Deciphering a novel image cipher based on mixed transformed Logistic maps

Yuansheng Liu, Eric Yong Xie, Ge Cheng, Chengqing Li

MOE (Ministry of Education) Key Laboratory of Intelligent Computing and Information Processing, College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China

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

Abstract

Since John von Neumann suggested utilizing Logistic map as a random number generator in 1947, a great number of encryption schemes based on Logistic map and/or its variants have been proposed. This paper re-evaluates the security of an image cipher based on transformed logistic maps and proves that the image cipher can be deciphered efficiently under the condition of two known plain-images with computation complexity of $O(2^{18} + L)$ or two chosen-plaintexts with computation complexity of $O(L)$. In contract, the required condition in the previous deciphering method is eighty-seven chosen plain-images with computation complexity of $O(2^{7} + L)$. In addition, three other security defects existing in Logistic map based encryption schemes widely are also reported.

Keywords: chaotic image encryption, cryptanalysis, known-plaintext attack, chosen-plaintext attack, Logistic map

1. Introduction

The seemingly similarity between chaos and cryptography promoted their combination to design efficient and secure encryption schemes, where one or more chaotic systems were adopted to determine position permutation relationship, generate pseudo-random number sequence (PRNS), and/or produce cipher-text directly [1, 2, 3, 4, 5, 6]. As an integral part of cryptography, security analysis on a given encryption scheme checks its real capability on achieving balance point between security and the cost computation, and also provides another perspective on studying property of the underlying theory [7]. Some cryptanalytic works have shown that many chaos-based encryption schemes have security problems of different extents from modern cryptographical point of view [8, 9, 10, 11, 12, 13].

Logistic map is one of the most famous chaotic systems. It comes from 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 cryptography can be traced back to John von Neumann’s suggestion on utilizing it as a random number generator in 1947 [14]. The map become very popular after the biologist Robert May used it as a discrete-time demographic model in 1976 [15]. Due to simple form and relatively complex dynamical properties of logistic map, it was extensively used to design encryption schemes or generate PRNS [16, 17, 18, 19]. Even in Web of Science, one can find that more than two hundred papers on application of logistic map in cryptography were published between 1998 and 2013. Among them, a few papers reported some security deficiencies specially caused by Logistic map, such as estimation of control parameter from neighboring states, short period of the states orbit [20, 21, 22]. To tackle the defects, various remedies were proposed, such as modify Logistic map itself [23] or postprocess the raw chaotic states [22].

In [23], a novel image cipher based on mixed transformed logistic maps was proposed, where the modulo addition and the XOR operations are employed in diffusion procedure, which are all controlled by PRNS generated by iterating the mixed transformed Logistic maps (MTLM). Essentially, the image cipher fall in the categories of encryption schemes based on function $y = (\alpha + x) \oplus (\beta + x)$, Extensive cryptographic properties of Eq. (1) have been given in [13]. Recently, Zhang et al. found that the cipher is insecure against chosen-plaintext attack and the equivalent secret key can be obtained by eighty-seven pairs of chosen plain-images [24].

This paper re-evaluates the security of the image cipher proposed in [23], and points out the following main inse-
security points: 1) the cipher can be broken efficiently with two pairs of known plain-images and their corresponding cipher-images; 2) the deciphering complexity can be further decreased under the scenario of chosen-plaintext attack; 3) the image cipher suffer other security defects like insensitivity with respect to change of plain-image/secret key and weak randomness of the used PRNS.

The remaining of the paper is organized as follows. The next section gives a brief introduction of the image cipher under study. Then, the comprehensive cryptanalysis on it are presented in Sec. 3 together with detailed experimental results. Finally, Sec. 4 concludes the paper.

2. The image cipher under study

The plain-image of the image cipher under study is a RGB color image of size $H \times W$ (height × width), which can be represented as an 8-bit integer matrix of size $3 \times L$, $I = \{I(i)\}_{i=1}^L = \{|R(i), G(i), B(i)\}_{i=1}^L$, by scanning the pixels in the raster order, where $L = H \cdot W$. Similarly, the corresponding cipher-image is denoted by $I' = \{I'(i)\}_{i=1}^L = \{|R'(i), G'(i), B'(i)\}_{i=1}^L$. Then, the four main parts of the image cipher under study are described as follows:

- **The secret key** is composed of six odd integers $r_i$, $i=1$ and three control parameters $k_1, k_2, k_3$, initial state $(x_0, y_0, z_0)$ of MTLM proposed in [23], which is given as

$$
\begin{align*}
&x_{i+1} = (3.73 \cdot k_1 \cdot (1 + x_i)^2 \cdot \sin(1/(1 + y_i^2))) \mod 1, \\
y_{i+1} = (3.53 \cdot k_2 \cdot x_{i+1} \cdot \sin(x_{i+1} \cdot y_i) \cdot (1 + z_i^2)) \mod 1, \\
z_{i+1} = (3.83 \cdot k_3 \cdot x_{i+1} \cdot (1 + y_{i+1} \cdot z_i)) \mod 1,
\end{align*}
$$

where $r_i \in [0, 256]$, $|k_1| > 37.7$, $|k_2| > 39.7$ and $|k_3| > 37.2$.

- **Keystream generation procedure**: Iterate the above MTLM $L$ times to obtain a chaotic states sequence $\{(x_i, y_i, z_i)\}_{i=1}^L$. Then, generate keystream as follows: for $i = 1 \sim L$, set

$$
\begin{align*}
X_i &= \lfloor 256 \cdot x_i \rfloor, \\
Y_i &= \lfloor 256 \cdot y_i \rfloor, \\
Z_i &= \lfloor 256 \cdot z_i \rfloor,
\end{align*}
$$

where $\lfloor x \rfloor$ quantizes $x$ to the nearest integers less than or equal to $x$.

- **The encryption procedure** consists of the following three operations.

- **Initial permutation**: For $i = 1 \sim H, j = 1 \sim W$, set

$$
\begin{align*}
R^i((i-1) \cdot W + j) &= R((t_1 - 1) \cdot W + t_2), \\
G^i((i-1) \cdot W + j) &= G((t_1 - 1) \cdot W + t_3), \\
B^i((i-1) \cdot W + j) &= B((t_1 - 1) \cdot W + t_6),
\end{align*}
$$

where

$$
t_a = \begin{cases} 
1 + (31 \cdot i \cdot r_a) \mod H, & \text{if } a \in \{1, 3, 5\}; \\
1 + (31 \cdot j \cdot r_a) \mod W, & \text{otherwise}.
\end{cases}
$$

- **Nonlinear diffusion**: For $i = 1 \sim L$, set

$$
\begin{align*}
R^i(i) &= \left(\left(\left(R^i(i) \ggg 4\right) + X_i\right) \circledast Y_i, \\
G^i(i) &= \left(\left(\left(G^i(i) \ggg 4\right) + X_i\right) \circledast Y_i, \\
B^i(i) &= \left(\left(\left(B^i(i) \ggg 4\right) + X_i\right) \circledast Y_i,
\end{align*}
$$

where $a \ggg 4 = 16 \cdot (a \mod 16) + \lceil p/16 \rceil$.

- **Zigzag diffusion**: 1) re-scan all pixels of $I^i = \{I^i(i)\}_{i=1}^L = \{|R^i(i), G^i(i), B^i(i)\}_{i=1}^L$ in the zigzag order and still store the result with $I^i$; 2) encrypt each element of $I^i$ in order by

$$
\begin{align*}
R^i(i) &= R^i(i) \oplus R'(i - 1) \oplus Z_i, \\
G^i(i) &= G^i(i) \oplus G'(i - 1) \oplus Z_i, \\
B^i(i) &= B^i(i) \oplus B'(i - 1) \oplus Z_i,
\end{align*}
$$

where $R'(0) = G'(0) = B'(0) = 0$.

- **Decryption procedure** is similar to the encryption one except the following points: 1) the above encryption operations are run in a reverse order; 2) Eqs. (2), (3) and (4) are replaced by

$$
\begin{align*}
R((t_1 - 1) \cdot W + t_2) &= R\left((i-1) \cdot W + j\right), \\
G((t_1 - 1) \cdot W + t_3) &= G\left((i-1) \cdot W + j\right), \\
B((t_1 - 1) \cdot W + t_6) &= B\left((i-1) \cdot W + j\right),
\end{align*}
$$

and

$$
\begin{align*}
R^i(i) &= \left(\left(\left(R^i(i) \circledast Y_i\right) - X_i\right) \mod 256 \ggg 4, \\
G^i(i) &= \left(\left(\left(G^i(i) \circledast Y_i\right) - X_i\right) \mod 256 \ggg 4, \\
B^i(i) &= \left(\left(\left(B^i(i) \circledast Y_i\right) - X_i\right) \mod 256 \ggg 4,
\end{align*}
$$

respectively.
3. Cryptanalysis

3.1. Chosen-plaintext attack proposed by Zhang et al.

To make cryptanalysis on the image cipher under study more complete, we first briefly review previous deciphering method proposed by Zhang et al. in [24].

Chosen-plaintext attack is an attack model assuming that the attacker owns right to modify plaintext and observe the corresponding ciphertext. Assume that a plain-image $I_1 = \{(i_1(i))_{i=1}^L\}$ and its corresponding cipher-image $I'_1 = \{(I'_1(i))_{i=1}^L\}$ are available, where $d \in [0, 255]$. For permutation domain of a fixed value, any permutation operation is canceled. According to Eqs. (3) and (4), one has

$$R'_1(i) \oplus R'_1(i-1) = X_i \oplus Y_i \oplus z_i,$$

and

$$G'_1(i) \oplus G'_1(i-1) = ((d \gg 4) + X_i) \oplus Y_i \oplus z_i.$$  

Incorporate $(Y_i \oplus z_i)$ in Eq. (5) into Eq. (6), one further has

$$R'_1(i) \oplus R'_1(i-1) \oplus G'_1(i) \oplus G'_1(i-1) = ((d \gg 4) + X_i) \oplus Y_i.$$  

The above equation can be attributed to a special case of Eq. (1).

$$y = (a + x) \oplus x.$$  

As shown in Table 2 of [13], only the scope of possible values of $X_i$ can be obtained by solving one set of Eq. (7). Given more pairs of chosen plain-images and the corresponding cipher-images, the scope would become more and more narrow, and all the 7 least significant bits of $X_i$ may be confirmed. In [24], Zhang et al. claimed that 256 plain-images of different fixed values can reveal $\{X_i\}_{i=1}^L$. As a RGB color image has three channel components, one can conclude that the chaotic keystream $\{X_i\}_{i=1}^L$ can be reconstructed with [256/3] = 86 pairs of chosen plain-images. According to Eq. (5), the keystream $(Y_i \oplus z_i)_{i=1}^L$ can be obtained. Once the equivalent keys of the two parts Nonlinear diffusion and Zigzag diffusion are recovered, only the Initial permutation is left. One can modify a single pixel value of the previous chosen plain-images to break the encryption.

In all, the essential idea of Zhang et al.’s attack is to narrow the scope of $x$ with different $(y, a)$ by verifying Eq. (1) of $\beta \equiv 0$. As $y \in [0, 255]$, they enumerate all possible values of $\alpha \in [0, 127]$, and then recover $x$ by observing the distribution of $y$. So, the required number of chosen plain-image is eighty-seven and the computation complexity is $O(128 \cdot L)$.

3.2. Known-plaintext attack

The known-plaintext attack is a weaker version of the chosen-plaintext attack as the attacker can not modify the plaintext.

Assume another plain-image $I_2 = \{(I_2(i))_{i=1}^L\} = \{((R_2(i), G_2(i), B_2(i)))_{i=1}^L\}$, and the corresponding cipher-image $I'_2 = \{(I'_2(i))_{i=1}^L\} = \{(R'_2(i), G'_2(i), B'_2(i))_{i=1}^L\}$ are available. According to Eqs. (3) and (4), one has

$$R'_1(i) \oplus R'_1(i-1) \oplus R'_2(i) \oplus R'_2(i-1) = ((R'_1(i) \gg 4) + X_i) \oplus ((R'_2(i) \gg 4) + X_i).$$  

Referring to Proposition 2 in [12], one has

$$(a + (X_i \oplus 128)) = (a + X_i) \oplus 128.$$  

Thus, one can see that $X_i$ is equivalent to $(X_i \oplus 128)$ in terms of existence of Eq. (8). According to Eq. (2), one has

$$R'(i \cdot W) = R(u),$$  

where $u = (((((\cdots r_i) \mod H) \cdot W + 1) \cdot W + 1) \cdots \cdot H)$. Referring to Eq. (9), one further has

$$R'_1(i \cdot W) \oplus R'_1(i \cdot W - 1) \oplus R'_2(i \cdot W) \oplus R'_2(i \cdot W - 1) = ((R_1(u_i) \gg 4) + X_{i\cdot w}) \oplus ((R_2(u_i) \gg 4) + X_{i\cdot w}).$$  

As $r_1$ is an odd integer and $r_1 \in [0, 256]$, there are only 128 possible values. Thus, one can enumerate the value of $r_1$ and then verify $r_1$ by checking whether $X_{i\cdot w} \in [0, 127]$ satisfies Eq. (10) for any $i \in [1, H]$. If all the verifications pass, the search value of $r_1$ is considered as the right sub-key. Apparently, the computation complexity of the search procedure is $O(128 \cdot X \cdot 128) = O(2^{19} \cdot H)$, and the success of this method is determined by the verification of Eq. (10). The probability of $(\alpha, \beta)$ passing verification of Eq. (1) under different values of $y$ are shown in Fig. 1. Assume that the elements of $\{R_1(i \cdot W + 1)\}_{i=1}^H$ and $\{R_2(i \cdot W + 1)\}_{i=1}^H$ follow uniform distribution, one can assure that the probability a wrong version of $r_1$ pass the verification procedure is less than $(1/2)^H$, which means the value of $r_1$ can be successfully recovered with only three times verification in a very extremely high probability. In the same way, we can obtain other five odd integers $(r_1)_{i=2}^{\beta}$. Therefore, the computation complexity of deciphering the Initial permutation is

$$O(6 \times 128 \times 3 \times 128) = O(9 \cdot 2^{15}) \approx O(2^{18}).$$

Once the permutation part has been deciphered, some bits of $\{X_i\}_{i=1}^L$ can be revealed with even one pair of known plain-image and the corresponding cipher-image. Now, Eq. (7) become

$$R'(i) \oplus R'(i-1) \oplus G'(i) \oplus G'(i-1) = ((R'(i) \gg 4) + X_i) \oplus ((G'(i) \gg 4) + X_i).$$
Obviously, the above equation falls in the general form of Eq. (1). In [13, Sec. 3.2], Li et al. proved that $Pr(0) = 0.5$, $Pr(1) = 0.4062$, $Pr(2) = 0.3818$, and $Pr(i) \approx 0.37$ for $i > 3$, where $Pr(i)$ denotes the probability that the $i$-th bit can be confirmed. For each pair of known plain-image and the corresponding cipher-image, there are three equations of the form of Eq. (1). Due to the inherent relations among the three equations, it is very hard to estimate the probability that $\{X_i\}_{i=1}^L$ can be obtained. When two known plain-images are available, one can obtain $\binom{2}{1} = 15$ equations. Therefore, one can assure that most bits of $\{X_i\}_{i=1}^L$ can be obtained with a high probability. It is easy to conclude that the computation complexity on confirming bit of $\{X_i\}_{i=1}^L$ is $O(L)$.

To verify the real performance of the above known-plaintext attack, a great number of experiments were performed with plain-images of size $256 \times 256$ (height \times width). Here, a typical example is shown, where the secret key $\{r_i\}_{i=1}^6 = \{123, 57, 67, 89, 253, 221\}$, $k_1 = 38.583, k_2 = 41.135, k_3 = 39.846$, and $(x_0, y_0, z_0) = (0.485, 0.913, 0.751)$. Two known plain-images "Baboon" and "Street", shown in Fig. 2(a) and Fig. 2(b) respectively, are used to recover $\{r_i\}_{i=1}^6$. The decryption results that the equivalent key of diffusion part $\{X_i\}_{i=1}^L$ and $\{Y_i \oplus Z_i\}_{i=1}^L$ are revealed with one and two known plain-images are shown in Fig. 2(d) and Fig. 2(e) respectively. It is counted that 26.53\% and 83.96\% of the pixels of the images shown in Fig. 2(d) and Fig. 2(e) are correct. Therefore, one can conclude that two known plain-images can achieve a satisfactory deciphering performance.

3.3. Improved chosen-plaintext attack

Based on the above discussion, this subsection presents an improved chosen-plaintext attack based on the following proposition.

**Proposition 1.** Assume that $\alpha, \beta$, and $x$ are all $n$-bit integers, then a lower bound on the number of queries $(\alpha, \beta)$ to solve Eq. (1) in terms of modulo $2^n - 1$ for any $x$ is $1$ if $n = 2$; $2$ if $n > 2$.

**Proof.** See proof in [13, Sec. 3.3].

Corollary 3.1 in [13] listed two typical sets of $(\alpha, \beta)$ to determine $x$ in Eq. (1) when $n = 8$, where with the two queries are $(0, 170)$ and $(170, 85)$. Thus, one can chooses a plain-image $I = \{(R(i) \equiv 0, G(i) \equiv 170, B(i)) \equiv 85\}_{i=1}^L$, and

![Figure 1: The probability of $(\alpha,\beta)$ passing verification of Eq. (1) under different values of $y$.](image1)

![Figure 2: Known-plaintext attack: (a) the known plain-image “Baboon”; (b) the known plain-image “Street”; (c) the cipher-image of a plain-image “Lenna”; (d) the decryption result that the equivalent secret key of diffusion part is reconstructed with the known plain-image “Baboon”; (e) the decryption result of Fig. 2(c) with two known plain-images.](image2)
then one further has

\[
\begin{align*}
R'(i) &\oplus R'(i-1) \oplus G'(i) \oplus G'(i-1) = (0 \oplus X_i) \oplus (170 \oplus X_i), \\
G'(i) &\oplus G'(i-1) \oplus B'(i) \oplus B'(i-1) = (170 \oplus X_i) \oplus (85 \oplus X_i).
\end{align*}
\]

Thus, \([X_i]_{i=1}^{L}\) can be revealed with the above chosen-plaintext attack. Once \([X_i]_{i=1}^{L}\) is recovered, another chosen-plaintext image required to breaking Initial permutation as above. Therefore, the equivalent key of the image cipher under study can be revealed with only two chosen plain-images and the computation complexity of the improved chosen-plaintext attack is only \(O(L)\).

### 3.4. Other security defects

In this subsection, we list three other security defects existing in Logistic map based encryption schemes widely.

- **Low sensitivity with respect to change of secret key:**

  From the cryptographical point of view, a good secure image cipher should be sensitive to the secret key [25]. In [23] Sec. 4.3], the author claimed that the cipher under study has a great sensitivity to the secret key based on some limited test results. Unfortunately, we found that the image cipher under study fails to satisfy this security principle. From the previous analysis, one can see that \([X_i]_{i=1}^{L}\) and \([Y_i \oplus Z_i]_{i=1}^{L}\) are the equivalent key of Nonlinear and Zigzag diffusion parts. When \(Y_i' \oplus Z_i' = Y_i \oplus Z_i\), one has \(Y_i'\) and \(Z_i'\) are equivalent to \(Y_i\) and \(Z_i\), respectively. Moreover, according to Eq. (9), \((X_i, Y_i \oplus Z_i)\) is equivalent to \((X_i \oplus 128, Y_i \oplus Z_i \oplus 128)\) with respect to the encryption/decryption procedure.

- **Low sensitivity to change of plaintext:**

  Another cryptographical property required by a good cipher is the avalanche effect, i.e., the ciphertexts of two plaintexts with a slight change (e.g., only one pixel or bit is modified) should be very dramatically different [25]. However, the image cipher under study is actually far away from the property. From the encryption procedure, there is only zigzag diffusion operation can spread the change to influence cipher-image, and the change of one pixel of plain-image can only influence pixels after the present pixel with the zigzag order. For example, assume \(R'(L-1)\) is permuted from \(R'(i)\). If the value of \(R'(i)\) is modified, there are only three cipher pixels \(R'(L-W-1), R'(L-1)\) and \(R'(L)\) are changed.

- **Insufficient randomness of the keystream:**

In [23] Sec. 2.2], it was claimed that transformed Logistic maps does not have security issues existing in Logistic map. Li at al. [26] has found that the randomness of pseudo-random bit sequences derived from the logistic map is very weak. To further test the randomness of the keystream generated by transformed logistic maps, we tested 100 keystreams of length \(256 \times 256 \times 3 = 196608\) by using the NIST statistical test suite [27]. The 100 keystreams were generated with randomly selected secret keys. For each test, the default significance level 0.01 was adopted. The results are shown in Table 1, from which one can see that the keystream 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 |
|-------------------------------------|-----------------------------|
| Approximate Entropy \((m = 10)\)    | 0                           |
| Block Frequency \((m = 128)\)       | 0                           |
| Cumulative Sums (Forward/Reverse)   | 0/0                         |
| FFT                                 | 100                         |
| Frequency                           | 0                           |
| Longest Run of Ones \((m = 10000)\) | 99                          |
| Non-overlapping Template \((m = 9, B = 000000001)\) | 0                           |
| Random Excursions \((x = 1)\)      | 0                           |
| Rank                                | 99                          |
| Runs                                | 0                           |
| Serial \((m = 16)\)                | 0                           |
| Universal                           | 0                           |

**4. Conclusion**

This paper studied the security of an image cipher based on an variant of Logistic map. Observing its essential structure, we found that the previous deciphering method can be improved in terms of reducing the number of known plain-images from eight-seven to two. Under condition of chosen-plaintext attack, computation complexity of the deciphering method can be even reduced a little. In addition, some other security defects, insensitivity to change of plaintext/secret, weak randomness of used PRNG, were also mentioned.
Acknowledgement

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

References

[1] G. Álvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (08) (2006) 2129–2151.
[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos 8 (06) (1998) 1259–1284.
[3] 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.
[4] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, International Journal of Bifurcation and Chaos 14 (10) (2004) 3613–3624.
[5] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications 285 (1) (2012) 29–37.
[6] H. Liu, X. Wang, A. Kadir, Image encryption using DNA complementary rule and chaotic maps, Applied Soft Computing 12 (5) (2012) 1457–1466.
[7] D. E. Knuth, Deciphering a linear congruential encryption, IEEE Transactions on Information Theory 31 (6) (1985) 49–52.
[8] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of dynamic look-up table based chaotic cryptosystems, Physics Letters A 326 (3) (2004) 211–218.
[9] Y. Chen, X. Liao, K.-W. Wong, Chosen plaintext attack on a cryptosystem with discretized skew tent map, IEEE Transactions on Circuits and Systems II: Express Briefs 53 (7) (2006) 527–529.
[10] E. Solak, C. Çikal, O. T. Yildiz, T. Biyikoglu, Cryptanalysis of fridrich’s chaotic image encryption, International Journal of Bifurcation and Chaos 20 (05) (2010) 1405–1413.
[11] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing 91 (4) (2011) 949–954.
[12] C. Li, Y. Liu, T. Xie, M. Z. Chen, Breaking a novel image encryption scheme based on improved hyperchaotic sequences, Nonlinear Dynamics (2012) 1–7.
[13] C. Li, Y. Liu, L. Y. Zhang, M. Z. Chen, Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation, International Journal of Bifurcation and Chaos 23 (04).
[14] S. M. Ulam, J. von Neumann, On combination of stochastic and deterministic processes, Bletin of the American Mathematical Society 53 (11) (1947) 1120.
[15] R. M. MAY, Simple mathematical-models with very complicated dynamics, Nature 261 (5560) (1976) 459–467.
[16] M. Baptista, Cryptography with chaos, Physics Letters A 240 (1-2) (1998) 50–54.
[17] S. C. Phatak, S. S. Rao, Logistic map: A possible random-number generator, Physical Review E 51 (4) (1995) 3670–3678.
[18] L. Kocarev, G. Jakimoski, Logistic map as a block encryption algorithm, Physics Letters A 289 (4-5) (2001) 199–206.
[19] G. Jakimoski, L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 (2) (2001) 163–169.
[20] 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.
[21] K. Persohn, R. Povinelli, Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation, Chaos Solitons & Fractals 45 (3) (2012) 238–245.
[22] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, K. To, Period extension and randomness enhancement using high-throughput reseeding mixing PRNG, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 20 (2) (2012) 385–389.
[23] J. S. Sam, P. Devaraj, R. S. Bhuvaneswaran, A novel image cipher based on mixed transformed logistic maps, Multimedia Tools and Applications 56 (2) (2012) 315–330.
[24] Y. Zhang, D. Xiao, W. Wen, M. Li, Cryptanalyzing a novel image cipher based on mixed transformed logistic maps, Multimedia Tools and Applications, DOI: 10.1007/s11042-013-1684-5 (2014).
[25] B. Schneider, Applied cryptography: protocols, algorithms, and source code in C, John Wiley & Sons, 2007.
[26] 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.
[27] A. Rukhin, et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22rev1a, available online at http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html (2010).