International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.217-224
http://dx.doi.org/10.14257/ijsia.2015.9.7.19

Secret Sharing-Based Chaotic Image Encryption

Tiejun Zhang[a], Aya El-Fatyany [b], Li Li[c], Mohamed Amin [b], Ahmed A. Abd El-Latif [b]

[a]*Harbin University of Science and Technology, China Affiliation(s)*
[b] *Department of Mathematics, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt*
[c]*Shenzhen Institute of Information Technology, Shenzhen, 518172, China*
ahmed_rahiem@yahoo.com

Abstract

This paper presents an image encryption scheme for secure digital images based on secret sharing and coupled map lattices. In this scheme, the secret image is encrypted before the sharing phase based on key sequences generated by chaotic map lattices. Experimental results and analysis show that the proposed scheme has better security and can be easily protects both confidentiality and loss-tolerance simultaneously in shadow images.

Keywords: *Image encryption, Coupled map lattice, Confidentiality, Robustness*

1. Introduction

Secure secret image during transmission over unsecured channel is very important for robust image encryption, so we add the key sequence which is generated by chaotic map lattice for achieving both confidentiality and loss-tolerance. Image encryption phase based on Shamir's (k, n)-threshold method [1] has been studied [1-6], which is known as secret image sharing. Any *k* of the *n* shadow images generated by those methods can reconstruct the original secret image. Thus it tolerates at most *n*-*k* shadow images faulty or lost, and the loss-tolerance property is guaranteed. The confidentiality is usually realized by the cryptographic techniques, such as permutation on the original image before sharing phase with the variable *X* in Shamir's polynomial defined by constant numbers [1-4] or generated by RSA algorithm [4], which is neither efficient nor secure. Wherefore, proposing a new phase to protect both confidentially and loss-tolerance needs another study. In this work, we present a new scheme for encrypting secret images firstly and after that sharing them based on one way coupled map lattice and multiple chaotic systems, which protect both confidentiality and loss-tolerance simultaneously in sharing images over unsecured channel.

2. The Proposed Method

In this section, we propose an image encryption based on Shamir's polynomial and chaotic map lattices. The polynomial applied in the proposed scheme is given in Eq. (1) where $R_i^{\,j}$ is the random number for computing, the *i*th share $f_j(X_i^{\,j})$ in section *j*.

$$f_j(X_i^{\,j}) = P_1^{\,j} + P_2^{\,j} * X_i^{\,j} + \ldots P_k^{\,j} * X_i^{\,j\,(k-1)} + R_i^{\,j} \pmod{251} \quad (1)$$

where $P_l^{\,j}, X_i^{\,j}, R_i^{\,j} \in [0, 250]$, $l \in [1, k]$, $i \in [1, n]$, $j \in [1, M * N / k]$.

The proposed method is shown in Fig. 1. The implementation of the image sharing phase is the same as in [8]. There are two different keys used to encrypt the pixel values, one key is $X_i^{\,j}$, and the other is $R_i^{\,j}$. The difference between the

ISSN: 1738-9976 IJSIA

proposed method and method [8] is the second key R_i^j which helps to generate the secret shadow images. R_i^j is generated based on chaotic logistic map in form of lattice. The generation of X_i^j is the same as in method [8], while the steps generating R_i^j are nearly the same as those generating X_i^j in method [8] with different step 1 and step 2. In step 1 and step 2 of the proposed method, R_i^j is computed by one way coupled map lattice [5] as in Eqs. (5-6) instead of Eqs. (2-4).

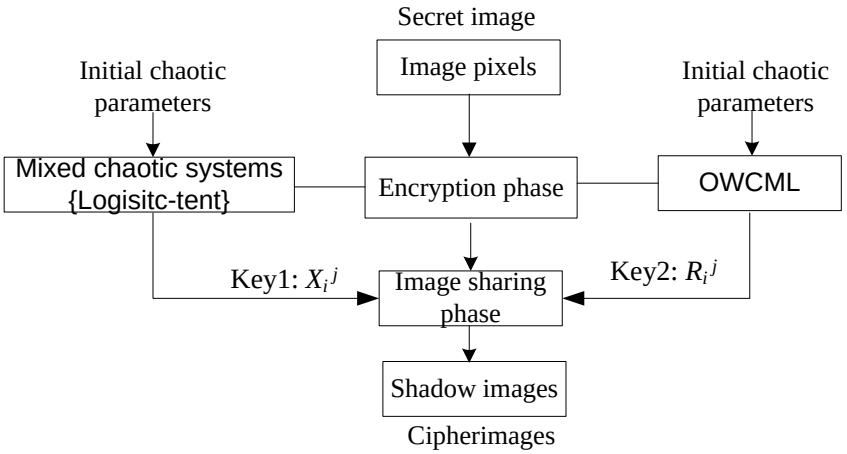


Figure 1. Encryption Diagram for the Proposed Method

$$\text{Logistic-Tent map: } T(x) = \begin{cases} (rx_n(1-x_n)+(4-r)x_n/2) \bmod 1 & x \le 0.5 \\ (rx_n(1-x_n)+(4-r)(1-x_n)/2) \bmod 1 & x \ge 0.5 \end{cases}, r \in [0, 2] \quad (2)$$

$$x_m = T(x_{m-1}),\ x_t \in [0, 1] \quad (3)$$

$$X_i^j = Round\ (x_m * 250) \quad (4)$$

$$\text{Coupled map lattice: } y_m = (1-\Upsilon)*r*y_{m-1}*(1-y_{m-1}) + \Upsilon*r*(1-y_{m-1})*(1-(y_{m-1}+1)),$$

$$y_t \in [0, 1],\ r \in [0, 4],\ \Upsilon=0.02 \quad (5)$$

$$R_i^j = Round\ (y_m * 250) \quad (6)$$

According to the steps in generating R_i^j, it assures to generate different R_1^j , R_2^j, …, R_n^j for all the n shares in each section j, and thus it will generate at most one of them equal to zero, e.g., R_i^j=0. Consider the same case discussed in Section 1 in which neighboring image sections from section 1 to section s are black areas. Even though the pixel values $P_1^1 = P_2^1 = \ldots = P_k^1 = \ldots = P_1^s = P_2^s = \ldots = P_k^s = 0$, after adding different random number R_i^j in each polynomial for share i in section j, at most one value $f_j(X_i^j)$=0 for all the n shares. Therefore, it will obtain different share value S_1^j,..., S_i^j,…, S_n^j and only $S_i^j = 0$ in section j. Furthermore, it has a low probability for $S_i^1 = S_i^2 = \ldots = S_i^s = 0$ in the same shadow image as shown in Figure 2. Thus it will not reveal any information about the secret image with large black neighboring areas.

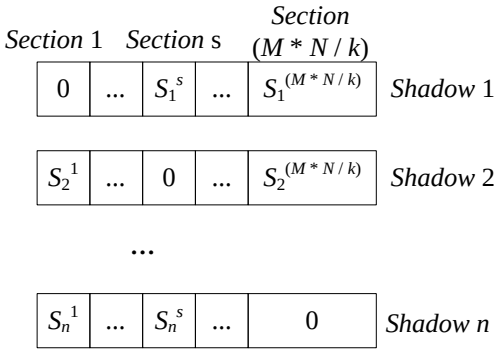


Figure 2. Shadow Image Generation

From the steps in generating X_i^j and R_i^j, we can see that X_i^j and R_i^j with the same share number i in different sections are generated with the same iteration number m but different initial values i.e. x_0, $x_0 + \delta_1$, …$x_0 + t_1 * \delta_1$, …, $x_{\max}$, and y_0, $y_0 + \delta_2$, …$y_0 + t_2 * \delta_2$, …, $y_{\max}$. This means that the distribution of pixel values in each shadow image is constrained by value x_0, t, δ_1, x_{max}, and y_0, t_1, δ_2, y_{max}. If $x_t = x_0 + t_1 * \delta > x_{max}$, $x_{t1} = x_0$. It is the same for y_{t2}. The value t_1 and t_2 in the initial value computation reflects after t_1 and t_2 times it will repeat the initial value x_0 and y_0 respectively, and they influence the X_i^j and R_i^j reflecting in the shadow image. For the images will small area of black pixels, the value t_1 and t_2 influence slightly for the randomness of shadow image since $f_j(X_i^j)$ is determined by P_l^j, X_i^j and R_i^j. Even X_i^j and R_i^j in section j are the same as in section q, P_l^j and P_l^q are different and nonzero, thus $f_j(X_i^j)$ does not equal to $f_q(X_i^q)$. But it is not the same for images with large area of black pixels which have zero pixel values in several sections. In the section with all zero pixel values, Eq. (2) degenerate to Eq. (7).

$$f_j(X_i^j) = R_i^j \pmod{251} \quad (7)$$

The corresponding pixel values $f_j(X_i^j)$ in the shadow image are only defined by R_i^j. In this case if t_2 is small, the pixel values $f_j(X_i^j)$ will repeat after a small image area which causes block effect and it is not random. Thus t_2 should be large enough in order to repeat previous pixel values only after a large image area in the same shadow image. For the inequality $y_0 + t_2 * \delta_2 > y_{max}$ with determined y_0 and y_{max}, if t_2 is large, δ_2 is small. Thus the increasing number δ_2 should be small.

3. Experimental Results

The We applied our proposed method on four kinds of standard gray scale images with size of 256*256, *i.e.* Pepper, Table, Houses and Girl are adopted in the experiments as shown in Figure 3 –Figure 6. And we used (2, 4) threshold scheme. While, each shadow image has 128*256. We implement three testing groups to compare the performance between method [8] and the proposed method. In table1 include the initial parameters for each chaotic map. Method [8] applies only chaotic tent map to generate X_i^j. our proposed method using one way coupled map lattice and logistic –tent map to generate X_i^j and R_i^j respectively. Figures 7(a-e)- Figures 8(a-e)- Figures 9(a-e)-Figiures 10(a-e) represents the shadow images and the recovered images by using any two shares images for the original images Figure 3, Figure 4, Figure 5, Figure 6. Our proposed method and method [8] have the same confidentiality as our proposed method using logistic-tent map for encryption first and then using one way coupled map lattice in share. . In comparison, Figure 11(a-d)-Figure 14(a-d) show the better confidentiality by using the proposed method with one way coupled map lattice parameter r = 3.999, $x0$ = 0.01, $m0$ = 100, andδ = 0.01. In contrast, Figure19(a-d)-Figure 20(a-d) used method [8] showed lower confidentiality than our proposed method. But we can clear the results by using another groups of experiments with one way coupled map lattice r = 3.999, $x0$ = 0.001, $m0$ = 100, andδ = 0.01on other images as Figure 15(a-d)-Figure 16(a-d). By using the last groups of experiments r = 3.999, $x0$ = 0.0001, $m0$ = 100, andδ = 0.01 we obtain the best performance on the images Figure 17 (a-d), Figure 18 (a-d). The experiments show that the proposed method could achieve a high security from human vision and more confidentiality by using Logistic-Tent map and One Way Coupled map Lattice

Table 1. Parameters Selected for Three Chaotic Maps Respectively

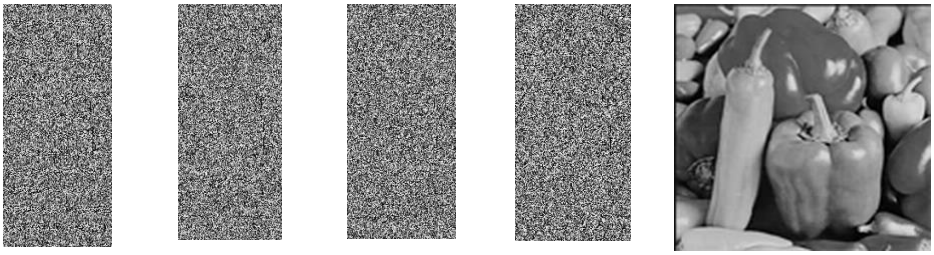
	R	x_0	m_0	Δ
Chaotic logistic- tent map for X_i^j generating all the shadow images	1.97	0.1	100	0.01
Chaotic one way coupled map lattice for R_1 generating Fig. 11-Fig. 14	3.999	0.01	100	0.01
Chaotic one way coupled map lattice for R_1 generating Fig. 15-Fig. 16	3.999	0.001	100	0.001
Chaotic one way coupled map lattice for R_1 generating Fig. 17-Fig. 18	3.999	0.0001	100	0.0000001

Figure 3. Pepper

Figure 4. Table

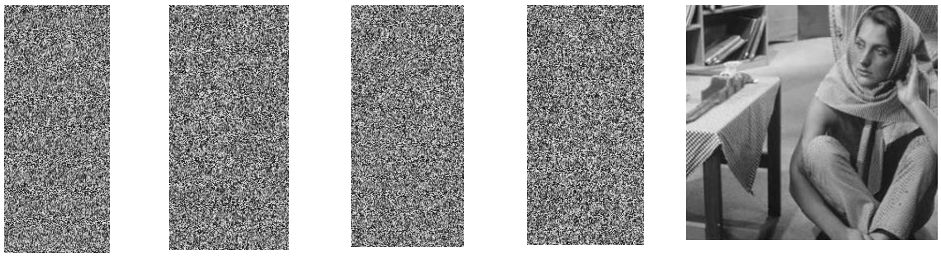
Figure 5. Houses

Figure 6. Girl



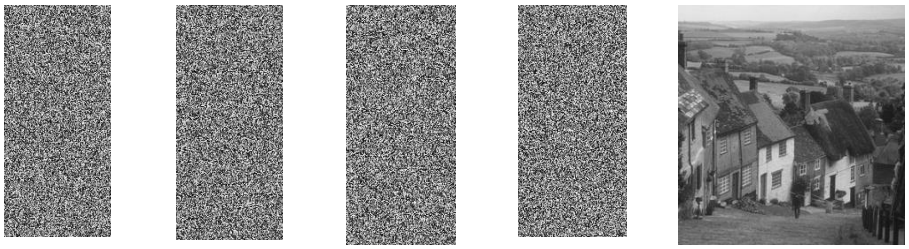
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Pepper

Figure 7. Shadow Images for *Pepper* Generated by Proposed Method



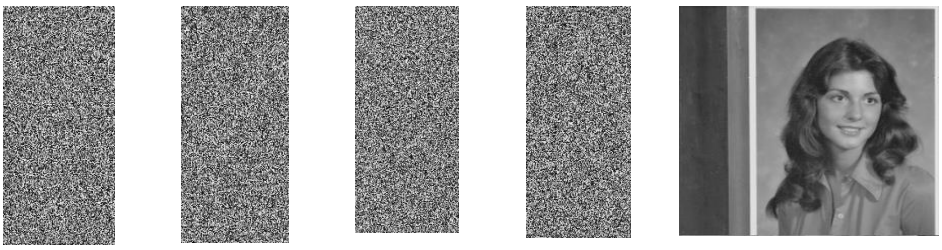
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Eyes

Figure 8. Shadow Images for *Table* Generated by Proposed Method



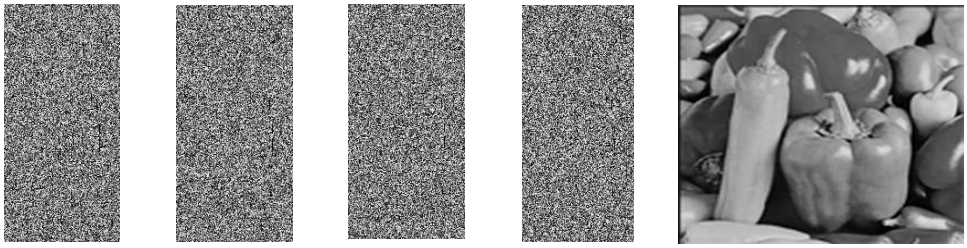
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Houses

Figure 9. Shadow Images for *Houses* Generated by Proposed Method



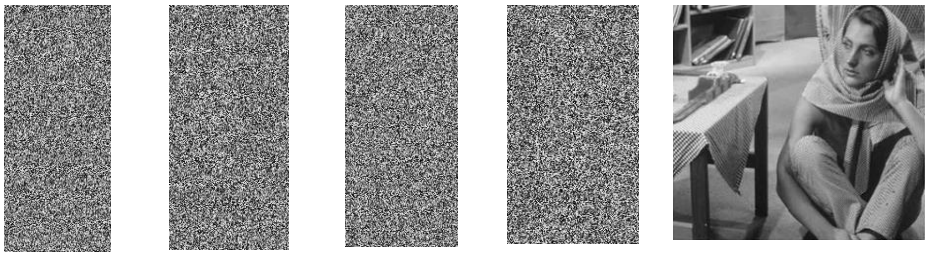
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Girl

Figure 10. Shadow Images for Girl Generated by Proposed Method



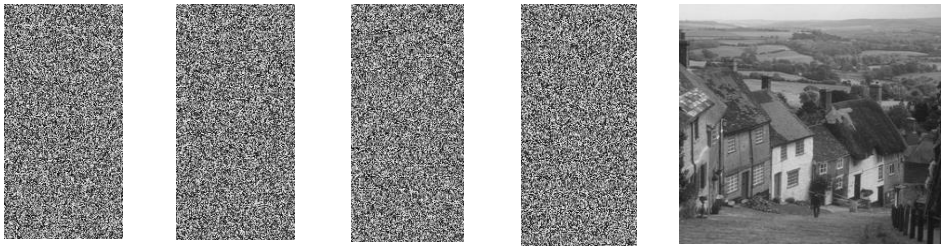
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Pepper

Figure 11. Shadow Images for Pepper Generated by Proposed Method with One Way Map Lattice Parameter r = 3.999, $x0$ = 0.01, $m0$ = 100, and δ= 0.01



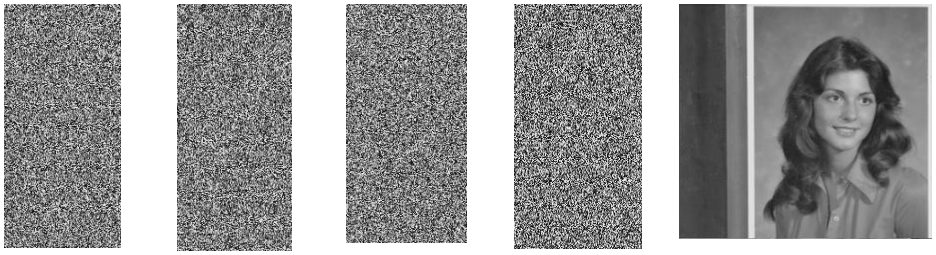
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Eyes

Figure 12. Shadow Images for Table Generated by Proposed Method with One Way Map Lattice Parameter r = 3.999, $x0$ = 0.01, $m0$ = 100, and δ= 0.01



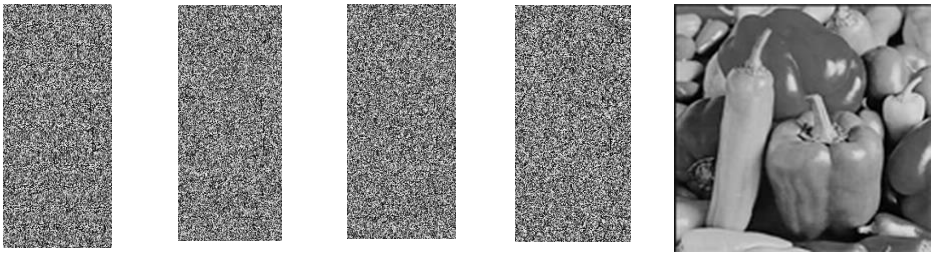
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Houses

Figure 13. Shadow Images for Houses Generated by Proposed Method with One Way Map Lattice Parameter r = 3.999, $x0$ = 0.01, $m0$ = 100, and δ= 0.01



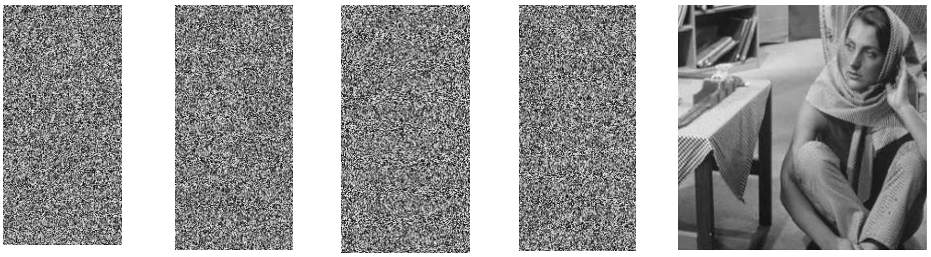
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Girl

Figure 14. Shadow Images for Girl Generated by with One way Map Lattice Parameter r = 3.999, $x0$ = 0.01, $m0$ = 100, and δ= 0.01



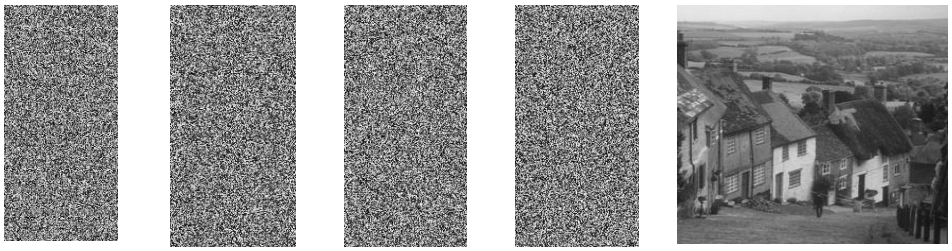
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Pepper

Figure 15. Shadow Images for Pepper Generated by Proposed Method with One Way Map Lattice Parameter *r* = 3.999, *x*0 = 0. 001, *m*0 = 100, and δ= 0.01



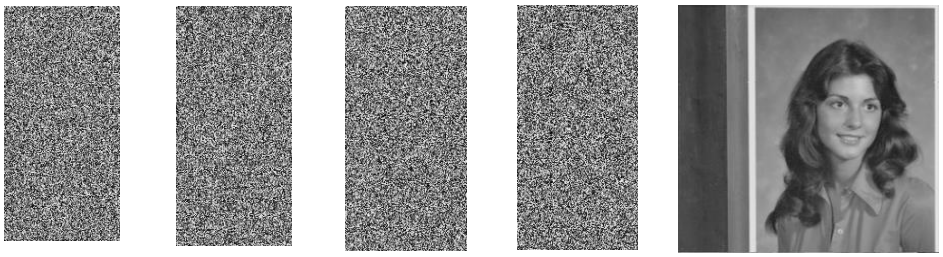
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Eyes

Figure 16. Shadow Images for Table Generated by Proposed Method with One Way Map Lattice Parameter *r* = 3.999, *x*0 = 0.001, *m*0 = 100, andδ= 0.01



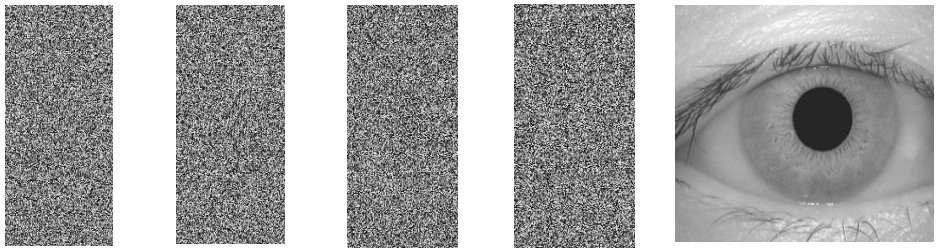
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Houses

Figure 17. Shadow Images for Houses Generated by Proposed Method with One Way Map Lattice Parameter *r* = 3.999, *x*0 = 0. 0001, *m*0 = 100, andδ= 0.01



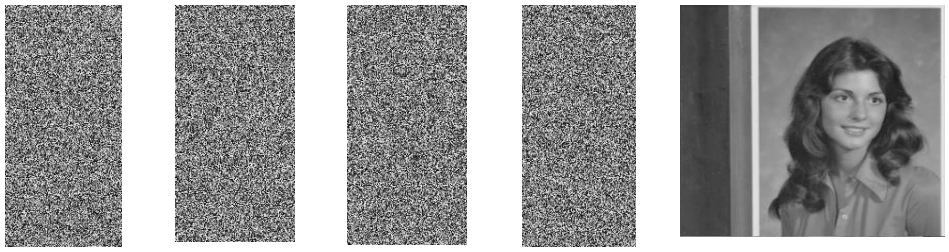
(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Girl

Figure 18. Shadow Images for Girl Generated by with One Way Map Lattice Parameter *r* = 3.999, *x*0 = 0.0001, *m*0 = 100, andδ= 0.01



(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Girl

Figure 19. Shadow Images for Iris Generated by Method [8]



(a) Shadow 1 (b) Shadow 2 (c) Shadow 3 (d) Shadow 4 (e) Recovered Girl

Figure 20. Shadow Images for Girl Generated by Method [8]

4. Security Analysis and Comparison with Related Schemes

4.1 Security Analysis:

a) *Brute-force Attack:* K possible values of X_i^j and R_i^j are $P(251,k)=251*250*\ldots*(251-k+1)$. There are totally $(P(251, k))^2$ possible values**.**

b) *Collusion Attack:-*

b.1) *Best case*:- K of($R_1^j,\ldots, R_n^j$ and $X_1^j,\ldots, X_n^j$)is the same in each section; there are totally
$2K + 1$ variables for K equations. Thus it has infinite solutions. P_l^j with a successful probability $(1/251)^{M*N/k}$ for all sections.
b.2) *Worst case*:- K of($R_1^j,\ldots, R_n^j$ and $X_1^j,\ldots, X_n^j$) is different in each section; there are totally $k + 2K$ variables for K equations. It also has infinite solutions. The successful probability is $(1/251)^{k*(M*N/k)} = (1/251)^{M*N}$ for all sections. The conspirators only succeed in a low probability between $(1/251)^{M*N}$ and $(1/251)^{M*N/k}$.

4.2 Comparison with Related Schemes:

	Li's et al scheme [8]	**Proposed scheme**
Probability to recover the original image	$1/ P(251, k)^{(2*M*N/k)}$.	$1/ P(251, k)^{(2*M*N/k)}$.
Chaotic system used	Tent and logistic chaotic map	one way coupled map lattice and Logistic-Tent map
Strength of the random sequence	long period is low by using two chaotic system	long period is high by using one way coupled map lattice and Logistic-Tent map

5. Concluding Remarks

This paper has presented an image encryption scheme for sharing secret images based on Shamir's polynomial and chaotic map lattices. The proposed scheme adapted one way coupled map lattice in Shamir's polynomial equation as a key stream for encryption. Experimental results and security analysis shows that the proposed scheme has good security and performance in sharing secret images such as confidentiality and loss-tolerance.

Acknowledgment

This work is supported by ministry of higher education and scientific research (Egypt-Tunisia co-operation research: 4-13-A1), Natural Science Foundation of Heilongjiang Province, China: QC2014C076", and the National Natural Science Foundation of China (Project number: 61361166006).

References

[1] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, (**1979**), pp. 612-613.
[2] C. C. Thien, and J. C. Lin, "Secret image sharing, Computers and Graphics, vol. 26, (**2002**), pp. 765-770.
[3] S. J. Lin, and J. C. Lin, "VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," Pattern Recognition, vol. 40, (**2007**), pp. 3652-3666.
[4] C. N. Yang, and C. B. Ciou, "Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability," Image and Vision Computing, vol. 28, (**2010**), pp. 1600-1610.
[5] R. Zhao, J. J. Zhao, F. Dai, and F. Q. Zhao, "A New Image Secret Sharing Scheme to Identify Cheaters," Computer Standards &Interfaces, vol. 31, no. 1, (**2009**), pp. 252-257.
[6] M. Amin, O. S. Faragallah, and A. A. Abd El-Latif, "A chaotic block cipher algorithm for image cryptosystems," Commun Nonlinear Sci Numer Simulat, vol. 15, (**2010**), pp. 3484-3497.
[7] W. P. Fang, "Secret image sharing safety," IEICE Proceeding on 14th Asia-Pacific IEEE International Conference Communications (APCC2008), Akihabara, Tokyo, Japan, October (**2008**).
[8] L. Li, A. A. A. El-Latif, Z. Shi and, X. Niu, "A New Loss-Tolerant Image Encryption Scheme Based on Secret Sharing and Two Chaotic Systems", Research Journal of Applied Sciences, Engineering and Technology, vol. 4, no. 8, pp. 877-883, 2012 ISSN: 2040-7467 (**2011**).
[9] Li. Li, A. A. Abd El-Latif, C. Wang, Q. Li and X. Niu, "A Novel Secret Image Sharing Scheme based on Chaotic System", Proc. SPIE. 8334, Fourth International Conference on Digital Image Processing (**2012**).

