Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **5**, September **2017**

The Method of Obtaining Best Unary Polynomial for the Chaotic Sequence of Image Encryption

Meng Yu[1],Zhifan Du[2],Xin Liu[2],Ding Qun[2] and Hong Chen[2*]

[1]College of Economics and Business Administration
Heilongjiang University
No.74, Xuefu Raod, Nangang District, Harbin, 150080,P.R.China
my100dreams@126.com
[2]College of Electronic Engineering
Heilongjiang University
No.74, Xuefu Raod, Nangang District, Harbin, 150080,P.R.China
*Corresponding author: hbjingjie@126.com

Received February , 2017; revised June, 2017

Abstract. *In order to get a better chaotic sequence which not only is safer for image encryption but also avoids the complex hardware structure of producing the chaotic sequence, a new method of obtaining a best unary polynomial (for shot BUP) has been studied out in this paper. BUP can make a chaotic sequence more complicated and more suited for encrypting image. Based on Chua's system, the working principle and process of obtaining a BUP are given, and the characteristics of the chaotic sequence transformed by the BUP are analyzed. Then the experiments that an image is encrypted by the sequence before and after the BUP transformation are conducted. The results of experiments demonstrate that the sequence transformed by the BUP not only has better characteristics and greater security but also enlarges the key space of image encryption.*
Keywords: Best unary polynomial, Transformation, Chaotic sequence, Image encryption

1. **Introduction.** Since chaos is sensitive to parameters and initial values and owns good randomness, it is very applicable for the image encryption. People have researched a lot of chaotic systems [1-3] and chaos encryption methods [4-6]. With the improvement of the deciphering techniques and the difficulties of finding out a new chaotic system, it is urgent to research some new methods which can make existing chaotic systems produce better characteristics and more kinds of the chaotic sequences for image encryption. Due to the sensitivity of chaos and very short cycle windows in the chaotic area, the chaotic sequence may be easy in a degradation state or weak chaotic state, influences encryption effect, even cannot encrypt image. In order to make chaos stronger and avoid degeneration, [7] puts forward a new method of unary polynomial transformation (UPT) chaos for chaotic image encryption, which is not only very easy to realize but also can greatly improve chaos characteristics without changing the original chaotic system. Although it has proved the effectiveness of UPT from many ways, it only chooses a simple unary polynomial $x^2 + x^3$ among a variety of unary polynomials for researching on the effect of UPT image encryption, and has not researched which the unary polynomials used for transforming chaos can be more suitable for encryption. Since UPT can not only improve chaos characteristics and make encryption safer, but also under different limit conditions, there are the different unary polynomials which can produce many different

kinds of chaotic sequences with better characteristics, it is necessary to be further studied which kind of unary polynomials would be the best for making chaos more complex and safer for encryption. In order to make the chaos more complex and hardware circuit structure relatively simple, a method of getting a best unary polynomial (for shot BUP) is proposed in this paper. Since Lyapunov Exponent (LE) is an important index to quantitatively measure the complexity of chaos, the maximum Lyapunov Exponent [8] is used to study and determine a BUP by the simulation experiment. Firstly, Chapter two in this paper presents the principle and process of obtaining a BUP in detail. Then chapter three analyzes the characteristics of chaotic sequence transformed by the BUP. Furthermore image encryption and decryption experiments are conducted by the chaotic sequence before and after BUP transformation in chapter four. Finally, conclusions are given in chapter five.

2. **Principle of Obtaining a BUP.** Since Chua's system is a typical chaotic system [9], it is chosen as the chaotic signal source to produce the chaotic sequence for experiments. Its state equation is normalized into:

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} -\alpha \\ 0 \\ 0 \end{bmatrix} h(x) \tag{1}$$

Where $h(x) = m_1 x + \frac{1}{2}(m_0 - m_1)(|x+1| - |x-1|)$. A number of experiments have showed that when (1) satisfies

$$\alpha = 10,\ \beta = 14.87,\ m_0 = -0.27,\ m_1 = 0.32,\ x(0) = 0.2,\ y(0) = 0.2,\ z(0) = 0.2 \tag{2}$$

Chua's system is in chaos. We choose its x as the output terminal of a chaotic sequence to study the validity of proposed method in the paper.

Lyapunov Exponent (LE) is an important index to quantitatively measure the complexity of chaos. When LE is positive, it indicates that system is in chaos. The bigger LE is, the more complex chaos is. Since the main purpose of using the BUP to transform chaotic sequence is to increase the complexity of chaotic sequence, we use Lyapunov Exponent experiment to find out the BUP, and its process is shown below.

The maximum LE is:

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln \frac{d_i}{d_0} \tag{3}$$

Where d_i is Euclidean distance between points in chaotic system; d_0 is Euclidean distance between initial value points in chaotic system. In Matlab simulation environment, ode45 is used to numerically solve Chua's system (1). In order to consider the influence of simulation integral interval τ, (3) is rewritten as follows:

$$LE = \lim_{n\to\infty} \frac{1}{n\tau} \sum_{i=1}^{n} \log(\frac{d_i}{d_0}) \tag{4}$$

The chaos will be more complex after being transformed by an appropriate unary polynomial. Therefore, the following will study how to get a best unary polynomial. The general form of a unary polynomial is:

$$p(x) = \sum_{i=0}^{q} g_i x^i \tag{5}$$

Where q is positive integer, g_i is the coefficients in the unary polynomial. Since (5) has $q+1$ independent coefficients and qth power, it is quite hard to analyze (5). In order to not lose the generality of the unary polynomials (5), it is changed as follows:

$$p(x) = (ax + b)^m \tag{6}$$

Where a and b are coefficients, m is exponent. They make sure that (6) not only retains each term in unary polynomial (5) but also reduces uncertain coefficients to two, when (6) is expanded.

In the actual design of the polynomial hardware circuit, it is clear that the bigger the power of a polynomial is, the huger the structure of the hardware is, and the more complex the process is, because the bigger power may easily lead to a very large or very small calculated value. But if the digits of each coefficient are limited, the hardware structure and the process do not have big impact. In order to determine m , firstly, let both a and b in (6) equal to 1, and the range of m in (6) is chosen as $\{m\,|1 \le m \le 20, m \in N^+\}$. Then the influence of coefficients is going to discuss later. According to (4), the LE corresponding to (6) in different m can be calculated. As we know, LE can be used to quantitatively determine the complexity of chaos, the best value of m in (6) can be determined. The relationship diagram between m in (6) and LE of Chua's chaotic x after transforming with $(x+1)^m$ is shown in Figure 1.

When $m < 16$, although m is increased, LE is decreased instead, as shown in Figure 1. Therefore, it is not necessary to use $m < 16$ in (6), which can save the hardware resource.

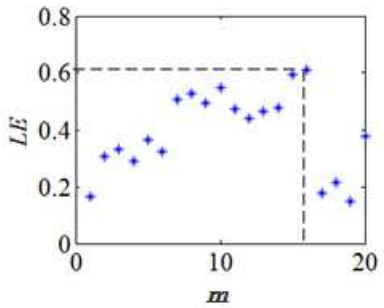


FIGURE 1. The m-LE relationship diagram for $a = b = 1$ and $1 \le m \le 20$

On the basis of above analysis, the m of (6) is determined as $\{m\,|1 \le m \le 16, m \in N^+\}$. It is clear that there are two undetermined coefficients a and b in (6). Firstly, one coefficient is fixed and the influence of the other coefficient will be analyzed on LE. After that, go back to analyze the opposite case in this way. Therefore, the complexity of chaos after UPT can be directly obtained.

2.1. **Case 1.** Assume that b in (6) is equal to 1, and only think about the LE changed condition when the range of values for a and m are $\{a\,|1 \le a \le 9, a \in N^+\}$ respectively. According to the simulation calculation results of LE, the changing relationship curve among m, a and LE is shown in Figure 2(a). In this figure, the maximum LE is 0.7695 corresponding to $a = 2$ and $m = 8$, which chaotic motions are the most complex. Therefore, (6) is determined and the unary polynomial becomes:

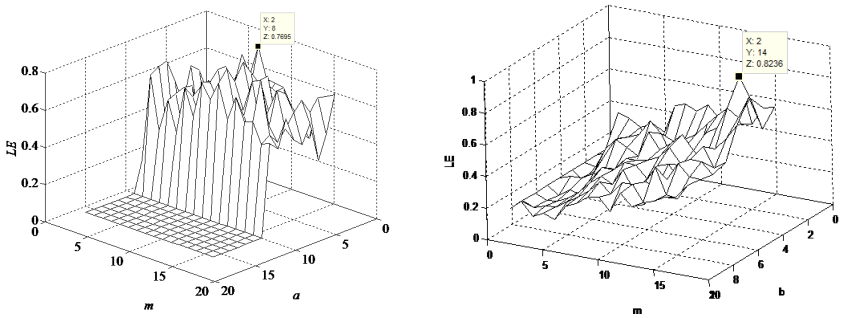
$$p(x) = (2x + 1)^8 \tag{7}$$

2.2. **Case 2.** Assume that a in (6) is equal to 1 and only think about the changed conditions of LE when the range of values for b and m are $\{b\,|1 \leq b \leq 9, b \in N^+\}$ and $\{m\,|1 \leq m \leq 16, m \in N^+\}$ respectively. The calculation results of LE are shown in Figure 2(b).

Clearly, as shown in the Figure 2(b), the maximum LE is 0.8236 corresponding to b=2 and m=14, then the unary polynomial is changed into:

$$p(x) = (x+2)^{14} \tag{8}$$

Comparing (8) with (7), it can be seen that when the power m increases by 6, but LE only increases by 0.0541. Comprehensively considering main factors such as hardware scale and signal process, the BUP is chosen as (7).



(a) (b)

FIGURE 2. The LE relationship curve:(a)a-m-LE curve,(b)b-m-LE curve

3. **Analysis of Chaos Sequence Transformed by BUP.** Chua's system (1) is discretized by fourth-order Runge-kutta iteration, which initial conditions are (2), iterative step h=0.05, and iterations n=75536. During initial stage of iteration, (1) can not enter chaos immediately. Therefore, the first 10000 points produced by variable x in (1) are discarded, the chaotic sequence $x(n)$ is gotten. Then a cipher sequence $p(n)$ is obtained by using the BUP (7) to transform $x(n)$. But can $p(n)$ satisfy the randomness? This question determines whether $p(n)$ is suitable for image encryption, because the security of image encryption in the form of sequential cipher relies mostly on the randomness of cipher sequence. For this reason, the followings respectively from two angles of autocorrelation and randomness test analyze the randomness of the chaotic sequence transformed by the BUP.

3.1. **Autocorrelation of Chaotic Sequence Transformed By BUP.** According to the definition of autocorrelation:

$$R(n) = \sum_{j=-\infty}^{\infty} x(j)x(j-n) \tag{9}$$

In the Matlab environment, the autocorrelation function of the sequence $p(n)$ can be realized by programming, as shown in Figure 3.

Obviously, the autocorrelation of the sequence $p(n)$ is a two-valued function. When n is zero, the correlation to its own is 1; When n is the value of any other sequences, $R(n)$ are almost zero. It shows that any two of sequence value are uncorrelated, which satisfies the characteristic of a random sequence autocorrelation.

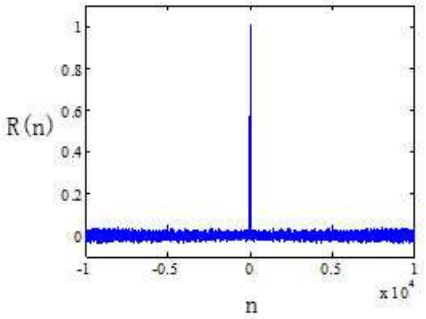


FIGURE 3. The autocorrelation of $p(n)$

3.2. **Randomness test of chaotic sequence transformed by BUP.** Randomness of two-valued sequence in the mathematical statistic is reflected mainly in frequency test, sequential test and run test. In order to find out whether $p(n)$ satisfies the statistical property of random sequence, 40000 points are extracted from the 20000th point of $p(n)$ and quantified into binary sequence $p(k)$, then the above three aspects are conducted as follows.

1. Frequency test is used to determine whether the number of 0 and 1 in the sequence $p(k)$ are essentially equal. Since the total number of samples is N=40000, if the number of 0 and 1 appeared in $p(k)$ are equal, the number of 0 and 1 should be all equal to 20000. After statistical analysis to quantized sequence $p(k)$, its results show that the number of 0 and 1 appeared in $p(k)$ respectively are $N_0 = 19998$ and $N_1 = 20002$. In this case, a hypothesis test to the fluctuation in $p(k)$ should be carried on. x^2 hypothesis test is carried on as follow:

$$x^2 = (N_0 - N_1)^2/N = 0.0001 \tag{10}$$

x^2 distribution table shows that the x^2 is 3.841 and significant level is 0.05 [10]. It is clearly seen that $p(k)$ can pass hypothesis test.

2. Sequential test is used to determine whether the transition state probability appeared in $p(k)$ are essentially equal. A transition state N_{00} in $p(k)$ is its current value and its next value respectively are 0 and 0; a transition state N_{01} is from 0 and 1; Similarly, N_{10} is from 1 and 0; and N_{11} is from 1 to 1. If $p(k)$ is a random sequence, the number of each transition state should be equal: $\zeta = (N-1)/4 \approx 10000$. The results of statistical analysis to $p(k)$ are $N_{00} = 10068$, $N_{01} = 9949$, $N_{10} = 9949$ and $N_{11} = 10033$. Therefore, x^2 hypothesis test to fluctuations in the sample should be carried on as follow:

$$x^2 = [(N_{00} - \zeta)^2 + (N_{01} - \zeta)^2 + (N_{10} - \zeta)^2 + (N_{11} - \zeta)^2]/\zeta = 1.2003 \tag{11}$$

x^2 distribution table shows that the value of x^2 is 5.9915 and significant level is 0.05[10]. Clearly, $p(k)$ can pass hypothesis test.

3. Run test is used to determine whether the number of 0 runs and 1 runs in $p(k)$ are essentially equal. If $p(k)$ is a random sequence, the number of runs whose length is L is $N/2^L$ accounting for $1/2^L$ of the ideal runs total number [11]. The statistical results are shown in Table 1. Obviously, the proportion of different length runs basically conforms to statistical property of random sequence in total proportion of runs. Therefore, $p(k)$ can pass run test.

In conclusion, the chaotic sequence transformed by the BUP has good randomness.

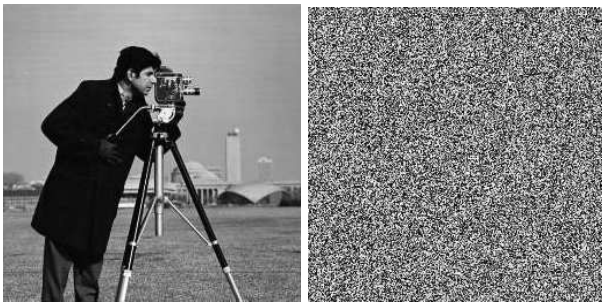
4. **Image Encryption and Decryption Experiments.** α in Chua's system (1) is chosen as a changed parameter for studying the impacts on the states of (1). The following

TABLE 1. Run Test to $p(k)$

	L=1	Proportion	L=2	Proportion	L=3	Proportion
0 runs	19998	50.00%	10051	25.13%	5078	12.70%
1 runs	20002	50.01%	10057	25.14%	5079	12.70%

does experiments on encrypting and decrypting image by using the chaotic sequence before and after being transformed by the BUP (7). The clear image is Figure 4(a). In the experiment, the initial values in (2) are used as keys, iteration step is $h = 0.05$, and iterations are $N = N_{um}+10000$ (N_{um} is the number of image pixels). The chaotic sequence transformed by (7) is used to encrypt clear image. After that obtained cipher image is Figure 4(b). Figure 4(b) shows that the pixel values of the cipher image are distributed in random way and pixel gray distribution is uniform. Clearly, the clear image is completely hidden and any details can not be seen.

Chua's system (1) is not in chaos state when $\alpha = 6.5$, and its sequence can not be used to encrypt the image, as shown in Figure 5(a). But after it transformed by the BUP (7), encryption effect is improved because most of outlines are covered although the clear image can not be completely encrypted, as shown in Figure 5(b). When $\alpha = 6.84$, (1) is in the degeneration state of chaos and it is not suitable for encryption, and most of outlines and information can be seen, as shown in Figure 5(c). But after the degenerative chaos transformed by (7), the clear image is encrypted uniformly, and the image information can be completely hidden, as shown in Figure 5(d). Above analysis shows that the encryption effect of chaos transformed by the BUP is better than that of original chaos, which can improve the characteristics of degenerative chaos.



(a) (b)

FIGURE 4. The clear image and the cipher image

Since chaos image encryption method belongs to symmetrical keys, the process of decryption is exactly the same as that of encryption. Therefore, under the conditions that are completely same to (2), the operation of decrypting the cipher image is exactly the same as that of encrypting the clear image.

Under the conditions of the same as encryption keys, the cipher image in Figure 4(b) is decrypted, as shown in Figure 5(e). This decrypted image is entirely consistent with the clear image in Figure 4(a). But when only α in (2) is changed from 10 to 10^{-15} , the wrong decryption image is shown in Figure 5(f). Although the value of only one parameter in (2) differs by 10^{-15}, any clear image information can not be seen. Since there are 7 parameters in (2), the key space of the chaos transformed by BUP for image encryption has at least $7*10^{15}$. This is very huge key space. In addition, in order to correctly decrypt the cipher image, all the others conditions, such as iteration step, iterations, etc., must match exactly with the those of encryption system. Therefore there is extremely difficult

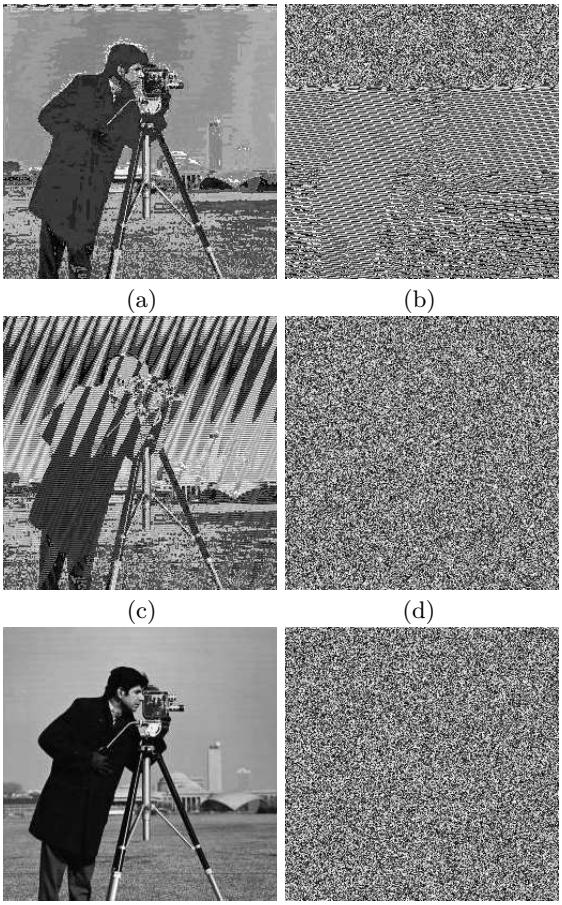


FIGURE 5. Image encryption and decryption before and after transformed by BUP

to decipher for attacker. The experiment shows that the chaos transformed by BUP has higher reliability and security.

5. **Conclusions.** The new method of getting BUP is proposed in this paper. A BUP (7) has been obtained by using the method based on Chua's system. It is simple and easy to realize hardware circuit obviously. Then Simulation results demonstrate that the chaotic sequence transformed by the BUP has good randomness and is more suitable for image encryption. When only one parameter between encryption and decryption differs by 10^{-15}, any clear image information can not be deciphered. However, when the same parameter in [6] differs by 10^{-10}, the same difficult decryption effect can be gotten. All of those have further proved that the chaotic sequence transformed by the BUP is feasible and effective for image encryption. The method of obtaining a BUP is not only suitable for Chua's system but also for others current chaotic systems. Obviously, there is not only one BUP (7) to be suitable for chaos transformation. According to different chaotic systems and conditions, more kinds of chaotic sequences with better characteristics can be obtained by this method. Since the range of parameters m, a and b in (6), according to the conditions, can be expanded, the new BUPs can be found. Meanwhile, the key space of chaos transformed by BUP for image encryption is expanded greatly.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (Grant No. 61471158)

REFERENCES

[1] Y. S. Zhang, D. Xiao, Y. L. Shu, and J. Li, Adaptive synchronization of hyperchaotic CHEN systems with application to secure communication,*IJICIC* , vol.9, no.3, pp. 1127-1144, 2013.

[2] N. S. Maooui, A. Karouma, and M. Zribi,Color image encryption using one-time keys and coupled chaotic systems, Signal processing: *image communication* , vol.29, no.5, pp. 628-640, 2014.

[3] Y. C. Zhou and L. Bao, Image encryption using a new parametric switching chaotic system, Signal processing: *image communication*, vol.9, no.11, pp. 3093-3052, 2013.

[4] Y. L. Luo, M. H. Du, and J. X. Liu, A symmetrical image encryption scheme in wavelet and time domain,*Commun Nonlinear Sci Number Simulat*, vol.9, no.2, pp.447-460, 2015.

[5] M. Francois, T. Grosges, D. Barchiesi, and R. Erra, A new image encryption scheme based on a chaotic function, Signal Processing:*Image Communication*. vol.9, no.3, pp.846-860, 2015.

[6] C.M. CHEN, W. FANG, K.H. WANG, T.Y. WU, Comments on an improved secure and efficient password and chaos-based two-party key agreement protocol, *Nonlinear Dynamics*, vol.87, no.3, pp. 2073-2075, 2017.

[7] L. Wu, H. Chen, and K. Yang, Improvement of the chaotic image encryption effect based on unary polynomial transformation, *ICIC-EL*, vol.27, no.3, pp. 249-259, 2012.

[8] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, Determining Lyapunov exponents from a time series, *Physica D*. vol.16, no.3, pp.285-317, 1985.

[9] T. Matsumoto, L. O. Chua, and M. Komuro, The double scroll, *JIEEE Transactions on Circuits and Systerms*, vol.32, no.8, pp.797-818, 1985.

[10] Z. Sheng, S. Q. Xie and C. Y. Pan, Probability and mathematical statistics, *Higher Education Press*, Beijing, 2008.

[11] S. Sajic, N. Maletic, and B. M. Todorovic, Random binary sequences in telecommunications, *Journal of Electrical Engineering-Elektrotechnicky Casopis*, vol.64, no.4, pp.230-237, 2013.