A New Study in Encryption Based on Fractional Order Chaotic System

Ming Yin and Li-Wei Wang

Abstract—In this paper, we introduce a novel approach to achieve the data encryption. The fractional order Lorenz chaotic system is used to generate the chaotic sequence and the characteristics of the chaotic sequence are studied. Some examples concerned with text and image encryption are also presented in the paper, which show exciting results by the approach we introduced.

Index Terms—Chaotic system, fractional order chaos, image encryption,

1. Introduction

A large number of studies have been focused on the encryption and the relative areas these years[1]-[4]. The main aim of cryptography is to ensure security by changing messages unavailable to anyone else except for the legal receiver. Encryption is also defined as the science of using mathematics to encrypt and decrypt the data, such as the text mode message and the image. It allows us to store sensitive information or transmit it across insecure channel, so that it cannot be achieved by anyone else.

To encrypt a plain text message, the sender applies an encryption algorithm. Similarly, to decrypt the received encrypted message, the receiver uses the decryption algorithm. Both sender and receiver must agree on a common algorithm. The most important thing about the encryption is to find a reliable approach to accomplish the encryption in sender and it must be safe enough to resist any attack. A safe key is used during the encryption and decryption process. To achieve the secret key, the chaos and chaotic sequence, such as Logistic map and Henon map, are introduced in the field of the encryption[4]-[7]. Chaotic systems have been testified very suitable for data message encryption, the main reasons are:
1) Chaotic systems have the ergodicity in the trajectory;
2) They are extremely sensitive to their initial conditions;
3) They are wideband, pseudo-random, and unpredictable.

In this paper, the fractional order Lorenz system will be introduced and also used to generate the chaotic sequence to accomplish the encryption on text and image.

2. The Approach to Generate Chaotic Sequence

2.1 Fractional Order Derivatives and Its Approximation

The definition of the fractional order derivatives have been introduced by different authors. In this paper, we use the well known Riemann-Liouville definition[7] to handle the chaotic function.

\[
\frac{d^n f}{d^\alpha t} = \frac{1}{\Gamma(n-\alpha)} \int_{0}^{t} (t-\tau)^{n-\alpha-1} \frac{d^n f(\tau)}{d\tau^n} d\tau
\]

where \(n-1 \leq \alpha < n\) and \(\Gamma(i)\) is the gamma function.

Now it is easy to establish a fractional order differential equation. However, it is difficult to get an analytic solution from the fractional order differential equation, even we could not get a numerical solution at all.

Fortunately, in [8], a general method to solve the fractional order differential has been introduced which approximate the fractional order operators by using the standard integer order operators. In Table 1 of [8], the authors introduced the approximations for \(F(s) = 1/s^n\), with \(\alpha = 0.1-0.9\) in steps 0.1 and errors of approximate 2 dB. We can use the following equations to calculate the fractional order differential equation.

\[
L\left\{\frac{d^n f(t)}{d^\alpha t}\right\} = s^n L\{f(t)\}
\]

where

\[
\frac{1}{s^{0.9}} = \frac{c_1 s^2 + c_2 s + c_3}{s^3 + c_4 s^2 + c_5 s + c_6}
\]

where \(c_1 = 1.766, \ c_2 = 38.27, \ c_3 = 4.914, \ c_4 = 36.15, \ c_5 = 7.789, \ \text{and} \ c_6 = 0.01\)

2.2 Normal Lorenz System and Fractional Order Lorenz System

The normal Lorenz system can be described by

\[
\begin{align*}
\frac{dx}{dt} &= a(y - x) \\
\frac{dy}{dt} &= -xz + bx - y, \ a, b, c > 0 \\
\frac{dz}{dt} &= xy - bz
\end{align*}
\]
where \(a=10.0\), \(b=28.0\), and \(c=8/3\). Under the initial condition \((1.0, 1.0, 1.0)\), the chaotic can be observed in Fig. 1.

\[
\begin{align*}
\frac{d\alpha x}{dt} &= a(y-x) \\
\frac{d\alpha y}{dt} &= -xz + bx - y, a, b, c > 0. \\
\frac{d\alpha z}{dt} &= xy - bz
\end{align*}
\]

where \(a, b, c\) are the parameter of the Lorenz system. Regarding (2) and (3), we change the system (5) into

\[
\begin{align*}
X(s) &= \frac{1}{s^{\alpha}}a(y-x) \\
Y(s) &= \frac{1}{s^{\alpha}}(-xz + bx - y), a, b, c > 0. \\
Z(s) &= \frac{1}{s^{\alpha}}(xy - bz)
\end{align*}
\]

It is clear that the fractional order differential equation turns to continue time-domain differential equation. Now, we can obtain the time-domain solution to the system (6), as shown in Fig. 2.

3. Encryption Algorithms and Experimental Results

3.1 Logistic Map

Logistic map is a rather simple chaotic map, which is defined as

\[
x(n+1) = \mu x_n (1-x_n), \quad 0 < x_n < 1, \quad 0 < \mu \leq 4.
\]

Choosing \(\mu = 4\), we can achieve the time-domain figure (see Fig. 3) and the histogram of the Logistic.

\[
\begin{aligned}
X_n \sim \text{Histrogram of Logistic map}
\end{aligned}
\]

Form Fig. 4, we can see that the statistical properties of logistic map provide with ergodic and symmetric properties which satisfy the application in encryption. Compared with the Logistic map, the fractional order Lorenz system also has a suitable trajectory space for the cryptography.

\[
\begin{aligned}
\text{Histogram of the logistic map}
\end{aligned}
\]

The probability density distribution function of the chaotic system output is rather difficult to achieve a clearly analytic expression. Fig. 5 shows one dimension probability distribution of the function. The data of the Lorenz system demonstrate better Gauss white noise properties.

According to Fig. 6, the cross correlation of the Lorenz chaotic system is almost equal to zero, and the cross correlation of logistic map strongly is concerned with the time-domain data. We can draw a conclusion that the data of the fractional order Lorenz system has better statistical properties.
3.2 Simulation Result

The approaches of encryption by the key have been studied in [4]-[8]. Some papers introduce the unique approach to accomplish the encryption, and some papers focus on the process of the encryption. To stress the advantages in encryption by our approach, we choose a simple way of using the key to encrypt the plain text. We perform a simple convolution operator, the steps are as follows:

Step 1: Find \( s(n) \).

Step 2: Find the encryption key from the fractional order Lorenz system.

\[
m(n), \quad n = 0, 1, 2, \ldots, N, \quad N = 2^k
\]

where \( N = 256 \) and \( m(n) \) is provided by chaotic output \( x, y, z \).

Step 3: Perform convolution operator, then

\[
y(n) = x(n) * s(n).
\]

Considering a plain text with the words “hello, world”, the ASCII code are \( s(n) = [104, 101, 108, 108, 111, 32, 119, 111, 114, 108, 100, 33] \), then \( y(n) \) can be represent as a filter output of the \( x(n) \), as shown in Fig. 7. We can certainly use the de-convolution to restore the plain text, the results are shown in Fig. 8.

We also carry out a simulation of the image encryption. The simulation results of the image encryption and de-encryption are provided in Fig. 9. The plain image Lena of size \( 512 \times 512 \) and 256 gray levels is employed, as shown in Fig. 9. It should be denoted that the cryptographic algorithms we used in Fig. 9 are rather simple. The plain image performs linear shift operation based on the chaotic key, and finally the XOR operation is executed between the plain image and the secret key image. We can achieve better results if we choose the more complicated plain image perturb algorithm.
4. Conclusion

In this article, a novel approach concerned with encryption is introduced. The secret key generation ways based on fractional order chaotic Lorenz system are used to achieve the chaotic sequence. The ergodic property and high sensitivity to the initial conditions make the sequence naturally meet the requirement of the data encryption. Through the simulation, we testify that the used fractional order Lorenz chaotic is a valuable approach in cryptographic.

Acknowledgement

The authors are grateful for the support by the General Science Research Project of Southwest University for Nationalities of China under Grant No. 234782.

References


Ming Yin was born in Neimongol Province, China, in 1977. She received the B.S. degree from Ningxia University in Communication Engineering, Ningxia, in 2000 and the M.S. degree from the University of Coventry in Communication Management, U.K., in 2006. She is now an associate professor of the Southwest University for Nationalities of China (SWUN). Her research interests include chaotic communication and communication system design.

Li-Wei Wang was born in Ningxia Province, China, in 1980. He received the B.S. degree from Ningxia University in Communication Engineering, Ningxia, in 2000 and the M.S. degree from the University of Beijing Jiaotong University in Circuit and System, in 2005. He is now an associate professor with the SWUN. His research interests include chaotic communication and image process.