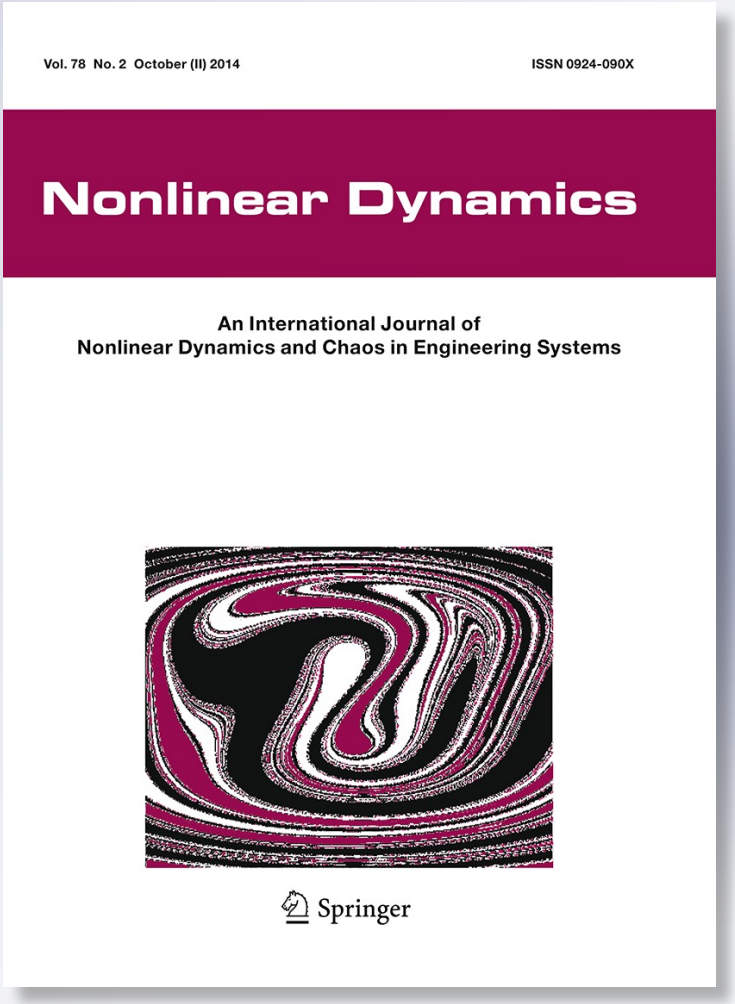
Cryptanalyzing image encryption using chaotic logistic map

Chengqing Li, Tao Xie, Qi Liu & Ge Cheng

Nonlinear Dynamics
An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems

ISSN 0924-090X
Volume 78
Number 2

Nonlinear Dyn (2014) 78:1545-1551
DOI 10.1007/s11071-014-1533-8



Springer

Nonlinear Dyn (2014) 78:1545–1551
DOI 10.1007/s11071-014-1533-8

ORIGINAL PAPER

Cryptanalyzing image encryption using chaotic logistic map

Chengqing Li · Tao Xie · Qi Liu · Ge Cheng

Received: 19 September 2013 / Accepted: 6 June 2014 / Published online: 3 July 2014

Abstract Chaotic behavior arises from very simple non-linear dynamical equation of logistic map which makes it was used often in designing chaotic image encryption schemes. However, some properties of chaotic maps can also facilitate cryptanalysis especially when they are implemented in digital domain. Utilizing stable distribution of the chaotic states generated by iterating the logistic map, this paper presents a typical example to show insecurity of an image encryption scheme using chaotic logistic map. This work will push encryption and chaos be combined in a more effective way.

Keywords Cryptanalysis · Chosen-plaintext attack · Image encryption · Logistic map

1 Introduction

With the rapid development of information transmission technology and popularization of multimedia capture device, 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 cannot protect multimedia data efficiently, mainly due to the big differences between textual and multimedia data, such as strong redundancy between neighboring elements of uncompressed multimedia data, bulky size of multimedia data, and some special requirements of the whole multimedia processing system. This challenge stirs the design of special multimedia encryption schemes to become a hot research topic in multimedia processing area in the past two decades.

Because there are some subtle similarities between chaos and cryptography, chaos were used to design potential secure and efficient schemes in all kinds of applications in cryptography. Due to easy presentation of image datum, most cryptographic schemes consider image data as operation object [6,17,22]. According to the record of *Web of Science*, about two thousands of articles on chaos-based cryptology were published in the past two decades. Unfortunately, many of them have been found to have security problems of different degrees from the viewpoint of modern cryptology [2,3,7,9–11,24]. In general, cryptanalysis (breaking or reporting some security defects) of a given encryption scheme requires rigorous theoretical support, so only about one-tenth of the proposed chaos-based encryption schemes were reported being cryptanalyzed till now. At the same time, the conventional cryptanalysis skills cannot be directly used to break the chaos-based

C. Li (✉) · T. Xie · Q. Liu
MOE Key Laboratory of Intelligent Computing and Information Processing, College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China
e-mail: Chengqingg@gmail.com

G. Cheng
School of Mathematics and Computational Science, Xiangtan University, Xiangtan 411105, Hunan, China

encryption schemes due to some reasons, such as difference of essential structure, and some special security defects caused by the properties of the adopted chaos system [5,13,25]. Therefore, short of security scrutiny of the proposed chaos-based encryption schemes has become bottleneck of progress of chaos-based cryptology. Some general rules about evaluating security of chaos-based encryption schemes are concluded in [1,14].

Logistic map is a discrete quadratic recurrence form of the logistic equation, a model of population growth first published by P. Verhulst in 1845. The application of logistic map in cryptology can be traced back to John von Neumann's suggestion on utilizing it as a random number generator in 1947 [23]. Due to simple form and relatively complex dynamical properties of logistic map, it was extensively used to design encryption schemes or pseudo-random number generator [4,8,20]. Even in *Web of Science*, one can find about two hundred records on application of logistic map in cryptography published between 1998 and 2013. A few papers reported some security deficiencies caused by logistic map [15,19].

In [18], an image encryption scheme based on the logistic and standard maps was proposed, where the two maps are iterated to generate some pseudo-random number sequences (PRNS) controlling twice exclusive OR (XOR) operations. In [21], it is reported that an equivalent key of the scheme can be obtained from only one known/chosen plain-image and the corresponding cipher-image. However, the equivalent key can only be used to decrypt other cipher-images of smaller or the same size of the known/chosen plain-image. Based on a dynamical property of logistic map on stable distribution of its chaotic states, the present paper re-evaluates the security of the scheme, and finds that the scope of all the subkeys can be narrowed much by an efficient brute-force search.

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 Sect. 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 $\mathbf{I} = \{(R(i,j), G(i,j), B(i,j))\}_{\substack{0\le i\le M-1\\ 0\le j\le N-1}}$. Denoting the cipher-image by $\mathbf{I}' = \{(R'(i,j), G'(i,j), B'(i,j))\}_{\substack{0\le i\le M-1\\ 0\le j\le N-1}}$, 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: $Xkey(0) = \lfloor 256x_0/(2\pi)\rfloor$, $Xkey(1) = \lfloor 256y_0/(2\pi)\rfloor$, $Xkey(2) = \lfloor K \mod 256\rfloor$, $Xkey(3) = (L \mod 256)$. Then, generate a pseudo-image $\mathbf{I}_{Xkey} = \{(R_{Xkey}(i,j), G_{Xkey}(i,j), B_{Xkey}(i,j))\}_{\substack{0\le i\le H-1\\ 0\le j\le W-1}}$ by assigning an $M \times N$ matrix with the four XORing keys repeatedly:

$$\begin{aligned} R_{Xkey}(i,j) &= Xkey(3k \mod 4),\\ G_{Xkey}(i,j) &= Xkey((3k+1) \mod 4),\\ B_{Xkey}(i,j) &= Xkey((3k+2) \mod 4),\\ &\text{where } k = iN + j. \end{aligned}$$

  (b) Iterate the standard map

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

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

  (c) Iterate the logistic map

$$f(x) = 4x(1-x) \tag{1}$$

  from the initial condition $z_0 = ((x_0' + y_0') \mod 1)$ for L times to get a new initial condition z_0'. Then, further iterate it for MN times to get MN chaotic states $\{z_i\}_{i=1}^{MN}$.

  (d) Generate a chaotic key stream (CKS) image $\mathbf{I}_{CKS} = \{(CKSR(i,j), CKSG(i,j), CKSB(i,j))\}$

[1] To make the presentation more concise and complete, some notations in the original paper are modified provided that its essential form kept unchanged.

$_{0\le i\le M-1}^{0\le j\le N-1}$ as follows: $CKSR(i,j) = \lfloor 256x_k/(2\pi)\rfloor$, $CKSG(i,j) = \lfloor 256y_k/(2\pi)\rfloor$ and

$$CKSB(i,j) = \tilde{z}_k = \lfloor 256 z_k \rfloor, \tag{2}$$

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 $k = 0, \ldots, MN-1$, set

$$R^{\star}(i,j) = R(i,j) \oplus R_{Xkey}(i,j),$$
$$G^{\star}(i,j) = G(i,j) \oplus G_{Xkey}(i,j),$$
$$B^{\star}(i,j) = B(i,j) \oplus B_{Xkey}(i,j),$$

    where $i = \lfloor k/N \rfloor$, $j = (k \mod N)$.
  - *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 $k = 1, \ldots, MN-1$, set

$$R^*(i,j) = R^{\star}(i,j) \oplus R^*(i',j'),$$
$$G^*(i,j) = G^{\star}(i,j) \oplus G^*(i',j'),$$
$$B^*(i,j) = B^{\star}(i,j) \oplus B^*(i',j'),$$

    where $i = \lfloor k/N \rfloor$, $j = (k \mod N)$, $i' = \lfloor (k-1)/N \rfloor$ and $j' = ((k-1) \mod N)$.
  - *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 $k = MN-2, \ldots, 0$, set

$$R^{**}(i,j) = R^*(i,j) \oplus G^{**}(i',j') \oplus B^{**}(i',j'),$$
$$G^{**}(i,j) = G^*(i,j) \oplus B^{**}(i',j') \oplus R^{**}(i',j'),$$
$$B^{**}(i,j) = B^*(i,j) \oplus R^{**}(i',j') \oplus G^{**}(i',j'),$$

    where $i = (k \mod M)$, $j = \lfloor k/M \rfloor$, $i' = ((k+1) \mod M)$, $j' = \lfloor (k+1)/M \rfloor$.
  - *Confusion II*: masking the pixel values with the CKS image pixel by pixel. For $k = 0, \ldots, MN-1$, set

$$R'(i,j) = R^{**}(i,j) \oplus CKSR(i,j),$$
$$G'(i,j) = G^{**}(i,j) \oplus CKSG(i,j),$$
$$B'(i,j) = B^{**}(i,j) \oplus CKSB(i,j).$$

    where $i = \lfloor k/N \rfloor$, $j = (k \mod N)$.
  - *Decryption procedure* is the simple reversion of the above encryption procedure.

3 Cryptanalysis

In [21, Sect. 4.2], it has been reported that an equivalent secret key of the image encryption scheme under study can be reconstructed with only one pair of known plain-image and the corresponding cipher-image. More rigorous presentation of the attack was represented in [12, Sect. 3.1]. The equivalent form of the secret key can only decrypt other cipher-image of smaller or the same size of the known plain-image. In this section, we first briefly introduce how the equivalent secret key is obtained, then discuss how to derive further information about secret key utilizing special dynamical properties of the logistic map.

Denoting the horizontal and vertical diffusion processes by HD and VD, respectively, the image encryption scheme under study can be represented as

$$\begin{aligned}\mathbf{I}' &= \mathrm{VD}(\mathrm{HD}(\mathbf{I} \oplus \mathbf{I}_{Xkey})) \oplus \mathbf{I}_{CKS} \\ &= \mathrm{VD}(\mathrm{HD}(\mathbf{I})) \oplus \mathrm{VD}(\mathrm{HD}(\mathbf{I}_{Xkey})) \oplus \mathbf{I}_{CKS} \\ &= \mathrm{VD}(\mathrm{HD}(\mathbf{I})) \oplus \mathbf{I}_{key},\end{aligned}$$

where

$$\mathbf{I}_{key} = \mathbf{I}^*_{Xkey} \oplus \mathbf{I}_{CKS}, \tag{3}$$

and

$$\mathbf{I}^*_{Xkey} = \mathrm{VD}(\mathrm{HD}(\mathbf{I}_{Xkey}).$$

As both HD and VD are independent on the secret key and $\mathbf{I}_{key}$ is dependent on neither the plaintext $\mathbf{I}$ nor the ciphertext $\mathbf{I}'$, one can see that $\mathbf{I}_{key}$ can be used as an equivalent key to decrypt any ciphertext of size which is smaller than or equal to $M \times N$, encrypted by the same secret key (x_0, y_0, K, L). In the following, we will show that the scope of x_0, y_0, K, and L can be further narrowed under the same condition.

The key idea of the enhanced attack is to search the values of $\{Xkey(i)\}_{i=0}^{3}$ by brute-force search and verify the search with stable self-correlation of the blue channel of $\mathbf{I}_{CKS}$, $\{CKSB(i,j)\}_{\substack{0\le i\le M-1\\0\le j\le N-1}}$, which is obtained from states of logistic map. Two main points supporting the attack are described as follows.

– *Deterministic relationship between* $\{Xkey(i)\}_{i=0}^{3}$ *and* $\mathbf{I}^{*}_{Xkey}$
Obviously, every element of $\mathbf{I}^{*}_{Xkey}$ comes from set $\{Xkey(0), Xkey(1), Xkey(2), Xkey(3), Xkey(0)\oplus Xkey(1), Xkey(0)\oplus Xkey(2), Xkey(0)\oplus Xkey(3), Xkey(1)\oplus Xkey(2), Xkey(1)\oplus Xkey(3), Xkey(2)\oplus Xkey(3), Xkey(0)\oplus Xkey(1)\oplus Xkey(2), Xkey(0)\oplus Xkey(1)\oplus Xkey(3), Xkey(1)\oplus Xkey(2)\oplus Xkey(3), Xkey(0)\oplus Xkey(2)\oplus Xkey(3), Xkey(0)\oplus Xkey(1)\oplus Xkey(2)\oplus Xkey(3)\}$. Given M, N, and $\{Xkey(i)\}_{i=0}^{3}$, $\mathbf{I}^{*}_{Xkey}$ is fixed. Assigning $\{Xkey(i)\}_{i=0}^{3}$ with four different numbers, e.g., $\{1, 2, 4, 9\}$, the construction of $\mathbf{I}^{*}_{Xkey}$ can be known. Scan $\mathbf{I}^{*}_{Xkey}$ in the raster order, and convert it into a one-dimensional sequence. Note that not every element of $\{Xkey(i)\}_{i=0}^{3}$ have independent influence on $\mathbf{I}^{*}_{Xkey}$ when $T = 4$, where T denotes period of the one-dimensional version of $\mathbf{I}^{*}_{Xkey}$. For example, the non-periodic component of $\mathbf{I}^{*}_{Xkey}$ is $\{Xkey(2), Xkey(2)\oplus Xkey(3), Xkey(0)\oplus Xkey(1)\oplus Xkey(3), Xkey(0)\oplus Xkey(1)\}$ when $M = N = 9$, where different combinations of $Xkey(0)$ and $Xkey(1)$ may generate the same version of $\mathbf{I}^{*}_{Xkey}$. Under condition $M = N$, the relationship between T and N is shown in Proposition 1. Fortunately, from Proposition 2, one can see that only a very minor portion of combinations of M and N making not every element of $\{Xkey(i)\}_{i=0}^{3}$ has independent influence on $\mathbf{I}^{*}_{Xkey}$.

– *Stable self-correlation of* $\{CKSB(i,j)\}_{\substack{0\le i\le M-1\\0\le j\le N-1}}$
Recall Eq. (2), one can calculate $\Delta_k = \mu_k - 4$, where

$$\mu_k = (\tilde{z}_{k+1}/256)/((\tilde{z}_k/256)\cdot(1-(\tilde{z}_k/256))).$$

As well known, distribution of chaotic trajectories generated by iterating the map Eq. (1) is stable. To verify this, distributions of a great number of chaotic trajectories generated by iterating Logistic map Eq. (1) for 10^5 times under random initial conditions were studied. All the distributions are quite similar to each other, so only one typical example is shown in Fig. 1 (See the invariant density of logistic map with parameter $r = 4$ in [16, Fig. 2]). Furthermore, distribution of Δ_k is stable also under different values of z_0. To verify this point, a great number of initial values of z_0 are chosen randomly. For each value of z_0, the corresponding sequence $\{\tilde{z}_k\}$ is produced by transforming the corresponding logistical states with Eq. (2). As distributions of Δ_k are similar to each other, only the distribution of Δ_k under the initial value used in Fig. 1 is shown in Fig. 2. To show the point more clearly, the distribution of Δ_k over some given intervals are shown in Table 1. In addition, distribution of Δ_k is very sensitive to change of $\tilde{z}_k$ or $\tilde{z}_{k+1}$ (See Figs. 2, 3, 4, 5). So, this stable self-correlation of $\{CKSB(i,j)\}_{\substack{0\le i\le M-1\\0\le j\le N-1}}$ can be used to verify the search of $\{Xkey(i)\}_{i=0}^{3}$.

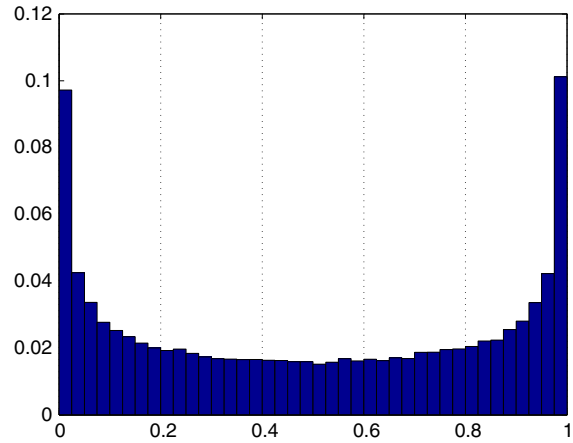


Fig. 1 Distribution of trajectory of the map Eq. (1) under initial state $z_0 = 0.226$

Proposition 1 *When $M = N$, T, and N satisfies that*

$$T = \begin{cases} 4 & if\ (N \mod 2) = 1; \\ 2N & if\ (N \mod 4) = 0; \\ 4N & if\ (N \mod 4) = 2. \end{cases} \tag{4}$$

Proof This proposition has been verified by computer for $N = 3, \ldots, 1204$. We leave this proposition under the larger scope of N as a conjecture.

Proposition 2 *The necessary condition making not every element of* $\{Xkey(i)\}_{i=0}^{3}$ *have independent influence on* $\mathbf{I}^{*}_{Xkey}$ *is that*

$$|M - N| \le 1. \tag{5}$$

Table 1 The distribution of Δ_k corresponding to the initial state $z_0 = 0.226$

z_0	$(-\infty, -10)$	$[-10^{i+1}, -10^{i})_{i=0}^{-4}$	$[-10^{-4}, 10^{-4})$	$[10^{i}, 10^{i+1})_{i=-4}^{0}$	$[10, +\infty)$
0.326	0.0195	0.0474 0.1435 0.3216 0.0897 0	0.0267	0.0150 0.0672 0.1588 0.0709 0.0196	0.0202
0.761	0.0204	0.0481 0.1431 0.3177 0.0899 0	0.0274	0.0143 0.0678 0.1610 0.0709 0.0197	0.0198
0.539	0.0203	0.0469 0.1437 0.3222 0.0905 0	0.0270	0.0141 0.0672 0.1581 0.0705 0.0192	0.0203
0.487	0.0200	0.0480 0.1412 0.3230 0.0905 0	0.0265	0.0146 0.0660 0.1593 0.0716 0.0193	0.0201
0.194	0.0206	0.0491 0.1419 0.3199 0.0879 0	0.0276	0.0150 0.0666 0.1599 0.0719 0.0192	0.0204
0.875	0.0210	0.0484 0.1430 0.3201 0.0893 0	0.0271	0.0152 0.0662 0.1603 0.0698 0.0198	0.0199
0.942	0.0211	0.0483 0.1417 0.3217 0.0877 0	0.0270	0.0154 0.0663 0.1597 0.0712 0.0194	0.0205
0.293	0.0205	0.0479 0.1426 0.3201 0.0905 0	0.0267	0.0147 0.0662 0.1597 0.0725 0.0187	0.0199

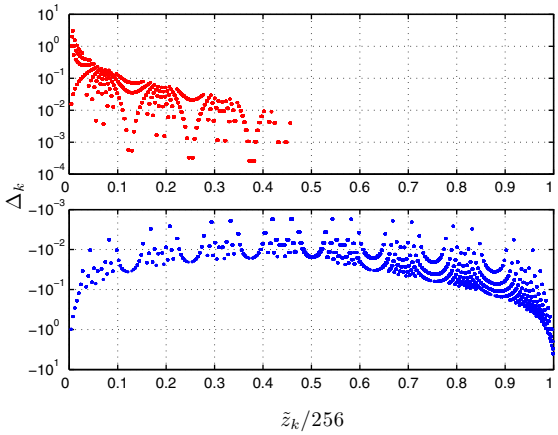


Fig. 2 Distribution of $\{(\tilde{z}_k/256, \Delta_k)\}_{k=1}^{10^5}$ when $z_0 = 0.226$

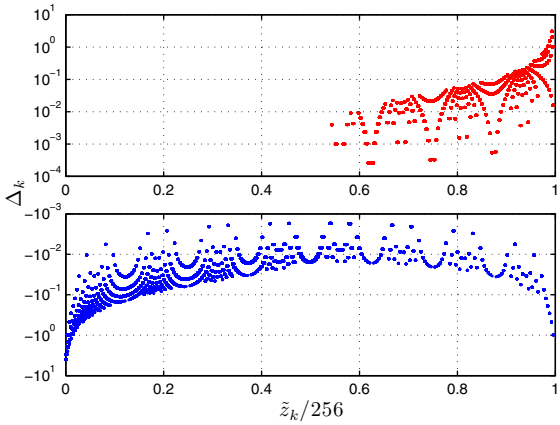


Fig. 3 The version of the distribution shown in Fig. 2 when only $\tilde{z}_k$ is wrong: $\tilde{z}_k$ is replaced by $\tilde{z}_k + 1$

Proof This proposition has been verified by computer for $3 \le M, N \le 1204$. We leave this proposition under the larger scope of M and N as a conjecture.

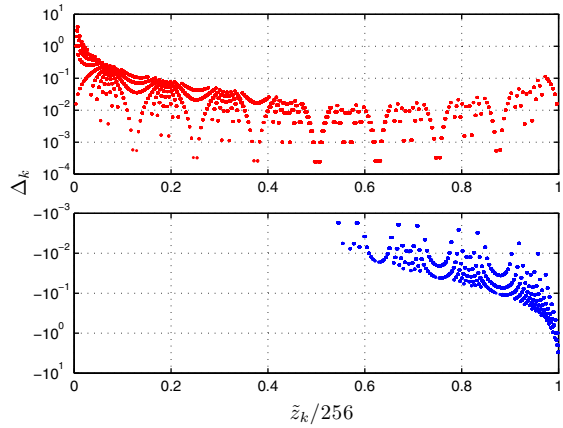


Fig. 4 The version of the distribution shown in Fig. 2 when only $\tilde{z}_{k+1}$ is wrong: $\tilde{z}_{k+1}$ is replaced by $\tilde{z}_{k+1} + 1$

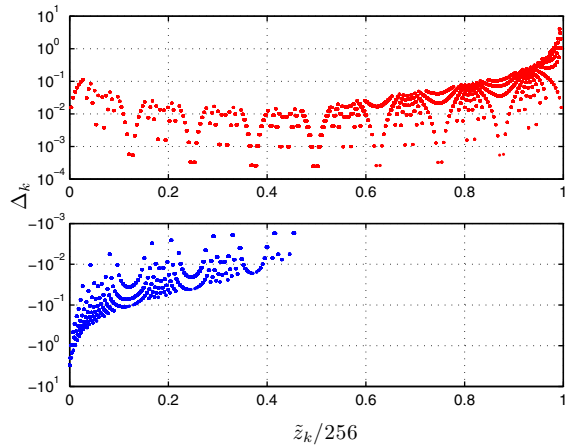


Fig. 5 The version of the distribution shown in Fig. 2 when $\tilde{z}_{k+1}$ and $\tilde{z}_k$ are both wrong: $\tilde{z}_k$ and $\tilde{z}_{k+1}$ are replaced by $\tilde{z}_k + 1$ and $\tilde{z}_{k+1} + 1$, respectively

Table 2 The distribution of Δ_k corresponding to 16 possible neighbouring values of the possible set of $\{Xkey\}_{i=0}^{3}$, {162,54,108,110}

index	$[-10^{i+1}, -10^{i})_{i=0}^{-4}$	$[-10^{-4}, 10^{-4})$	$[10^{i}, 10^{i+1})_{i=-4}^{0}$
1	0.0629 0.1614 0.2716 0.0629 0.0000	0.0157	0.0078 0.1023 0.1811 0.1023 0.0275
2	0.0515 0.1666 0.2698 0.0238 0.0000	0.0357	0.0119 0.0753 0.2023 0.1230 0.0357
3	0.0476 0.1468 0.3373 0.0714 0.0000	0.0357	0.0119 0.0992 0.1626 0.0714 0.0119
4	0.0480 0.1600 0.3240 0.0480 0.0000	0.0240	0.0080 0.0720 0.2000 0.0800 0.0320
5	0.0557 0.1474 0.3187 0.0557 0.0000	0.0438	0.0119 0.0876 0.1434 0.1235 0.0079
6	0.0478 0.1673 0.2709 0.0557 0.0000	0.0239	0.0039 0.0876 0.2151 0.0956 0.0278
7	0.0632 0.1660 0.2885 0.0553 0.0000	0.0197	0.0079 0.0869 0.1699 0.1067 0.0316
8	0.0434 0.1778 0.2529 0.0395 0.0000	0.0316	0.0079 0.0869 0.2252 0.0909 0.0395
9	0.0634 0.1587 0.3055 0.0674 0.0000	0.0317	0.0079 0.0634 0.1587 0.1230 0.0158
10	0.0515 0.1666 0.2698 0.0714 0.0000	0.0198	0.0000 0.0753 0.2182 0.1031 0.0198
11	0.0634 0.1507 0.3492 0.0714 0.0000	0.0079	0.0079 0.0753 0.1468 0.0873 0.0357
12	0.0396 0.1507 0.3253 0.0595 0.0000	0.0277	0.0079 0.0873 0.1904 0.0793 0.0277
13	0.0632 0.1581 0.2964 0.0790 0.0000	0.0079	0.0039 0.0909 0.1620 0.1027 0.0316
14	0.0478 0.1513 0.3067 0.0438 0.0000	0.0358	0.0079 0.0756 0.1713 0.1314 0.0239
15	0.0553 0.1699 0.2885 0.0830 0.0000	0.0276	0.0039 0.0750 0.1818 0.0909 0.0197
16	0.0517 0.1713 0.2868 0.0637 0.0000	0.0239	0.0000 0.0597 0.2071 0.1075 0.0239

Based on the above two points, some information of the secret key, $\{Xkey(i)\}_{i=0}^{3}$, can be obtained with the following steps:

1. Obtain $\mathbf{I}_{key}$ via

$$\mathbf{I}_{key} = \mathrm{VD}(\mathrm{HD}(\mathbf{I})) \oplus \mathbf{I}';$$

2. Search the value of $\{Xkey(i)\}_{i=0}^{3}$, and get the corresponding version of $\mathbf{I}^*_{Xkey}$;
3. Generate estimated version of $\{CKSB(i, j)\}_{\substack{0\le i\le M-1\\ 0\le j\le N-1}}$, $\{CKSB^*(i, j)\}_{\substack{0\le i\le M-1\\ 0\le j\le N-1}}$, from the blue channel of $\mathbf{I}^*_{CKS} = \mathbf{I}_{key} \oplus \mathbf{I}^*_{Xkey}$ (See Eq. (3)).
4. Calculate the distribution of $\{\Delta_k\}_{k=0}^{MN-2}$, and output the search value if the distribution match with the expected one (Refer to Table 1).

Once $\{Xkey(i)\}_{i=0}^{3}$ are determined, one can obtain $K = Xkey(2) \mod 256$, $L = Xkey(3) + n \cdot 256$, $n = 1 \sim 4$, $x_0 \in [Xkey(0)/256 \cdot (2\pi), (Xkey(0) + 1)/256 \cdot (2\pi))$, $y_0 \in [Xkey(1)/256 \cdot (2\pi), (Xkey(1) + 1)/256 \cdot (2\pi))$.

Obviously, the complexity of the whole attack is $O(2^{4\cdot 8} \cdot L)$, where L is the number of plain-bytes to be calculated. Considering $L = 256$ is enough for counting the distribution of $\{\Delta_k\}_{k=0}^{MN-2}$, the complexity of the attack is $O(2^{40})$. Note that the complexity of the attack can be reduced much by dividing the attack into the following two stages: (1) search for the possible values of $\{Xkey(i)\}_{i=0}^{3}$ of regular interval with a weaker matching condition; and (2) verify the left possible values of $\{Xkey(i)\}_{i=0}^{3}$ with a stronger matching condition. In our experiments, only the even possible values of $\{Xkey(i)\}_{i=0}^{3}$ are searched, and the matching condition is set as

$$\#\left(\{k \mid |\Delta_k| < 1/16\}\right) > (MN/2),$$

where $\#(\cdot)$ denotes cardinality of a set. In this case, the complexity is reduced to $O(2^{36})$. For a PC with CPU of 2.83GHz and RAM of 2.98GB, the attack can be completed within eleven minutes. A number of experiments were made to verify the correctness of the above attack. With the secret key $(x_0, y_0, K, L) =$ (3.98235562892545, 1.34536356538912, 108.5436 5761256745, 110), the output of the first stage of the attack is {160, 54, 108, 108}, {162, 54, 108, 110}. Then, the 16 possible neighboring values of each set are verified further, and the distributions of Δ_k corresponding for the second set are shown in Table 2. Obviously, the data shown in third row of Table 2 are closed to the data shown in Table 1 most. So, $\{Xkey(i)\}_{i=0}^{3} = \{162, 54, 109, 110\}$. One can further obtain that $K = 109 \mod 256$, $L = 110 + n \cdot 256$,

$n = 1 \sim 3$, $x_0 \in [81/64 \cdot \pi, 163/128 \cdot \pi)$, $y_0 \in [27/64 \cdot \pi, 55/128 \cdot \pi)$.

4 Conclusion

In this paper, the security of a new image encryption scheme based on logistic map is re-analyzed in detail. Although it was reported that equivalent secret key of the encryption scheme can be reconstructed with only one pair of known plaintext and the corresponding ciphertext, this paper further finds that the scope of all the subkeys can be narrowed further with relatively low computation under the same condition. The results reported in this paper will help study security of other image encryption schemes based on logistic map.

Acknowledgments This research was supported by the National Natural Science Foundation of China (No. 61100216, 61491240111) and the Alexander von Humboldt Foundation of Germany.

References

1. Álvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**(8), 2129–2151 (2006)
2. Álvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of a discrete chaotic cryptosystem using external key. Phys. Lett. A **319**(3–4), 334–339 (2003)
3. Arroyo, D., Rhouma, R., Alvarez, G., Li, S., Fernandez, V.: On the security of a new image encryption scheme based on chaotic map lattices. Chaos **18**(3), 033112 (2008)
4. Baptista, M.: Cryptography with chaos. Phys. Lett. A **240**(1–2), 50–54 (1998)
5. Chen, F., Wong, K.W., Liao, X., Xiang, T.: Period distribution of generalized discrete arnold cat map for $N = p^e$. IEEE Trans. Inf. Theory **58**(1), 445–452 (2012)
6. Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals **21**(3), 749–761 (2004)
7. Jakimoski, G., Subbalakshmi, K.: Cryptanalysis of some multimedia encryption schemes. IEEE Trans. Multimed. **10**(3), 330–338 (2008)
8. Kocarev, L., Jakimoski, G.: Logistic map as a block encryption algorithm. Phys. Lett. A **289**(4–5), 199–206 (2001)
9. Li, C., Li, S., Álvarez, G., Chen, G., Lo, K.T.: Cryptanalysis of a chaotic block cipher with external key and its improved version. Chaos Solitons Fractals **37**(1), 299–307 (2008)
10. Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G.: On the security defects of an image encryption scheme. Image. Vis. Comput. **27**(9), 1371–1381 (2009)
11. Li, C., Li, S., Chen, G., Halang, W.A.: Cryptanalysis of an image encryption scheme based on a compound chaotic sequence. Image. Vis. Comput. **27**(8), 1035–1039 (2009)
12. Li, C., Li, S., Lo, K.T.: Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simul. **16**(2), 837–843 (2011)
13. Li, S., Chen, G., Mou, X.: On the dynamical degradation of digital piecewise linear chaotic maps. Int. J. Bifurc. Chaos **15**(10), 3119–3151 (2005)
14. Li, S., Chen, G., Zheng, X.: Chaos-based encryption for digital images and videos. In: B. Furht, D. Kirovski (eds.) Multimedia Security Handbook, chap. 4, pp. 133–167. CRC Press, Boca Raton (2004)
15. Li, S., Li, C., Chen, G., Lo, K.T.: Cryptanalysis of the RCES/RSES image encryption scheme. J. Syst. Softw. **81**(7), 1130–1143 (2008)
16. Oteo, J.A., Ros, J.: Double precision errors in the logistic map: statistical study and dynamical interpretation. Phys. Rev. E **76**(3), 036,214 (2007)
17. Pareek, N., Patidar, V., Sud, K.: Image encryption using chaotic logistic map. Image. Vis. Comput. **24**(9), 926–934 (2006)
18. Patidar, V., Pareek, N., Sud, K.: A new substitution-diffusion based image cipher using chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simul. **14**(7), 3056–3075 (2009)
19. Persohn, K., Povinelli, R.: Analyzing logistic map pseudo-random number generators for periodicity induced by finite precision floating-point representation. Chaos Solitons Fractals **45**(3), 238–245 (2012)
20. Phatak, S.C., Rao, S.S.: Logistic map: a possible random-number generator. Phys. Rev. E **51**(4), 3670C3678 (1995)
21. Rhouma, R., Solak, E., Belghith, S.: Cryptanalysis of a new substitution-diffusion based image cipher. Commun. Nonlinear Sci. Numer. Simul. **15**(7), 1887–1892 (2010)
22. Tong, X., Cui, M.: Image encryption with compound chaotic sequence cipher shifting dynamically. Image. Vis. Comput. **26**(6), 843–850 (2008)
23. Ulam, S.M., von Neumann, J.: On combination of stochastic and deterministic processes. Bull. Am. Math. Soc. **53**(11), 1120 (1947)
24. Zhang, Y., Li, C., Li, Q., Zhang, D., Shu, S.: Breaking a chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **69**(3), 1091–1096 (2012)
25. Zhou, J., Au, O.C.: On the security of chaotic convolutional coder. IEEE Trans. Circuits. Syst. I **58**(3), 595–606 (2011)