©2016 Published in 4th International Symposium on Innovative Technologies in
Engineering and Science 3-5 November 2016 (ISITES2016 Alanya/Antalya - Turkey)

An image cryptology application using three-dimensional autonomous continuous chaotic equations

*[1]İhsan Pehlivan and [1]Akif Akgül
[1]Faculty of Technology, Department of Electrical and Electronics Engineering, Sakarya University, Turkey

Abstract

A In this paper, a three-dimensional autonomous chaotic system is introduced, which contains the quadratic, cubic and quartic nonlinearities. Cryptology application of the proposed chaotic system is discussed for the purpose of creating secure data bases and for sending secure messages. In particular, a chaotic encryption on an image implemented out to ensure data security.

Key words: Chaotic system, phase portrait, image cryptology, chaos based cryptology

1. Introduction

The dynamical systems are well known for its various applications such as in a population growth model, biomedical, engineering, etc. [1-12]. Thus the chaos is a ubiquitous and extremely complex nonlinear phenomenon in nature. In fact, chaos is a general term used to represent the chaotic dynamical system. A lot of research has been done and the system has been widely investigated in all kinds of characteristics.

In the past few years, motivated by many unknown interesting properties and some potential practical applications, great efforts and achievements have been made in constructing chaotic and hyperchaotic sytems [13-19]. In this paper, a chaotic system containing quadratic, cubic and quartic nonlinearities is proposed [20]. On the other hand; chaotic systems, have attracted lots of attention in recent years. Chaotic systems have been used in many different areas for different purposes. One of these areas is encryption. Numerous studies have been executed about importance security. There have been many previous studies with different methods and chaos encryption [21-28].

In this study, we executed the application of the chaotic system in cryptology where a chaotic encryption on an image is implemented out to ensure data security. In this application, encryption was done using chaotic system. The application on this article was performed with MATLAB (MatrixLaboratory), a program used in academic studies and Research and Developments as well as industrial enterprises.

This paper is organized as follows: In Section 2, the chaotic system is introduced. The basic dynamics of the proposed system have been discussed in the subsections. The cryptology application is given in Section 3. And finally, conclusion based on the theoretical and numerical investigation is given in Section 4.

*Corresponding author: Address: [1]Faculty of Technology, Department of Electrical and Electronics Engineering, Sakarya University, 54187, Sakarya TURKEY. E-mail address: ipehlivan@sakarya.edu.tr, Phone: +902642956461

2. The Chaotic System and Its Properties

The chaotic system introduced in this paper is described as the following autonomy differential equations:

$$\begin{cases} \dot{x} = a(x - y) \\ \dot{y} = -4ay + xz + mx^3 \\ \dot{z} = -adz + x^3y + bz^2 \end{cases} \qquad (1)$$

where x, y and z are state variables and a, b, d and m are parameters. The parameters values are set to $a = 1.8, b = -0.07, d = 1.5$ and $m = 0.12$. The system exhibits a chaotic behavior for the chosen values.

The initial values of the system are chosen as $(0.5, 0, 0)$ and simulations have been completed. This nonlinear system exhibits the chaotic dynamic behavior. In Figure 1, we produce the $x - y, x - z, y - z$ and $x - y - z$ phase portraits of the chaotic system (1) using the MATLAB ode45 function. Figure 1 demonstrates the phase portraits for $m = 0.12$.

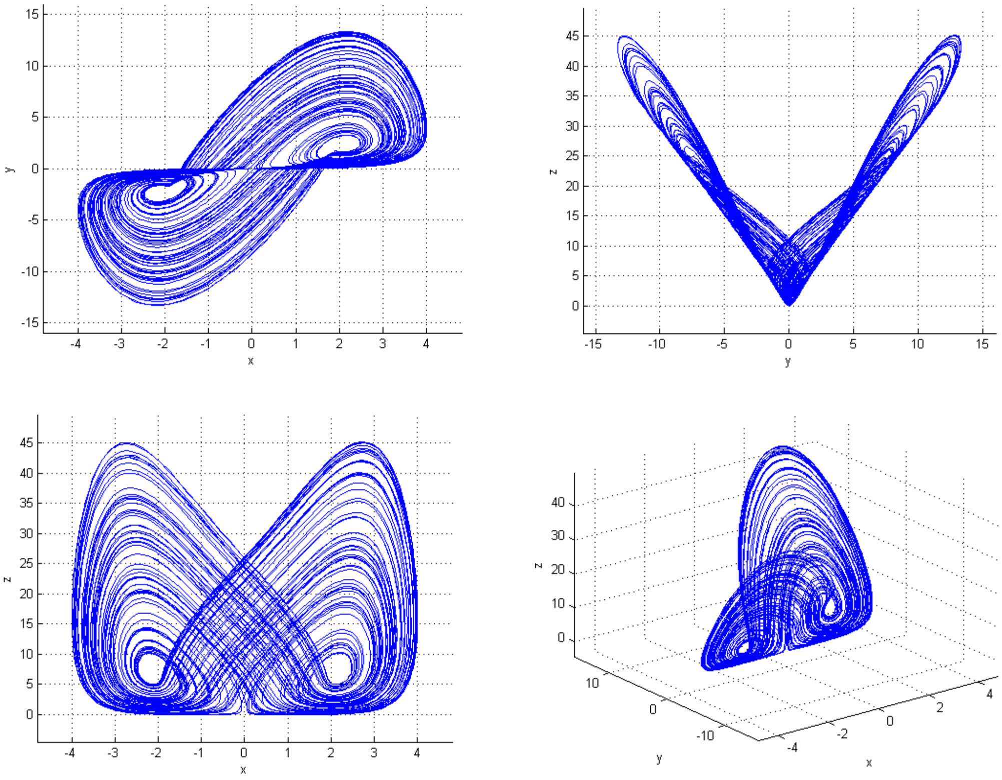

Figure 1. Phase portraits of system (1) with $a = 1.8, b = -0.07, d = 1.5$ and $m = 0.12$.

3. Method

3.1. Cryptology Application

Secure communication is one of the many application the areas of chaotic systems. In this article, a chaotic system was used to increase security of image. In addition to the chaotic system used, a nonlinear equation was also employed to increase security in communication.

The keys in encryption and image in figure 3 to be encrypted were confused with the help of the function given in nonlinear equation (1)

$$\frac{2x\left(1+xm+\left(1\text{-}m\right)+0.9\right)}{4.8} \tag{1}$$

where x value in the function represents the keys produced with the help of the chaos generator seen on block diagram on Figure 2, and m value represents the image data in Figure 3 (256*256) to be encrypted.

Figure 2 exhibits the general block diagram of encryption application for secure transmission of image. As can be seen from the block diagram, image data and keys produced with chaotic system are encrypted with the help of the function as in equation (1). Later, encrypted data in the block diagram can be decrypted with the inverse of the function.

The values 0.9 and 4.8 are the other parameters to be known while decryption the encrypted data. The order of m values during data encryption and decryption is very significant. It can be observed that the function is different from those with 0 and 1 m value.
If m value as 0 equation (2);

$$\frac{\left(2x\left(2-m\right)+0.9\right)}{4.8} \tag{2}$$

if m value as 1 equation (3);

$$\frac{\left(2x\left(1+xm\right)+0.9\right)}{4.8} \tag{3}$$

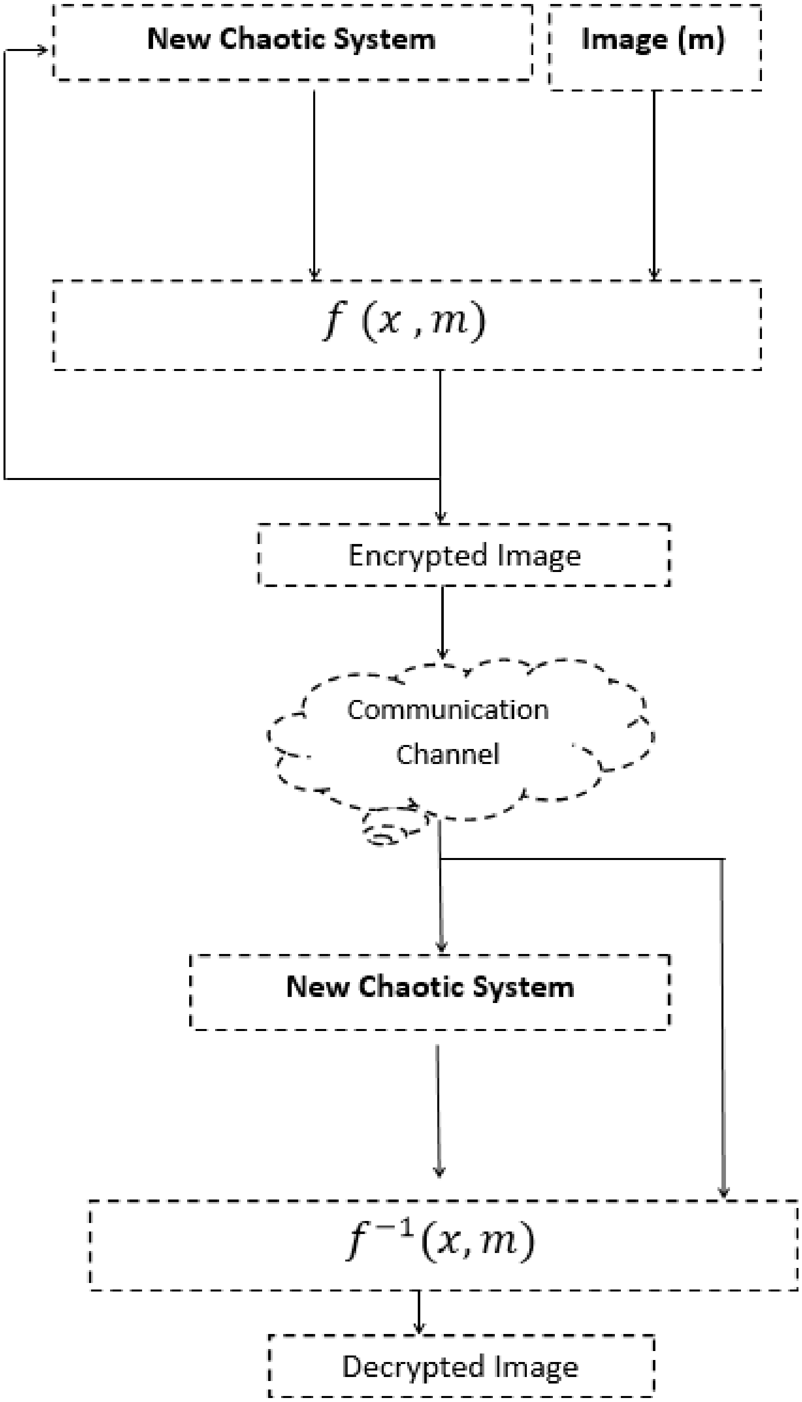

Figure 2. Block Diagram of Encryption and Decryption Image.

3.2. Application

Figure 3 show 256*256 bits image to be encrypted. Original image in Figure 3 were encrypted by using the chaotic system. Encrypted image with chaotic system is shown in Figure 4.

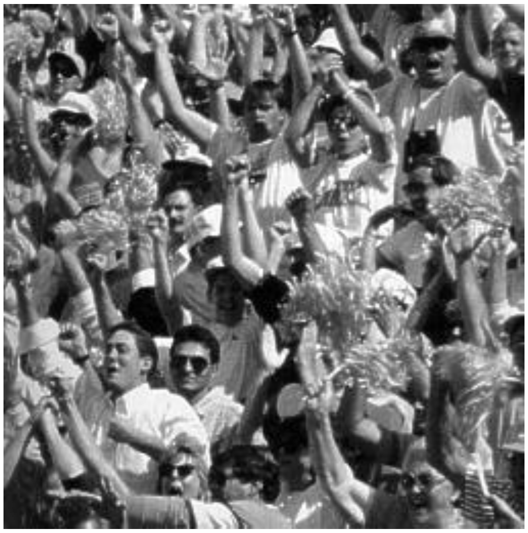

Figure 3. Original Image.

In order to decrypt the encrypted data in chaos based encryption applied here, one needs to know keys produced for each bit (256*256 keys for 256*256 bits of image) and the order of these keys, all parameters and initial values in chaotic systems, the non-linear equation used and all parameters belonging to this equation. Because of any mistake during the decryption of the encrypted data, such as changing even just one key data, encrypted data can not be decrypted and the original image can not be retained.

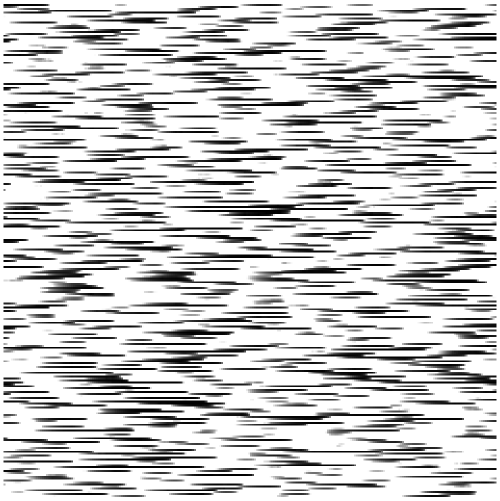

Figure 4. Using the Chaotic System Encrypted Image.

Figure 5 show decrypted image obtained from the decryption process which was performed as explained on the block diagram in part 4.1. There is no corruption in the image, which proves that both encryption and decryption processes were performed successfully.

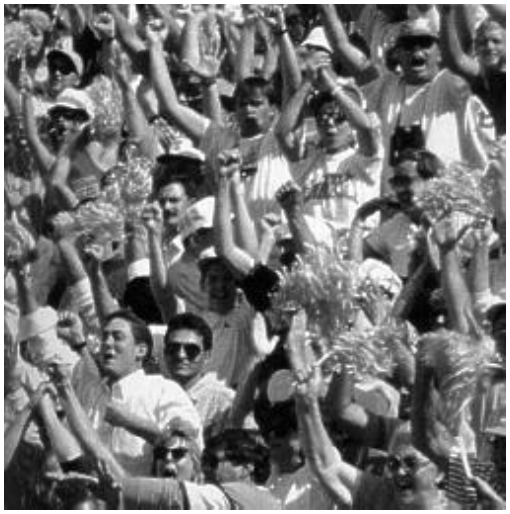

Figure 5. Decrypted Image.

Conclusions

This article has introduced a three-dimensional autonomous chaotic system.The cryptology application of the proposed system is also provided where a chaotic encryption on a image implemented out to ensure data security. In order to decrypt the encrypted data with chaos system applied here, one needs primarily to analyze chaotic system in this paper (all parameters, initial values in chaotic systems, etc.). Because the different chaotic system, encrypted data easily can not be decrypted and the original image can not be retained.

References

[1] E. N. Lorenz, Deterministic nonperiodic flow, Journal of Atmospheric Sciences, 1963, vol. 20: 130-141.

[2] T. Y. Li and J. A. Yorke, Period Three Implies Chaos, The American Mathematical Monthly, 1975, vol. 82: 985 – 992.

[3] O. E. Rossler, An equation for continuous chaos, Physics Letters A, 1976, vol. 57, no. 5, pp. 397-398.

[4] O. E. Rossler, Continuous chaos; four prototype equations, Annals of the New York Academy of Sciences, 1979, vol. 316, no. 1: pp. 376-392.

[5] T. Matsumoto, L. O. Chua, and S. Tanaka, Simplest chaotic nonautonomous circuit, Physical Review A, 1984, vol. 30: 1155-1157.

[6] G. Chen and T. Ueta, Yet another chaotic attractor, International Journal of Bifurcation and Chaos, 1999, vol. 09, no. 07: pp. 1465-1466.

[7] J. Lu, G. Chen, and S. Zhang, Dynamical analysis of a new chaotic attractor, International Journal of Bifurcation and Chaos, 2002, vol. 12, no. 5: pp. 1001-1015.

[8] J. C. Sprott, Some simple chaotic flows, Physical Review-Section E-Statistical Physics Plasma Fluids Related Interdiscpl Topics, 1994, vol. 50, no. 2: p. R647.

[9] J. C. Sprott, Simplest dissipative chaotic flow, Physics letters A, 1997, vol. 228, no. 4: pp. 271-274.

[10] J. C. Sprott, A new class of chaotic circuit, Physics Letters A, 2000, vol. 266, no. 1, pp. 19-23.

[11] C. Liu, T. Liu, L. Liu, and K. Liu, A new chaotic attractor, Chaos, Solitons and Fractals, 2004, vol. 22, no. 5: 1031-1038.

[12] R. A. V. Gorder and S. R. Choudhury, Analytical hopf bifurcation and stability analysis of T system, Communications in Theoretical Physics, vol. 55, no. 4, p. 609, 2011.

[13] I. Pehlivan and Y. Uyaroglu, Simplied chaotic diffusionless Lorentz attractor and its application to secure communication systems, IET Communications, 2007, vol. 1, no. 5: 1015-1022.

[14] Y. Uyaroglu and I. Pehlivan, Nonlinear sprott94 case a chaotic equation: Synchronization and masking communication applications, Computers and Electrical Engineering, 2010, vol. 36, no. 6, pp. 1093-1100.

[15] I. Pehlivan and Y. Uyaroglu, A new 3d chaotic system with golden proportion equilibria: Analysis and electronic circuit realization, Computers and Electrical Engineering, 2012, vol. 38, no. 6, pp. 1777-1784.

[16] V. Sundarapandian and I. Pehlivan, Analysis, control, synchronization, and circuit design of a novel chaotic system, Mathematical and Computer Modelling, 2012, vol. 55, no. 7-8, pp. 1904-1915.

[17] S. Cicek, Y. Uyaroglu, and I. Pehlivan, Simulation and circuit implementation of sprott case h chaotic system and its synchronization application for secure communication systems, Journal of Circuits, Systems, and Computers, 2013, vol. 22, no. 4.

[18] S. Gang-Quan, C. Hui, and Z. Yan-Bin, A new four-dimensional hyperchaotic Lorenz system and its adaptive control, Chinese Physics B, 2011, vol. 20, no. 1: p. 010509.

[19] P. Lijun, D. Lixia, and L. Huayan, Dynamics of the coupled Lorenz-Rössler systems, in Proceedings of the 2010 International Workshop on Chaos-Fractal Theories and Applications, IWCFTA '10, (Washington, DC, USA), pp. 271-274, IEEE Computer Society, 2010.

[20] A. Akgul, S. Hussain, I. Pehlivan, A new three-dimensional chaotic system, its dynamical analysis and electronic circuit applications, Optik - International Journal for Light and Electron Optics, Volume 127, Issue 18, September 2016, Pages 7062-7071, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2016.05.010.

[21] M. Sobhy and A.-E. Shehata, Chaotic algorithms for data encryption, in Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). IEEE International Conference, vol. 2, pp. 997-1000 vol.2, 2001.

[22] K. Sakthidasan and B. V. S. Krishna, A new chaotic algorithm for image encryption and decryption of digital color images, International Journal of Information and Education Technology, 2011, vol. 1, pp. 137-141.

[23] F. Yardim and E. Afacan, Lorenz-Tabanli dferansiyel kaos kaydırmalı anahtarlama (dcsk) model kullanılarak kaotik bir haberlesme sisteminin simulasyonu", Journal of the Faculty of Engineering and Architecture of Gazi University, 2010, vol. 25, no. 1: 101-110.

[24] I. Pehlivan and Z. Wei, Analysis, nonlinear control and circuit design of an another strange chaotic system, Turkish Journal of Electrical Engineering and Computer Sciences, 2012, vol. 20, no. Sup2: 1229-1239.

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

[26] H. Ogras, M. Turk, and S. Ogras, Kaos tabanlı sayısal csk ve dcsk modulasyon tekniklerinin matlab/simulink ortamında gercekletirilmesi, IV. lletisim Teknolojileri Ulusal Sempozyumu, Adana, 2009.

[27] H. Ogras and M. Turk, Digital image encryption scheme using chaotic sequences with a nonlinear function, World Academy of Science Engineering and Technology, 11-12 July, Stockholm, Sweden, vol. 6, pp. 461-464, 2012.

[28] O. Findik, Sifrelemede kaotik sistemin kullanlmasi, Master's thesis, Selçuk University, 2004.