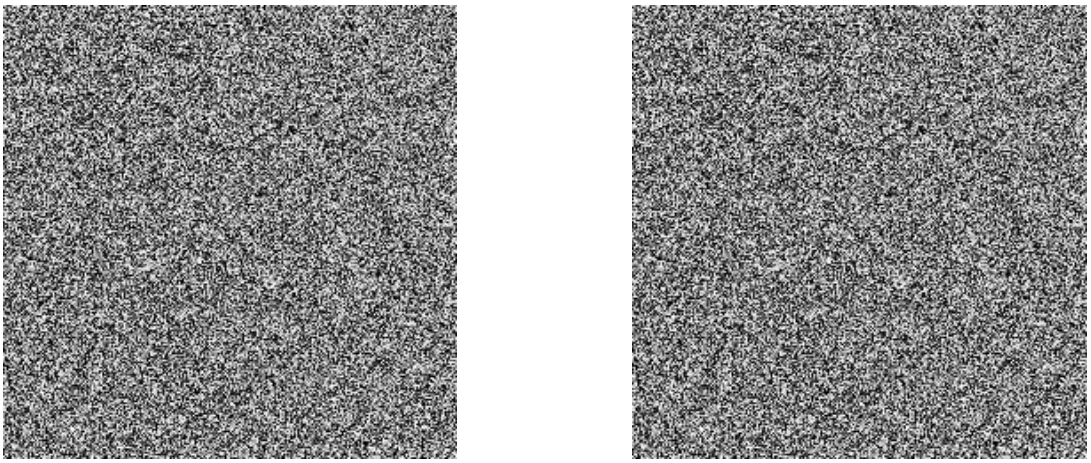


(c) Difference between Fig.2 (a) and Fig. 1(b)



(d) Difference between Fig.2 (b) and Fig.1(b)

Fig.2. Key sensitivity test I.



(a) Decrypted image by a_2=0.371+10^{-16} (b) Decrypted image by x_0^3=0.83+10^{-16}

Fig.3. Key sensitivity test II.

Differential Attack Analysis. Differential cryptanalysis focuses on the study of how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. As for image cryptosystems, attackers may usually modify only one pixel with one bit difference of the plain-image, then compare two cipher-images using the same cipher keys to find out some meaningful relationships between the plain-image and the cipher-image. If some meaningful relationships between plain-image and cipher-image are found in such analysis, they may further facilitate the attackers to determine the cipher keys or equivalent key streams. If one slight difference in the plain-image will cause significant, random and unpredictable changes in the cipher-image, the encryption scheme can resist differential analysis attack efficiently. To test the robustness of image cryptosystems against the differential cryptanalysis, two most common measures NPCR (number of pixel change rate) and UACI (unified average changing intensity) are used.

For a L-bit gray image with size $H \times W$, if C and $\bar{C}$ represent two cipher-images whose corresponding plain-images are of only one pixel difference, then NPCR and UACI are defined by

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}}{W \times H} \times 100\%, D_{i,j} = \begin{cases} 0, & if \ C_{i,j} = \bar{C}_{i,j}, \\ 1, & if \ C_{i,j} \neq \bar{C}_{i,j}. \end{cases} \quad \mathrm{UACI} = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W} \frac{|C_{i,j} - \bar{C}_{i,j}|}{2^L - 1} \times 100\%.$$

We randomly choose 10 pixels and calculate the valuses of NPCR and UACI. The results are shown in Table 4. We also randomly choose 200 pixels in plain-image randomly, and changing their intensity value by one unit at the selective pixel. The averages of 200 NPCR values and 200 UACI values are 99.6099% and 33.4781%. It is clear that the NPCR and UACI values are very close to the expected values 99.6094% and 33.4635%, thus the proposed image encryption technique shows good sensitivity to plaintext and hence invulnerable to differential attacks.

Tab. 4. Difference analysis of plain-image Lena.

Positions	(45,97)	(136,211)	(171,61)	(207,17)	(254,76)
NPCR(%)	99.6216	99.5743	99.6201	99.5972	99.6277
UACI(%)	33.4650	33.5188	33.4585	33.4358	33.4350
Positions	(235,50)	(107,221)	(14,33)	(18,236)	(155,246)
NPCR(%)	99.6262	99.6262	99.6033	99.6277	99.6475
UACI(%)	33.4334	33.5188	33.4129	33.5112	33.5168

Conclusion

An efficient permutation-diffusion based image encryption scheme using multiple tent maps is proposed. Both the permutation process and diffusion process are designed to be dependent on the plain-image contents and therefore the proposed image encryption scheme can resist cryptanalysis effectively. To improve the pemutation speed, one exchange permutation strategy is employed. The permutation is performed between two equal separate parts of the plain-image instead of the whole plain-image in traditional permuation process. Security analysis including key sensitivity analysis, key space analysis, statistical attack analysis, differential attack analysis, information entropy analysis are performed thoroughly. All the experimental results show that the proposed encryption scheme is secure thanks to its large key space, its high sensitivity to the cipher keys and plain-images. All these satisfactory properties make the proposed scheme a potential candidate for encryption of multimedia data such as images, audios and even videos.

Acknowledgement

This research is supported by Science and Technology Innovation-cultivation Fund of Guangdong Undergraduates and Innovation and Entrepreneurship Training Program of Guangdong Colleges.

References

[1] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998), 1259–1284.

[2] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Opt. Commun., 284(2011), 5290-5298.

[3] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, 1(2001), 6-21.

[4] Vinod Patidar, N.K. Pareek, G. Purohit, K.K. Sud, A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption, Optics Commun., 284(2011), 4331-4339.

[5] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Information Sciences, 181(2011), 1171-1186.

[6] W. Guo, J. Zhao, R. Ye, A chaos-based pseudorandom permutation and bilateral diffusion scheme for image encryption, I.J. Image, Graphics and Signal Processing, 6:11(2014), 50-61.

[7] R.Ye, A novel image encryption scheme based on generalized multi-sawtooth maps, Fundamenta Informaticae, 133(2014), 87-104.

[8] Y. Wang, K.W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals, 41(2009), 1773-1783.

[9] S. J. Li, C. Q. Li, G. R. Chen, N. G. Bourbakis, K. T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. Signal Process. Image Commun., 23(2009), 212-223.

[10] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution-diffusion based image cipher, Commun. Nonlinear Sci. Numer. Simulat., 15 (2010), 1887–1892.

[11] X. Wang, G. He, Cryptanalysis on a novel image encryption method based on total shuffling scheme, Opt. Commun., 284 (2011), 5804–5807.

[12]Y. Zhou, K. Panetta, S. Agaian, C. L. Philip Chen, Image encryption using P-Fibonacci transform and decomposition, Opt. Commun., 285(2012), 594-608.

[13] J. Chen, Z. Zhu, C. Fu, H. Yu, L. Zhang, An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering, 67 (2015), 191-204.

[14] Y. Zhang, X. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices, Applied Soft Computing, 26 (2015),10-20.

[15] B. Schiener, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and sons, New York, 1996.