Signal Processing 153 (2018) 231–242

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Some properties of the Logistic map over the finite field and its application

Bo Yang, Xiaofeng Liao*

Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China

ARTICLE INFO

Article history:
Received 15 May 2018
Revised 5 July 2018
Accepted 12 July 2018

Keywords:
Encryption
Chaos
Logistic map
Key stream generator
Finite field

ABSTRACT

The Logistic map is a classical chaotic system and has been used as a chaotic cipher in the real number field. This inevitably leads to the degradation of finite precision under the computer environment, and it also is very difficult to guarantee the security of the cryptosystem using the Logistic map over the real number field. To overcome these drawbacks, in this paper, we extend the Logistic map-3 to the finite field $\mathbf{Z}_{3^n}$, and give theoretical analysis about some period properties of the Logistic map-3 over $\mathbf{Z}_{3^n}$. Moreover, we discuss the control parameters which can change the behavior of the mapping, and also find that the maximum period can change with the control parameter. Furthermore, we analyze some characteristics including maximum period, generation time, NIST test, power spectrum, correlation property, phase diagram and Lyapunov exponent. Simulation results show that the period of Logistic map-3 over $\mathbf{Z}_{3^n}$ is longer than Logistic map-1 over $\mathbf{Z}_{3^n}$, and much longer than Logistic map-1 over $\mathbf{Z}_{2^n}$, and the same as Logistic map-2 over $\mathbf{Z}_{3^n}$. Simulation experiments also show that the Logistic map-3 over the finite field has some good features including non-periodic, random, noise-like properties, continuous spectrum, good correlation, well uniform distribution, controllable length of generated sequence, positive Lyapunov exponent, and good sequence generation speed. Therefore, we attempt to design a nonlinear transformation based key stream generator by using the Logistic map-3 over $\mathbf{Z}_{3^n}$ and apply to image encryption. The performance analyses including statistical analysis, Shannon entropy analysis, differential attack analysis, and speed analysis also show that our proposed method may be suitable for practical cryptographic application.

© 2018 Published by Elsevier B.V.

1. Introduction

In real-world, the non-linear phenomena is much more general than the linear phenomena. Chaos can be usually found in a deterministic system and it is a type of random-like behavior. In 80s and 90s twentieth century, researchers concentrated on how to lead to chaos, properties of chaos, and applications of chaos [1,2]. Chaotic maps have a number of significant and well characteristics which include randomness, sensitive to the initial value, the continuous power spectrum, unpredictable, etc. Hence, there are a large number of trials to discuss the dynamic behavior of the generalizing chaotic mapping in chaotic cryptography [3–13]. However, in practical application the state space of a chaotic system may be discrete because of the limited computation, memory and communication capabilities [14]. How to select chaotic mapping which satisfies the requirements of the cryptographic properties is a very important problem to be solved.

Kocarev proposed some guiding methods, i.e., the selected chaotic map must at least satisfy with mixing property, robust and large parameter set [14]. There are a lot of discrete chaotic maps such as Logistic map [15], Henon map [16], Arnold map [17], etc. Three traditional Logistic maps in the real domain are defined as Logistic map-1, $f_{1R}(x) = \mu x(1-x)$, Logistic map-2, $f_{2R}(x) = 1 - \mu x^2$, and Logistic map-3, $f_{3R}(x) = \mu - x^2$, respectively, where μ is the control parameter of map and x is a real number. However, the traditional chaotic map over the real domain has a disadvantage that the calculation accuracy of the floating point number can be doubled to increase when implementing the map by computer. And, this will lead to a serious drawback for practical application. In order to overcome the above problem, a large number of researchers have generalized chaotic maps to the finite field [5,18–22]. Determining length is considerably significant in actual engineering applications such as sequence generator and cryptography. A lot of researches have proven that the Logistic mapping

* Corresponding author.
E-mail address: xfliao@swu.edu.cn (X. Liao).

https://doi.org/10.1016/j.sigpro.2018.07.011
0165-1684/© 2018 Published by Elsevier B.V.

over the finite field can generate long sequences [23–26,29]. For the security of the cryptosystem, long period of password in a limited number domain can guarantee that it is very difficult to be attacked, while the traditional Logistic map is bounded to degenerate result in period property which is detrimental to the security of the resulting password system. While the Logistic map over integers is based on a rounding, and the Logistic map over the prime field is based on remainder. In addition, the values of variant maps are integers. However, there exist some drawbacks in conventional methods, such as finite precision, restricted complexity, finite randomness, and so on. These defects are detrimental to the security of the password system.

In [27], to overcome these drawbacks, the authors discussed some maximum periodic properties of generation sequences from the Logistic map-1 $f_{1R}(x) = \mu x(1-x)$ over the finite field $\mathbf{Z}_{2^n}$, and gave some but not comprehensive theoretical proof, and inferred the control parameter of the Logistic map would affect the values of the map.

The above three Logistic maps over the real field have similar characteristics, while the especial and complex properties of the Logistic maps over the finite field are not involved and still worthy of further study. In [28], the authors discussed the Logistic map-1 $f_{1R}(x) = \mu x(1-x)$ over the finite field $\mathbf{Z}_{3^n}$ and analyzed period properties of generation sequences from the Logistic map-1 over $\mathbf{Z}_{3^n}$. In [30], the authors analyzed the Logistic map-2 $f_{2R}(x) = 1-\mu x^2$ over the finite field $\mathbf{Z}_{3^n}$ and provided some characteristics of Logistic map-2 over $\mathbf{Z}_{3^n}$. In this paper, we will generate the Logistic map-3 $f_{3R}(x) = \mu - x^2$ to the finite field $\mathbf{Z}_{3^n}$. The Logistic mapping ranges from 0 to $3^n - 1$ by performing this expansion. Furthermore, we will derive the efficiently computational form of the Logistic map-3 over $\mathbf{Z}_{3^n}$, and analyze the period properties of generation sequences from Logistic map-3 when the sequence value takes all values over $\mathbf{Z}_{3^n}$ by theoretical analysis with the dynatomic polynomial arithmetic theory in detail. The maximum period of generation sequences from this map could be affected according to different control parameters. In addition, some examples are provided to demonstrate the effectiveness and correctness about our analysis. The analysis of characteristics about the Logistic map-3 over the finite field will be presented. The length of generation sequences from the Logistic map-3 over $\mathbf{Z}_{3^n}$ in this paper is much longer than that of the Logistic map-3 over the integer field, and also much longer than that of the Logistic map-1 over $\mathbf{Z}_{3^n}$, and the same as that of the Logistic map-2 over $\mathbf{Z}_{3^n}$. And the generation time of Logistic map-3 over $\mathbf{Z}_{3^n}$ is faster than that of Logistic map-1 over $\mathbf{Z}_{3^n}$, and also faster than that of Logistic map-2 over $\mathbf{Z}_{3^n}$. The length of these sequences is much longer which is available for the pseudorandom number generation, the chaotic encryption, etc. The Logistic map over the finite field has other some good characteristics such as non-periodic, random, noise-like properties, continuous spectrum, good correlation, well uniform distribution, controllable length of generated sequence, positive Lyapunov exponent and good sequence generation speed.

It is well-known that the chaotic stream cipher which has become an important branch of cryptography has been studied for decades. The security of a stream cipher system mainly depends on the unpredictability of the key stream, so how to design the high quality key stream generator is a very important issue. Usually, the main factors that affect the security of a stream cipher system are key space size, stream period, linear complexity of stream, etc [31]. So we attempt to design a nonlinear transformation based key stream generator by using the Logistic map-3 that its period is expanded effectively to the finite field $\mathbf{Z}_{3^n}$. At last, we will design an image encryption using this key stream generator, and apply to image encryption. In terms of a cryptographic system, the security and efficiency are two important factors. Many image encryption systems have been analyzed [32–38]. So we will carry out the performance analysis including statistical analysis, Shannon entropy analysis, differential attack analysis, and speed analysis.

The remaining part of this paper is organized as follows. Section 2 includes a few preliminaries which are fundamental for comprehension of our analysis. Period properties of Logistic map-3 over the finite field $\mathbf{Z}_{3^n}$ will be presented in Section 3. Some characteristics about maximum period, generation time, NIST test, power spectrum, correlation property, phase diagram and Lyapunov exponent will be presented in Section 4. Applications includes the key stream generator, image encryption, and performance analysis will be described in Section 5. Finally, conclusions will be drawn in Section 6.

2. Preliminaries

In this section, we first derive some forms of the Logistic map over the real domain, integer, and finite field respectively. Then, we will present some arithmetic methods about dynatomic polynomials which play an important role in analyzing the period property of sequences generated by polynomials. These methods are also useful in the analysis of chaotic cipher.

2.1. Logistic maps and their variants

The Logistic map-3 over the real domain can be defined as

$$f_{3R}(x_i) = \mu - x_i^2, \tag{1}$$

where $x_i \in [-\mu, \mu]$ is a real number for all $i = 1, 2, 3\cdots$, and $\mu \in [0, 2]$ is a control parameter. It is well known that for $\mu = 2$, this Logistic map enters into chaos.

To solve the calculation accuracy problem of floating point number, we can derive this Logistic map over integers from Eq. (1) as

$$f_{3R}^{(n)}(x_i') = 2^n\mu - (x_i')^2/2^n, \tag{2}$$

where n is the precision for elements of this Logistic map, $x_i' = 2^n x_i$, and $f_{3R}^{(n)}(x_i') = 2^n f_{3R}(x_i)$.

By Eq. (2), we can define a function for this Logistic map over integer field as

$$f_{3Int}^{(n)}(X_i) = \lfloor 2^n\mu - X_i^2/2^n \rfloor, \tag{3}$$

where $X_i \in [0, 2^n]$ is the integer part of x_i', and $\lfloor\cdot\rfloor$ is the floor function.

According to Eq. (3) and mod function, this Logistic map over the prime field is defined as follows:

$$f_{3\mathbf{Z}_p}(X_i) = (p-1)\mu - \frac{X_i^2}{p-1} \pmod p, \tag{4}$$

where p is an odd prime, $\mathbf{Z}_p$ is a prime field modulo p, $X_i \in [0, p-1]$ is an element in $\mathbf{Z}_p$, and $\mu_p \in [0, p-1]$ is a control parameter.

Definition 1. We define N as a modulo and $N = q^n$, where q is a small prime and n is a natural number, and by Eq. (4), we get that the Logistic map-3 over $\mathbf{Z}_N$ can be written by

$$X_{i+1} = f_{3\mathbf{Z}_N}(X_i) = (N-1)\mu_N - \frac{X_i^2}{N-1} \pmod N, \tag{5}$$

where $\mu_N \in [0, N-1]$ is the control parameter of the map, and $X_i \in [0, N-1]$.

According to above Definition, we get the below lemma.

Lemma 1.

$$X_{i+1} = f_{3\mathbf{Z}_N}(X_i) = X_i^2 - \mu_N \pmod N. \tag{6}$$

Proof. By using Eq. (5), and because $N - 1 \equiv -1 (\mathrm{mod}\ N)$,

$$X_{i+1} = (N-1)\mu_N - \frac{X_i^2}{N-1} \pmod N,$$

Download English Version:

https://daneshyari.com/en/article/6956989

Download Persian Version:

https://daneshyari.com/article/6956989

Daneshyari.com