Theoretical Computer Science 552 (2014) 13–25

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Period distribution of generalized discrete Arnold cat map

Fei Chen [a,b,*], Kwok-wo Wong [c], Xiaofeng Liao [d,e], Tao Xiang [e]

[a] Department of Computer Science and Technology, Shenzhen University, China
[b] Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong
[c] Department of Electronic Engineering, City University of Hong Kong, Hong Kong
[d] School of Electronic and Information Engineering, Southwest University, China
[e] College of Computer Science, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Received 26 February 2014
Received in revised form 18 June 2014
Accepted 2 August 2014
Available online 8 August 2014
Communicated by G. Ausiello

Keywords:
Arnold's cat map
Period distribution
Unstable periodic orbit
Encryption

ABSTRACT

The generalized discrete Arnold cat map is adopted in various cryptographic and steganographic applications where chaos is employed. In this paper, we analyze the period distribution of this map. A systematic approach for addressing the general period distribution problem for any integer value of the modulus N is outlined, followed by a complete analysis for the case of prime N. The analysis is based on similar techniques studying linear feedback shift register (LFSR) sequences. Together with our previous results when N is a power of a prime [1,2], the period distribution of the cat map is characterized nearly completely for any integer N. Our results are also useful for evaluating the security of the cryptographic and steganographic algorithms based on the cat map as well as computing all unstable periodic orbits of the chaotic Arnold cat map.

1. Introduction

In recent years, there is a tremendous work of utilizing chaotic systems or chaotic maps in various applications related to communication [3–9], cryptography [10–16] and watermarking [17–21]. One of the widely-used chaotic maps is the Arnold cat map which was firstly studied by the French Mathematician V.I. Arnold [22]. The original form of this map is

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \bmod 1 \tag{1}$$

where $x(n), y(n) \in [0, 1]$. It can be discretized as

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \bmod N \tag{2}$$

and be extended to a more general form [12]

$$\begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} \bmod N \tag{3}$$

where $x(n), y(n), p, q \in \{0, 1, \cdots, N-1\}$.

* Corresponding author at: Department of Computer Science and Technology, Shenzhen University, China.
E-mail addresses: feichenn@gmail.com (F. Chen), itkwwong@cityu.edu.hk (K.-w. Wong), xfliao@cqu.edu.cn (X. Liao), txiang@cqu.edu.cn (T. Xiang).

http://dx.doi.org/10.1016/j.tcs.2014.08.002
0304-3975/

The discretization of the cat map leads to the consequence that the mapping must have a finite period. This may turn out to be a problem or a weakness in critical applications such as cryptography and watermarking. In this paper, the generalized discrete cat map is analyzed mathematically to derive full knowledge on its period distribution when p and q traverse all elements of $\mathbb{Z}_N$. For the simplicity of presentation, the generalized discrete cat map is referred to as cat map in the remaining part of this paper if there is no confusion.

1.1. Motivation

The investigation on the period distribution of the cat map is significant in both theory and application. Chaotic systems are sensitive to initial conditions and the observation of a particular orbit provides only little information. However, the full knowledge of an unstable periodic orbit can be revealed by theoretical analysis and is useful in the study of chaotic motions. If a rational initial point $(\frac{x_0}{N}, \frac{y_0}{N})$ leads to a periodic orbit of the cat map defined by (1), it is easy to verify that (x_0, y_0) is a periodic point of the generalized discrete cat map governed by (2) and vice versa. Thus the study on the period properties of cat map contributes to chaos theory.

The cat map is adopted in many cryptographic and steganographic applications. In chaos-based image cryptosystems [11–14], this map is usually employed to perform pseudo-random permutations on the image pixels. The permuted image will have no difference with the un-permuted one if the permutation orbit has a length exactly equal to an integer multiple of the period of the cat map [12].

In chaos-based public-key cryptography, the cat map can be used to model existing public-key algorithms proposed in [15] and [16]. In [15], iterating the Chebyshev polynomial can be considered as the multiplication of matrices having the Chebyshev recurrent relationship. In [16], the commutative linear functions can be formulated as matrix multiplication. The modeling helps reveal the properties of the proposed algorithms in depth. The public-key algorithms are insecure if the period of the underlying map is not large enough.

Lou and Sung proposed an asymmetric steganographic scheme [17] that embeds a watermark in a digital image according to a stego-matrix constructed by the cat map. In [18], the cat map is utilized to determine the position in the host image where the watermark is embedded. These schemes are vulnerable upon attacks if the watermark embedding position is recoverable due to the improper choice of cat map parameters or orbits.

All these applications highlight the importance of the period properties of the cat map on the security performance of cryptographic and steganographic applications. The knowledge on the period distribution of this map helps in system design and analysis.

1.2. Literature review

The period distribution of the cat map has been partially analyzed using various methods such as matrix theory approach [23], graph theory approach [24] and some other special approaches [25,26]. Some typical results are reviewed here. Percival and Vivaldi [25] investigated the period distribution of the map (2) by the algebraic number theory. The possible periods for some specific values of N were derived. However, their work focused on the simple cat map (2) and only a few period problems were addressed.

As the exact period distribution of the cat map cannot be found using the number-theoretic method adopted in [25], Keating derived an approximation solution for the cat map with prime N by combining number theory and probability theory [26]. The asymptotic behavior of the period distribution when N tends to infinity has also been investigated. However, those results are not exact solutions to the period distribution problem. They are close to the exact values only when N approaches infinity.

Dyson and Falk [27] tackled the period problem using the Fibonacci sequence approach and reduced it to finding the period of the Fibonacci sequence modulo N. Some general period properties were obtained when N is an arbitrary integer, with the lower and upper bounds of the period derived. In particular, the maximum period m_N of (2) for a given N is governed by

$$\begin{aligned} &m_N = 3N, \quad N = 2 \times 5^k,\ k = 1, 2, \cdots, \\ &m_N = 2N, \quad N = 5^k \text{ or } N = 6 \times 5^k,\ k = 1, 2, \cdots, \\ &m_N \le \frac{12}{7} N, \quad \text{for all other } N. \end{aligned}$$

Like [25], these results are valid only for the simple cat map (2) and it is hard to extend the analysis to the generalized cat map (3).

Chen et al. [12] presented an example illustrating the periodic property of the generalized cat map (3). They showed that the period is five when the parameters are chosen as $p = 40$ and $q = 8$.

Besides the aforementioned work, there are many other studies on this topic. However, only partial or asymptotic results are obtained, but not the exact solutions. Despite the work of previous studies, there are still many unsolved problems such as the number of possible periods and their exact values, whether there are cat maps possessing a given period, and the corresponding number of maps, if any, etc. All these problems can only be solved by studying the exact period distribution.