Breaking a new substitution-diffusion based image cipher using chaotic standard and logistic maps

Chengqing Li*,a, Shujun Li*,b, Kwok-Tung Loa

aDepartment of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China
bFachbereich Informatik und Informationswissenschaft, Universität Konstanz, Fach M697, Universitätsstraße 10, 78457 Konstanz, Germany

Abstract

Recently, an image encryption scheme based on chaotic standard and logistic maps was proposed. This paper studies the security of the scheme and shows that it can be broken with only one chosen-plaintext. Some other security defects of the scheme are also reported.

Key words: cryptanalysis, chosen-plaintext attack, encryption, image

1. Introduction

With the rapid development of information technology, multimedia data are transmitted over all kinds of wired/wireless networks more and more frequently. Consequently, the security of multimedia data becomes a serious concern of many people. However, the traditional text encryption schemes can not be used in a naive way to protect multimedia data efficiently in some applications, mainly due to the big differences between textual and multimedia data and some special requirements of the whole multimedia system. This challenge stirs the design of special multimedia encryption schemes to become a hot research topic in multimedia signal processing area in the past decade. Because of the subtle similarity between chaos and cryptography, a great number of multimedia encryption schemes based on chaos have been presented [1, 2, 3, 4]. Unfortunately, many of them have been found to have security problems from the cryptographical point of view [5, 6, 7, 8, 9]. Some general rules about evaluating security of chaos-based encryption schemes can be found in [10, 11].

Since 2003, Pareek et al. have proposed a number of different encryption schemes based on one or more chaotic maps [12, 13, 14, 15]. Recent cryptanalytic results [16, 17, 18] have shown that all the three schemes proposed in [12, 13, 14] have security defects. In [15], a new image encryption scheme based on the Logistic and standard maps was proposed, where the two maps are used to generate a pseudo-random number sequence (PRNS) controlling two kinds of encryption operations. The present paper focuses on a re-evaluation of the security of this new scheme, and reports the following findings: 1) the scheme can be broken with only one chosen image; 2) there are also some other security defects of the scheme.

---

*Corresponding authors.

Email address: zjulcq@gmail.com (Chengqing Li)

URL: www.hooklee.com (Shujun Li)

The rest of this paper is organized as follows. Section 2 introduces the image encryption scheme under study briefly. Our cryptanalytic results are presented in Sec. 3 in detail. The last section concludes the paper.

2. The image encryption scheme under study

The plaintext encrypted by the image encryption scheme under study is a RGB true-color image of size $M \times N$ (height$\times$width), which can be denoted by an $M \times N$ matrix of 3-tuple pixel values $\boldsymbol{I} = \{(R(i,j), G(i,j), B(i,j))\}_{\substack{0 \leq i \leq M-1 \\ 0 \leq j \leq N-1}}$. Denoting the cipher image by $\boldsymbol{I}' = \{(R'(i,j), G'(i,j), B'(i,j))\}_{\substack{0 \leq i \leq M-1 \\ 0 \leq j \leq N-1}}$, the image encryption scheme can be described as follows[1].

- *Secret key*: three floating-point numbers x_0, y_0, K, and one integer L, where x_0, $y_0 \in (0, 2\pi)$, $K > 18$, $100 < L < 1100$.

- *Initialization*: prepare data for encryption/decryption by performing the following steps.

  a) Generate four XORing keys as follows: $Xkey(0) = \lfloor 256x_0/(2\pi) \rfloor$, $Xkey(1) = \lfloor 256y_0/(2\pi) \rfloor$, $Xkey(2) = \lfloor K \bmod 256 \rfloor$, $Xkey(3) = (L \bmod 256)$.

  b) Iterate the standard map Eq. (1) from the initial conditions (x_0, y_0) for L times to obtain a new chaotic state (x'_0, y'_0). Then, further iterate it for MN more times to get MN chaotic states $\{(x_i, y_i)\}_{i=1}^{MN}$.

$$\begin{cases} x = (x + K\sin(y)) \bmod (2\pi), \\ y = (y + x + K\sin(y)) \bmod (2\pi), \end{cases} \tag{1}$$

  c) Iterate the Logistic map Eq. (2) from the initial condition $z_0 = ((x'_0 + y'_0) \bmod 1)$ for L times to get a new initial condition z'_0. Then, further iterate it for MN times to get MN chaotic states $\{z_i\}_{i=1}^{MN}$.

$$z = 4z(1-z). \tag{2}$$

  d) Generate a chaotic key stream (CKS) image $\boldsymbol{I}_{CKS} = \{(CKSR(i,j), CKSG(i,j), CKSB(i,j))\}_{\substack{0 \leq i \leq M-1 \\ 0 \leq j \leq N-1}}$ as follows: $CKSR(i,j) = \lfloor 256x_k/(2\pi) \rfloor$, $CKSG(i,j) = \lfloor 256y_k/(2\pi) \rfloor$ and $CKSB(i,j) = \lfloor 256z_k \rfloor$, where $k = iN + j + 1$.

- *Encryption procedure*: a simple concatenation of the following four encryption operations.

  – *Confusion I*: masking the plain pixel values by the four XORing keys $\{Xkey(i)\}_{i=0}^3$. For $k = 0, \ldots, MN - 1$, do the following masking operations.

$$\begin{aligned} R^\star(i,j) &= R(i,j) \oplus Xkey((3 \cdot k) \bmod 4), & (3) \\ G^\star(i,j) &= G(i,j) \oplus Xkey((3 \cdot k + 1) \bmod 4), & (4) \\ B^\star(i,j) &= B(i,j) \oplus Xkey((3 \cdot k + 2) \bmod 4), & (5) \end{aligned}$$

  where $i = \lfloor k/N \rfloor$, $j = (k \bmod N)$.

---

[1]To make the presentation more concise and complete, some notations in the original paper are modified.

- *Diffusion I*: scanning all pixel values from the first one row by row (from top to bottom), and masking each pixel (except for the first scanned pixel) by its predecessor in the scan. Set $R^*(0,0) = R^\star(0,0)$, $G^*(0,0) = G^\star(0,0)$, $B^*(0,0) = B^\star(0,0)$. For $k = 1, \ldots, MN-1$,

$$
\begin{align}
R^*(i,j) &= R^\star(i,j) \oplus R^*(i',j'), \tag{6} \\
G^*(i,j) &= G^\star(i,j) \oplus G^*(i',j'), \tag{7} \\
B^*(i,j) &= B^\star(i,j) \oplus B^*(i',j'), \tag{8}
\end{align}
$$

where $i = \lfloor k/N \rfloor$, $j = (k \bmod N)$, $i' = \lfloor (k-1)/N \rfloor$ and $j' = ((k-1) \bmod N)$.

- *Diffusion II*: scanning all pixel values from the last one column by column (from right to left), and masking each pixel (except for the first scanned pixel) by its predecessor in the scan.

  Set $R^{**}(M-1,N-1) = R^*(M-1,N-1)$, $G^{**}(M-1,N-1) = G^*(M-1,N-1)$, $B^{**}(M-1,N-1) = B^*(M-1,N-1)$. For $k = MN-2, \ldots, 0$,

$$
\begin{align}
R^{**}(i,j) &= R^*(i,j) \oplus G^{**}(i',j') \oplus B^{**}(i',j'), \tag{9} \\
G^{**}(i,j) &= G^*(i,j) \oplus B^{**}(i',j') \oplus R^{**}(i',j'), \tag{10} \\
B^{**}(i,j) &= B^*(i,j) \oplus R^{**}(i',j') \oplus G^{**}(i',j'), \tag{11}
\end{align}
$$

where $i = (k \bmod M)$ and $j = \lfloor k/M \rfloor$, $i' = ((k+1) \bmod M)$, $j' = \lfloor (k+1)/M \rfloor$.

- *Confusion II*: masking the pixel values with the CKS image pixel by pixel. For $k = 0, \ldots, MN-1$,

$$
\begin{align}
R'(i,j) &= R^{**}(i,j) \oplus CKSR(i,j), \tag{12} \\
G'(i,j) &= G^{**}(i,j) \oplus CKSG(i,j), \tag{13} \\
B'(i,j) &= B^{**}(i,j) \oplus CKSB(i,j). \tag{14}
\end{align}
$$

where $i = \lfloor k/N \rfloor$, $j = (k \bmod N)$.

- *Decryption procedure*: the simple reversion of the above encryption procedure.

3. Cryptanalysis

3.1. A chosen-plaintext attack

In the chosen-plaintext attack, the attacker can choose plaintexts arbitrarily and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which helps reveal the other plaintexts encrypted with the same secret key. For the image encryption scheme under study, an equivalent version of the secret key can be reconstructed easily from only one pair of chosen-plaintext as shown in Proposition 1.

Lemma 1. *Let $\bar{\boldsymbol{I}}^{**}$ denote the encryption result of $\boldsymbol{I}$ without performing the two confusion steps. Then, $\boldsymbol{I}' = \bar{\boldsymbol{I}}^{**} \oplus \bar{\boldsymbol{I}}^{**}_{Xkey} \oplus \boldsymbol{I}_{CKS}$.*

Proof. After the first confusion step, $\boldsymbol{I}^\star = \boldsymbol{I} \oplus \boldsymbol{I}_{Xkey}$, where $\boldsymbol{I}_{Xkey}$ is the pseudo-image composed of the four XORing keys. Observing the operations involved in the two diffusion steps, we can see both steps can be performed on $\boldsymbol{I}$ and $\boldsymbol{I}_{Xkey}$ separately and XOR the results, which means that $\boldsymbol{I}^{**} = \bar{\boldsymbol{I}}^{**} \oplus \bar{\boldsymbol{I}}^{**}_{Xkey}$. Then, after performing the last confusion step, we have $\boldsymbol{I}' = \bar{\boldsymbol{I}}^{**} \oplus \bar{\boldsymbol{I}}^{**}_{Xkey} \oplus \boldsymbol{I}_{CKS}$, which proves this lemma. □

Proposition 1. *If I_0 is a zero image, i.e., $I_0 = 0$, then $I' = \bar{I}^{**} \oplus I_0'$.*

Proof. This is a straightforward result of the fact $I_0^{\star} = 0 \oplus I_{Xkey} = I_{Xkey}$. □

In case I_0' is known, the above proposition means that the plain-image I can be recovered from I' by the following steps: 1) $\bar{I}^{**} = I' \oplus I_0'$; 2) perform the two diffusion steps on $\bar{I}^{**}$ in an inverse order, which exactly recovers I. In other words, by taking I_0 as a chosen-image, we can get an equivalent key I_0' to decrypt any cipher-image encrypted with the same secret key (x_0, y_0, K, L).

We have performed some experiments to verify the correctness of the above chosen-plaintext attack. With the secret key $(x_0, y_0, K, L) = (3.98235562892545, 1.34536356538912, 108.54365761256745, 110)$, the equivalent key I_0' was constructed from the zero image, which are shown in Figs. 1a and b, respectively. Then, I_0' was used to recover the cipher-image shown in Fig. 1c, and successfully recovered the plain-image "Lenna" (Fig. 1d).

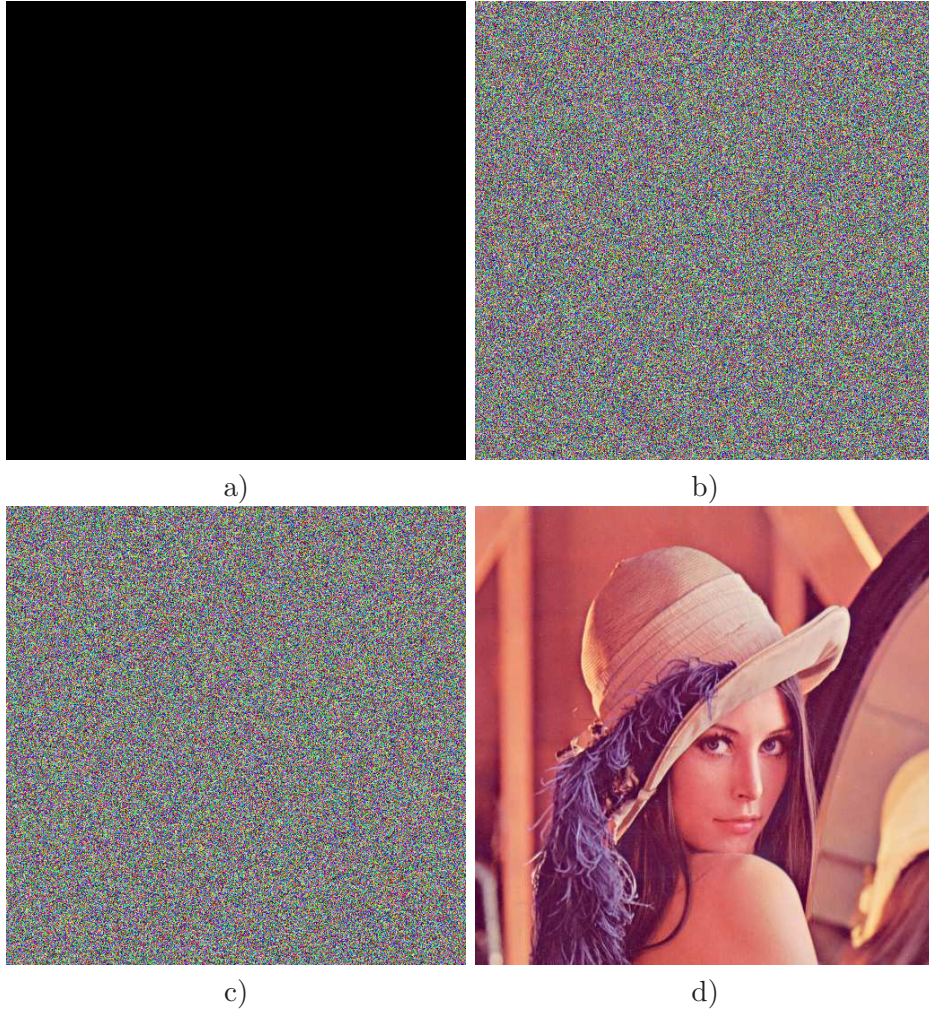Figure 1: An experimental result of the proposed chosen-plaintext attack: a) the chosen plain-image $I_0 = 0$; b) the equivalent key I_0'; c) a cipher-image encrypted with the same key; d) the recovered plain-image "Lenna".

3.2. Some other security problems

3.2.1. Insufficient randomness of the PRNS $\{CKSB(k)\}$

As illustrated in [19], the randomness of the pseudo-random bit sequence derived from chaotic states generated by iterating Logistic map is very weak. To further verify the randomness of the PRNS $\{CKSB(k)\}$ generated via the Logistic map of fixed control parameter, the NIST statistical test suite [20] was employed to test the randomness of 100 PRNSes of length $512 \cdot 512 = 262144$ (the number of bytes used for encryption of a 512×512 plain color image). Note that the 100 sequences were generated with randomly selected secret keys. For each test, the default significance level 0.01 was used. The results are shown in Table 1, from which one can see that the PRNS $\{CKSB(k)\}$ is not random enough.

Table 1: The performed tests with respect to a significance level 0.01 and the number of sequences passing each test in 100 randomly generated sequences.

Name of Test	Number of Passed Sequences
Frequency	95
Block Frequency ($m = 100$)	0
Cumulative Sums-Forward	93
Runs	0
Rank	0
Non-overlapping Template ($m = 9$, $B = 010000111$)	10
Serial ($m = 16$)	0
Approximate Entropy ($m = 10$)	0
FFT	0

3.2.2. Insensitivity with respect to change of plaintext

In [15, Sec. 5.5], it is recognized that the sensitivity of cipher-image generated by an image encryption scheme with respect to change of plain-image is very important, but the image encryption scheme under study is actually very far from the desired property. As well known in cryptography, this property is termed as avalanche effect. Ideally, it requires the change of any single bit of plain-image will make every bit of cipher-image change with a probability of one half. However, the image encryption scheme under study can not satisfy this property due to the following points.

- Only one kind of operation (XOR) is involved in the whole scheme;

- Any bit of plain-image only influences the bits at the same level in the cipher-image;

- Any pixel of plain-image does not influence other pixels in the cipher-image uniformly.

To show this defect clearly, we made an experiment by changing only one bit of the red channel of the plain-image shown in Fig. 1d. It is found that only some bits at the same level in the corresponding cipher-image were changed. The locations of the changed bits are shown in Fig. 2, in which the white dots denote changed locations and black ones denote unchanged ones.
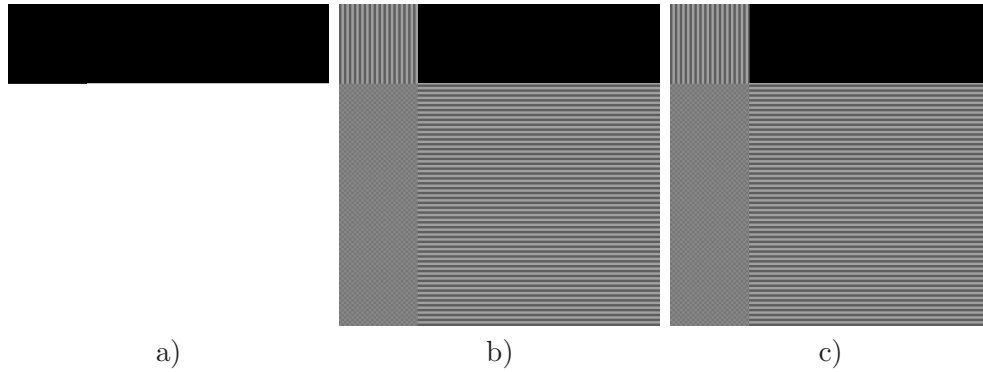
Figure 2: The locations of changed bits in different color channels of the cipher-image, when the 6-th bit of the red component of the pixel at location (127, 127) in the plain-image was changed: a) red channel; b) green channel; c) blue channel.

4. Conclusion

In this paper, the security of a new image encryption scheme based on two chaotic maps is analyzed in detail. It is found that the scheme can be broken with only one chosen plain-image. In addition, some other security defects about randomness of a PRNS involved, and sensitivity with respect to change of plain-image are also reported. Due to such a low level of security, we recommend not to use the image encryption scheme under study in any serious applications.

Acknowledgement

References

[1] H.-C. Chen, J.-C. Yen, A new cryptography system and its VLSI realization, Journal of Systems Architecture 49 (7-9) (2003) 355–367.

[2] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3d chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.

[3] N. J. Flores-Carmona, M. Carpio-Valadez, Encryption and decryption of images with chaotic map lattices, Chaos 16 (3) (2006) art. no. 033118.

[4] X. Tong, M. Cui, Image encryption with compound chaotic sequence cipher shifting dynamically, Image and Vision Computing 26 (6) (2008) 843–850.

[5] C. Li, G. Chen, On the security of a class of image encryption schemes, in: Proceedings of 2008 IEEE Int. Symposium on Circuits and Systems, 2008, pp. 3290–3293.

[6] S. Li, C. Li, G. Chen, K.-T. Lo, Cryptanalysis of the RCES/RSES image encryption scheme, Journal of Systems and Software 81 (7) (2008) 1130–1143.

[7] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos 18 (3) (2008) art. no. 033112.

[8] G. Jakimoski, K. Subbalakshmi, Cryptanalysis of some multimedia encryption schemes, IEEE Transactions on Multimedia 10 (3) (2008) 330–338.

[9] C. Li, S. Li, G. Chen, W. A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, Image and Vision Computing 27 (8) (2009) 1035–1039.

[10] G. Álvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.

[11] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital images and videos, in: B. Furht, D. Kirovski (Eds.), Multimedia Security Handbook, CRC Press, 2004, Ch. 4, pp. 133–167.

[12] N. Pareek, V. Patidar, K. Sud, Discrete chaotic cryptography using external key, Physics Letters A 309 (1-2) (2003) 75–82.

[13] N. Pareek, V. Patidar, K. Sud, Cryptography using multiple one-dimensional chaotic maps, Communications in Nonlinear Science and Numerical Simulation 10 (7) (2005) 715–723.

[14] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9) (2006) 926–934.

[15] V. Patidar, N. Pareek, K. Sud, A new substitution-diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation 14 (7) (2009) 3056–3075.

[16] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a discrete chaotic cryptosystem using external key, Physics Letters A 319 (3-4) (2003) 334–339.

[17] C. Li, S. Li, G. Álvarez, G. Chen, K.-T. Lo, Cryptanalysis of a chaotic block cipher with external key and its improved version, Chaos, Solitons & Fractals 37 (1) (2008) 299–307.

[18] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image and Vision Computing 27 (9) (2009) 1371–1381.

[19] C. Li, S. Li, G. Álvarez, G. Chen, K.-T. Lo, Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations, Physics Letters A 369 (1-2) (2007) 23–30.

[20] A. Rukhin, et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22, available online at `http://csrc.nist.gov/rng/rng2.html` (2001).