Text Encryption by Using One-Dimensional Chaos Generators and Nonlinear Equations

Akif Akgül[1], Sezgin Kaçar[1], Burak Arıcıoğlu[2], İhsan Pehlivan[2]

[1] Sakarya University Faculty of Technical Education
aakgul@sakarya.edu.tr, skacar@sakarya.edu.tr
[2] Sakarya University Faculty of Technology
baricioglu@sakarya.edu.tr, ipehlivan@sakarya.edu.tr

Abstract

In this study, a chaos based encryption method with nonlinear equations in MATLAB environment is proposed to increase communication security. Encryption methods that generated by using the properties of three different chaos generators are analyzed. Logistic Map, Pinchers Map and Sine-Circle Map chaos generators which are commonly referred in the literature are used to realize applications. Performance is analyzed by using time and entropy values.

1. Introduction

There has been many studies to prevent the third parties from getting the information during communication. As in the other fields of technology, the faultless systems have not been achieved in security electronics too. Even if the information is encrypted well, there is always a possibility that the information can be decrypted by the third parties. To minimize this possibility, different encryption methods have been developed. In the recent years, the rapid advance in digital electronics makes it possible to have more secure communication systems through the applications of microprocessor and computer based electronic systems[1].

It is accepted that today's encryption algorithms, even the powerful ones can be cracked in a given time[2]. The recent encryption studies emphasize that there is a high correlation between chaos and cryptology sciences due to the special properties of chaotic systems[3]. The chaotic systems have the properties of wide-band, noise -like, hard to predict and aperiodic [4]. Due to the chaotic signals show noise-like behavior and strong dependence on initial values and parameters[5],it makes chaos based encryption more preferable for secure communication. The encrypted data shows complex or noise-like feature and this is very important for data to remain uncracked.

In this paper, chaos based encryption technique is analyzed rather than standard encryption techniques. To increase randomness, the cipher which is needed for encryption and decryption is generated by high level and efficient 1-D chaos generators[6]. The obtained cipher is used for to encrypt to data with the help of nonlinear function. For the decryption of data, what is done for the encryption is done in reverse order to obtain the original data. Moreover, in this study, the ciphers are generated with different chaos generators for encryption and decryption and the performance analysis is made between these chaos generators. In the first part of this paper, chaos and encryption related information is given. In the second part, chaos generators which are used in this study and in the next part, the applications are made are mentioned. In the last part, the results are analyzed.

2. 1-D Chaos Generators

There is plentiful of 1-D chaos generators. 1-D chaotic systems are high efficient and simple[6]. In this paper, Logistic Map, Pinchers and Sine-Circle Map chaos generators which are commonly employed in the literature are used to make application and performance analysis of these generators are made.

2.1. Logistic Map

Logistic Map is one of the most common chaos generators that is used in the literature[7]. The chaotic part of the Logistic Map is examined by considering the bifurcation diagram in the figure 1. The control parameter r in the given equation is examined for the r values of between 0 and 4. As it is seen in the figure 1, if the parameter r has values of between 0 and 3, the result is 1 , if the parameter r has values of between 3 and 3.4, the result is 2, if the value of parameter r is around 3.5 then the result is 4 and if the value is less than 3.5699 and near the entering chaos the result is 8. For the value of parameter r is more than 3.5669 system enters to chaos. When the value of parameter r is between 0 and 3.5699, the system has no positive Lyapunov exponent. If the system has no positive Lyapunov exponent, the system does not have the chaotic behavior[8].

$$x_{n+1} = r * x_n * (1 - x_n) \tag{1}$$

In equation 1, x shows the system's variable and the n shows the number of the repetition. x(0) is the initial value of the system and r is the system's parameter[9].

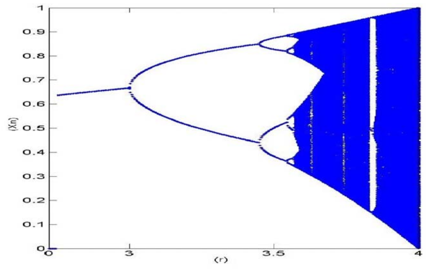


Figure 1. Bifurcation diagram of the Logistic Map

2.2. Pinchers Map

Another 1-D map which is used in encryption in this study is Pinchers Map. The equation for Pinchers Map is given below.

$$x_{n+1} = \mid tanh * s(x_n - c) \mid \qquad (2)$$

In this equation too x is the system's variable and the n is the number of the repetition as in the equation 1. s and c are the parameters of the system. To initialize the system x(0) the initial value must be defined. In the figure 2, the bifurcation diagram of the system is examined when the value of the parameter c is between 0 and 2. As it seen in the figure the system enters chaos when the value of the parameter is approximately between 0.05 and 0.7.

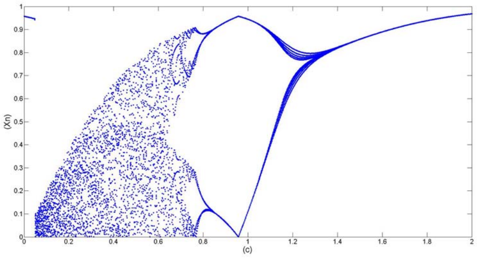


Figure 2. Bifurcation diagram of the Pinchers Map

2.3. Sine-Circle Map

Sine-Circle 1-D map is the third chaos generator that is used in this paper. The equation for the sine-circle map is defined as below.

$$x_{n+1} = x_n + \Omega - K/(2\pi) * sin2\pi * x_n(mod1) \qquad (3)$$

In this equation too x is the system's variable and the n is the number of the repetition as in the equation 1 and 2. To initialize the system x(0) the initial value must be defined. Here K and omega are the parameters of the system.

In figure 3 the bifurcation diagram of the system is given. By changing the value of the parameter omega between 0 and 1, whether the system is chaotic or not is examined. The main difference between Sine-Circle Map and Logistic and Pinchers Map is in the sine-circle map the system does not enter chaos in defined intervals. As it seen in the figure 3, the system shows non-chaotic behavior at some interval when the value of the parameter omega is between 0 and 1 [10].

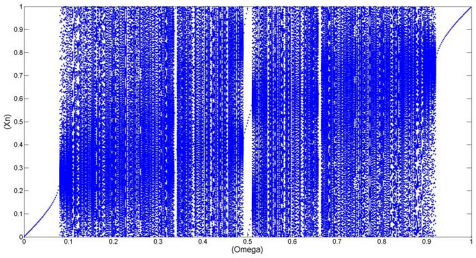


Figure 3. Bifurcation diagram of the Sine-Circle Map

3. Realization of Text Encryption Application

The purpose of this part is encryption of a given text. The cipher needed for encryption is generated by chaos generators to increase the randomness. At the same time, to increase the security of the communication nonlinear equation is used [11]. The ciphers obtained and the data to be encrypted are encrypted with the help of nonlinear function which is given in the equation 4.

$$f(x,m) = \frac{m(3x^4 - x^2 + \sqrt{x})}{5} \qquad (4)$$

Here x shows the ciphers generated by chaos maps and the m shows the data to be encrypted.

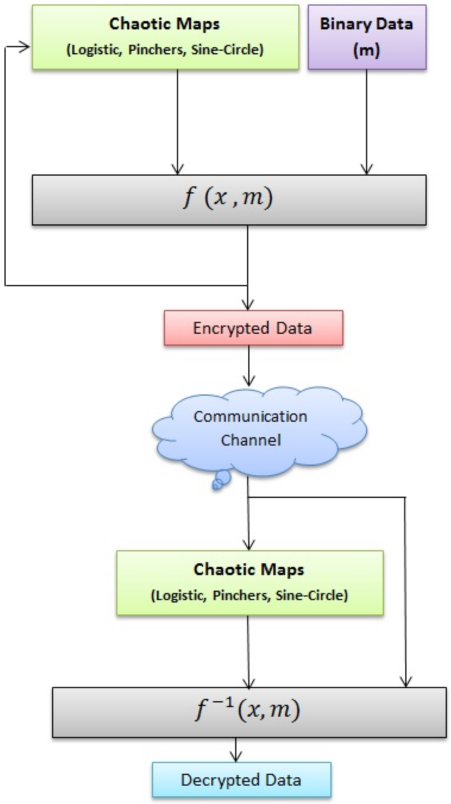
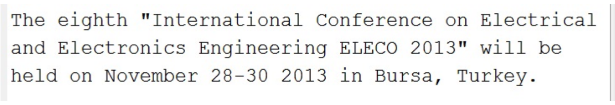


Figure 4. The block diagram of the encryption and decryption processes.

In the block diagram in the figure 4, the data which is encrypted with the help of the nonlinear function is send to communication channel. For the decryption, the encrypted data received from the communication channel is transferred to the chaos generator and the inverse of the nonlinear function. Decryption can be done if the chaos generator that is used for encryption and decryption is the same.

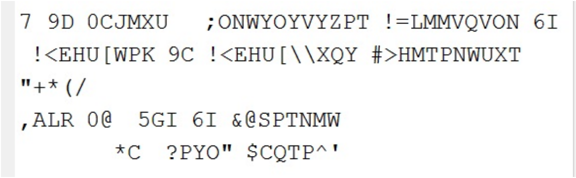
For the encryption, the plaintext in the figure 5 is used. This plaintext represents m in the block diagram in the figure 4.



```
The eighth "International Conference on Electrical
and Electronics Engineering ELECO 2013" will be
held on November 28-30 2013 in Bursa, Turkey.
```

Figure 5. Plaintext

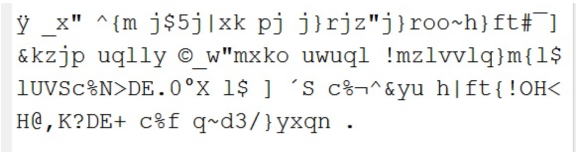
In the figure 6, the encrypted text whose cipher is generated by using Logistic Map is shown.



```
7 9D 0CJMXU   ;ONWYOYVYZPT !=LMMVQVON 6I
 !<EHU[WPK 9C !<EHU[\\XQY #>HMTPNWUXT
"+*(/
,ALR 0@  5GI 6I &@SPTNMW
       *C  ?PYO" $CQTP^'
```

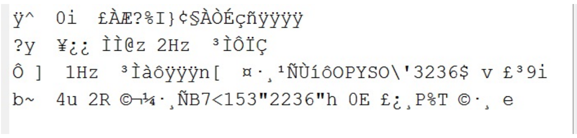
Figure 6. With Logistic Map Encrypted Data

In the figure 7 the text that is encrypted with the help of Pinchers Map and in the figure 8 the text that is encrypted with Sine-Circle Map generated cipher are shown.



```
ÿ _x" ^{m j$5j|xk pj j}rjz"j}roo~h}ft#¯]
&kzjp uqlly ©_w"mxko uwuql !mzlvvlq}m{l$
lUVSc%N>DE.0°X l$ ] ´S c%¬^&yu h|ft{!OH<
H@,K?DE+ c%f q~d3/}yxqn .
```

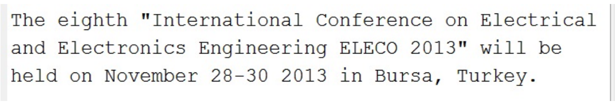
Figure 7. With Pinchers Map Encrypted Data



```
ÿ^  0i  £ÀÆ?%I}¢§ÀÒÉçñÿÿÿÿ
?y  ¥¿¿ ÌÌ@z 2Hz  ³ÌÔÏÇ
Ô ]  1Hz  ³Ìàôÿÿÿn[  ¤·¸¹ÑÙíôOPYSO\'3236$ v £³9i
b~  4u 2R ©¬¼·¸ÑB7<153"2236"h 0E £¿¸P%T ©·¸ e
```

Figure 8. With Sine-Circle Map Encrypted Data

In the figure 9, the decrypted text by inversing the nonlinear equation and with help of chaos generator is shown.



```
The eighth "International Conference on Electrical
and Electronics Engineering ELECO 2013" will be
held on November 28-30 2013 in Bursa, Turkey.
```

Figure 9. Decrypted Text

4. Analysis and Results

In this paper , the performance analysis of the encryption which is made by chaos generator is done by considering the value of entropy and time. The method entropy is the one of the ways to measure how secure the data is[9]. As the entropy value of the encrypted data increases, the reliability of the encryption is also increases. To calculate the entropy value one of the Shannon, Norm, threshold, logarithmic and Sure entropy techniques can be used. In this study, the first and basic entropy calculation technique namely Shannon Entropy technique is used to calculate the entropy value. The equation for Shannon Entropy Technique is given below[12].

$$ShanEn(x) = -\sum_{i=1}^{N}(p_i(x))^2(log_2(p_i(x)))^2 \qquad (5)$$

Here in this equation pi(x) shows probability mass function of the i-th term of the dataset, N shows the number of the probability mass function values. In this study , the encryption done with Sine-Circle Map has the largest entropy value which means the encryption is more complex than the other two methods. The entropy values of the chaos generators are given in the figure 10.

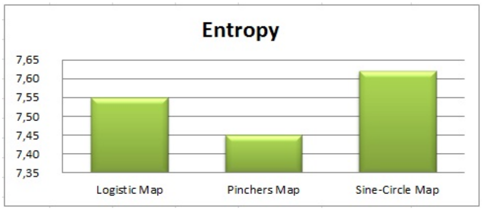


Figure 10. The entropy values of the chaos generators

Moreover, in this paper the encryption and the decryption times of the three chaos generators are compared. As it seen in the figures 11 and 12, logistic map has the longest encryption time while its decryption time is the shortest.

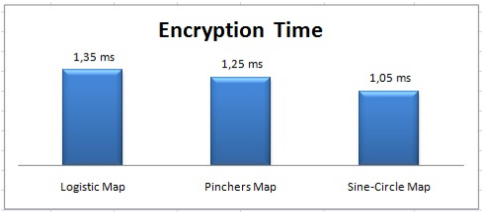


Figure 11. The encryption times

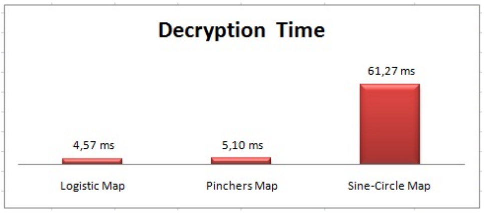


Figure 12. The decryption times

On the other hand, while the Sine-Circle Map has the shortest encryption time, its decryption time is the longest. The inverse proportion between the encryption and the decryption time can be explained with the entropy values. The chaos generator with largest entropy value, in this study Sin-Circle Map which provides more complex encryption than the other two methods, requires more time for decryption.

It is very difficult to get the same encryption performance if non-chaotic methods are used rather than chaotic ones. The results of the analysis shows that, cryptologic systems which are realized by using the three chaos generators those are studied in this paper are efficient and feasible to employ. In addition , it is observed that the encryption and the decryption times and the entropy values of the three chaos generators are different from each other. Sine-Circle Map has the advantage of more secure method, but Sine-Circle Map requires much more time to decrypt and this made this method is very disadvantageous if the text to be decrypted is very long. Finally, the more important advantage of text encryption with these three chaos generators is that the encryption can be realizable by using microprocessor or FPGA.

5. References

[1] A. Akgul, O. Cetin, F.Akar, ”High Secure Infrared Communication Application”, *SIU 2011 - IEEE 19. Sinyal İşleme ve İletişim Uygulamaları Kurultayı,* pp: 474-477, Antalya. Nisan, 2011.

[2] O. Fındık, ”Şifrelemede Kaotik Sistemin Kullanılması ”, M.S. thesis, *Comp. Dept.*, Selçuk. Univ., Konya., 2004.

[3] J.M. Amigó, L. Kocarev,J. Szczepanski, ”Theory and practice of chaotic cryptography”, *Physics Letters A,*, no.366, pp: 211-216, 2007.

[4] F. E. Yardım, E. Afacan, ”Lorenz-Tabanlı Diferansiyel Kaos Kaydırmalı Anahtarlama (Dcsk) Modeli Kullanılarak Kaotik Bir Haberleşme Sisteminin Simülasyonu ”, *Gazi Üniv. Müh. Mim. Fak. Der.,*, vol. 25, no.1, pp: 101-110, 2010.

[5] S. Lian, ”Efficient image or video encryption based on spatiotemporal chaos system”, *Chaos, Solitons and Fractals,*, no.40, pp: 2509-2519, 2009.

[6] K.Sakthidasan, B.V.Santhosh, ”A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images ”, *International Journal of Information and Education Technology,*, vol. 1, no.2, pp: 137-141, June, 2011.

[7] H. Ogras, M. Turk , ”Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function ”, *World Academy of Science Engineering and Technology,*,July, Stockholm, 2012.

[8] O. Yavuz, ”Kaotik Ortamlarda Güvenli Veri Transferi ”, M.S. thesis, *Comp. Dept.*,Karadeniz Technical. Univ., Trabzon., 2006.

[9] M.M.R.A. Milani, H.Pehlivan, S.H.Pour, ”Kaos Tabanlı Bir Şifreleme Yöntemi ve Analizi”, in *Akademik Bilişim’11-XIII. Akademik Bilişim Konferansı Bildirileri*, Malatya., 2011, pp. 487-493.

[10] ”Chaos, Fractals and Dynamical Systems-SineCircle Map”, Theja Tulabandhula, Department of Electrical Engineering, pp: 1-5.

[11] T. Chien, T.L. Liao, ”Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization”, *Chaos, Solitons and Fractals,*, no.24, pp. 241-255, 2005.

[12] S. Kacar, Z. Eksi, A. Akgul, F. Horasan ”MATLAB Paralel Hesaplama Araç Kutusu ile Shannon Entropi Hesaplanması”, in *1st Internatıonal Symposıum On Innovatıve Technologıes In Engıneerıng And Science*, Sakarya., pp. 765-773 7-9, June, 2013.