Optik 124 (2013) 1773–1776

Contents lists available at SciVerse ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Cryptanalysis of an image cryptosystem based on logistic map

Bin Wang[a,b], Xiaopeng Wei[a,b], Qiang Zhang[b,*]

[a] School of Mechanical and Engineering, Dalian University of Technology, Dalian 116024, China
[b] Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian 116622, China

ARTICLE INFO

Article history:
Received 21 December 2011
Accepted 20 May 2012

Keywords:
Chaotic cryptosystem
Image encryption
Logistic map
Cryptanalysis

ABSTRACT

In recent years, the studies of chaos-based image encryption have become an important aspect of the security of image transmission. So far, a large amount of chaotic maps have been used in image encryption with the permutation–diffusion architecture, such as logistic map, cat map, tent map and so on. In this paper, a defect of designing an image cryptosystem based on logistic map is proposed. According to the cryptanalysis of the defect, the initial value of logistic which is used to encrypt plain-image can be deduced by the decreased key space, when the parameter of logistic map is given. Finally, the theoretical analysis and numerical experimental results show that the defect could be used to break the image cryptosystem based on logistic map.

1. Introduction

With the rapid progress of communication network and information technology, the security of information transmission has heightened the need for both research and applications, especially the security of image information transmission. Due to their features of ergodicity, sensitivity to initial conditions and sensitivity to controllable parameters, etc., chaotic maps are potential to be used into information encryption, especially image encryption. Inspired by the similarity between chaotic map and cryptography, a large number of chaos-based image encryption algorithms had been proposed [1–14]. In Ref. [12], the authors firstly proposed a general permutation–diffusion cryptographic chaos-based architecture for image encryption, which was shown as Fig. 1. This architecture included two iterative stages, namely permutation stage and diffusion stage. The former permuted the plain-image but not changed the value of pixel, and the latter changed the value of pixel but not changed the position of pixel. In order to improve the effect of algorithms, the whole permutation–diffusion round would be repeated R rounds.

The permutation–diffusion architecture was inspired from the classic Shannon's paper on cryptography [15]. There are three types of two-dimensional chaotic maps which are widely used in the former stage, namely Standard chaotic map, Cat chaotic map and generalized Baker chaotic map [4,7]. For an $N \times N$ image lattice, the discretized versions denote as the Eqs. (1)–(3), respectively.

$$\begin{cases} x_{i+1} = (x_i + y_i) \bmod N \\ y_{i+1} = (y_i + K \sin \dfrac{2\pi x_{i+1}}{N}) \bmod N \end{cases}, \quad \text{with} \quad K > 0 \tag{1}$$

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y \end{bmatrix} (\mathrm{mod} N) \tag{2}$$

$$\begin{cases} x_{i+1} = \dfrac{N}{n_j}(x_i - N_j) + y_i \bmod \dfrac{N}{n_j} \\ y_{i+1} = \dfrac{k_j}{N}\left(y_i - y_i \bmod \dfrac{N}{n_j}\right) + N_j \end{cases}, \quad \text{with} \quad \begin{cases} n_0 + n_1 + \cdots + n_t = N \\ N_j = n_0 + n_1 + \cdots + n_j \\ 0 \le y_i \le N \\ N_j \le x_i \le N_j + n_{j+1} \\ 0 \le j \le t-1 \\ n_0 = 0 \end{cases} \tag{3}$$

where K, p, q and $n_j = 1,2,\ldots,t-1$ are controllable parameters for permutation stage, N is the width of image, (x_i, y_i) and (x_{i+1}, y_{i+1}) are the ith and the i+1th state of chaotic maps, respectively. Although these three chaotic maps could effectively confuse the position of image pixel in the permutation stage, some parameters which were used in the in the permutation stage may cause a security loophole [4,16].

In the diffusion stage, logistic map and tent map were frequently employed to generate the key stream or subkey for the stream ciphers or block ciphers, and change the value of pixels which had been permuted [7,8,17–19]. They can be denoted as follows Eqs. (4)–(5), respectively:

$$x_{i+1} = \mu x_i (1 - x_i) \tag{4}$$

* Corresponding author.
E-mail address: zhangq@dlu.edu.cn (Q. Zhang).

0030-4026/$ – see front matter © 2012 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2012.06.020

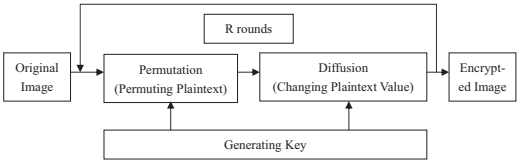

Fig. 1. The Flowchart of permutation–diffusion architecture of chaos-based image cryptosystems.

$$x_{i+1} = \begin{cases} \dfrac{x_i}{\mu}, x_i \in [0, \mu] \\ \dfrac{1-x_i}{1-\mu}, x_i \in [\mu, 1] \end{cases} \quad (5)$$

here, μ is controllable parameter for chaotic maps, x_i and x_{i+1} are the ith and the i+1th state of chaotic maps. Some other chaotic maps could be employed in the diffusion stage, such as Chen's chaotic system, Lorentz chaotic system and others [9,20]. It is well known that a good chaos-based image encryption algorithm should be fast to encrypt image and decrypt image, and sensitive to the cipher key. So a lot of 1-D chaotic maps were used into image encryption, such as logistic map, chebyshev map, cubic map, sine map, Henon map and tent map [2,4,7,13,17,18,21–23], especially logistic map which had been widely used.

The logistic map is not only used in the permutation stage, but also in the diffusion stage. In the permutation stage, researchers obtained the orbit of logistic map by the same parameter and initial value, and permuted the original image by the order from ordering the orbit of logistic map [2,17]; In the diffusion stage, researchers converted the orbit of logistic map to bit stream, and used the bit stream to diffuse the permuted image [4,7,18,21].

This paper focuses on the cryptanalysis of the scheme which is recently proposed by [17]. The defect results from the order of orbit of logistic map which is used to confirm the rough span of initial value of logistic map. It can be employed to decrease key space and obtain the initial value by brute force attack. The defect is proved to be insecure for the image cryptosystem by the theoretical analysis and numerical experimental results.

The paper is organized as follows. In the next section, the conventional cryptanalysis of image encryption is described in detail. In Section 3, the image encryption based on study is briefly described, and theoretical analysis of image encryption is proposed in detail. Performance and simulation results are reported in Section 4. Finally, conclusions are drawn in Section 5.

2. Conventional cryptanalysis of image encryption

The basic concepts related to cryptography and cryptanalysis, such as plaintext, ciphertext, keyspace, etc., and their relationships, can be described in a formal way by using the following mathematical notations [24,25]. A cryptosystem is a five-tuple $(P, C, K, \{e_k : k \in K\}, \{d_k : k \in K\})$, where the following conditions are satisfied.

(1) P is a finite set of all the possible plain texts.
(2) C is a finite set of all the possible ciphertexts.
(3) K is the key space and a finite set of all the possible keys.
(4) For each $k \in K$, there is an encrypting rule $e_k \in \varepsilon$ and a corresponding decrypting rule $d_k \in \phi$. Both $e_k : P \to C$ and $d_k : C \to P$ are functions so that $d_k(e_k(x)) = x$ for every plaintext $x \in P$. ε and ϕ represent the sets of all possible encrypting and decrypting rules, respectively.

The main methods of cryptanalysis of image encryption can be briefly stated as follows [25,26]:

(1) A ciphertext-only attack is one where the adversary (or cryptanalyst) tries to deduce the decryption key or plaintext by only observing ciphertext. The opponent possesses one or more ciphertext, $y_1, y_2, \ldots, y_n \in C$. Any encryption scheme vulnerable to this type of attack is considered to be completely insecure.
(2) A known-plaintext attack is one where the adversary has a quantity of plaintext, $x_1, x_2, \ldots, x_n \in C$ and corresponding ciphertext, $y_1, y_2, \ldots, y_n \in C$. This type of attack is typically only marginally more difficult to mount.
(3) A chosen-plaintext attack is one where the adversary chooses plaintext, $x_1, x_2, \ldots, x_n \in C$ is then given corresponding ciphertext, $y_1, y_2, \ldots, y_n \in C$, when the opponent has obtained temporary access to the encryption machinery. Subsequently, the adversary uses any deduced information in order to recover plaintext corresponding to previously unseen ciphertext.
(4) A chosen-ciphertext attack is one where the adversary selects the ciphertext, $y_1, y_2, \ldots, y_n \in C$ and is then given the corresponding plaintext, $x_1, x_2, \ldots, x_n \in C$, when the opponent has obtained temporary access to the decryption machinery.

There are more details which relate to conventional cryptanalysis of image encryption, the reader is advised to see Refs. [25–27].

3. Analyzing the image encryption algorithm

3.1. The image encryption algorithm

In this paper, *PI* denotes plain-image and *CI* denotes cipher-image with the same size $M \times N$, where M is the height of the plain-image and cipher-image, N is the width of the plain-image and cipher-image. The image *PI* is further represented as a $M \times 8N$ binary matrix *BI*. According to the permutation–diffusion architecture, the encryption scheme proposed in [17] can be described by the following two procedures. Please note that this paper uses different notations from the original ones in [17] to get the simpler and clearer description.

(1) Permutation procedureIn this procedure, the rows of plain-image *BI* are permuted to form an intermediate image *MI* by a matrix $TM = \{tm_1, tm_2, \ldots, tm_M\}$ of size $1 \times M$. *TM* is the position of the order from ordering values $\{x_1, x_2, \ldots, x_M\}$ which are obtained by x_0 after doing iterations in Eq. (4). This is where the defect comes from, namely the order of the orbit of logistic map is used in permutation stage.
(2) Diffusion procedureIn this procedure, each column of *MI* is shuffled to form the *CI* by a matrix $TN = \{tn_{1,j}, tn_{2,j}, \ldots, tn_{M,j}\}^T$ of size $M \times 8N$, where, $1 \le j \le 8 \times N$ which are generated by initial value x_0 after doing iterations in Eq. (4).
(3) DecryptionThe decryption process is similar to that of encryption procedure in the reversed order.There are more details which relate to the proposed image encryption, the reader is advised to see the original paper [17].

3.2. Cryptanalysis

In this part, the property of the order of the orbit is analyzed with a constant parameter of logistic map. It can be used to prove that the defect does not meet the randomicity, and confirm the rough span of initial value of logistic map.

Definition 1. For a orbit of logistic map (1) $x_1, x_2, \ldots, x_n$, if $x_{i+1} > x_i$, $O_i = 1$, and if $x_{i+1} < x_i$, $O_i = 0$.

Lemma 1. *x_i does not exist, where $x_{i+1} < x_i$ and $x_{i+2} < x_{i+1}$, namely $O_{i,i+1} \neq 00$.*