BOOK CHAPTER | Chaos-Based Security

Chaos-Based Information Security: A Novel Approach to Securing the Cyberspace

Adeyemi, Vincent Ademola & Nuñez-Perez, Jose Cruz
Instituto Politécnico Nacional, IPN-CITEDI
Tijuana, Baja California 22435, México
Email: vademola.adeyemi@ieee.org

ABSTRACT

In this age, the cyberspace has become the fastest and certainly the easiest means of sharing information, including confidential ones, but with attending consequences, one of which is the stolen of information by unauthorized users. The objective of this work is the application of chaotic dynamical systems to develop a symmetric cryptosystem to protect information in the cyberspace. The proposed system consists of encryption and decryption modules, each performing three rounds in their respective process. To demonstrate the system, a grayscale image was used. The results show that the information was adequately encrypted and protected by chaos in the cyberspace and can be fully recovered without loss of quality by intended users.

Keywords – chaos, cryptosystem, cyberspace, security.

INTRODUCTION

Since the invention of the Internet, the technology has opened enormous possibilities for information sharing like never before. However, this is not without some attending consequences, one of which is the possibility of losing confidential and personal information to hackers. The consequences of our confidential and personal information in the hands of unauthorized users cannot be overemphasized [1]. The challenge of protecting information in the cyberspace is not a trivial one, hence, commendable efforts have been made in this regard [2-4]. The objective of the present contribution is the application of chaos theory to develop a cryptosystem [5, 6] for securing information in the cyberspace. Chaos is a phenomenon of nonlinear dynamical systems and possesses the properties of being sensitive to initial conditions and system parameters, non-periodic, and deterministic [7]. A cryptosystem consists of encryption and decryption algorithms, and there are two types, namely, symmetric and asymmetric. The symmetric cryptosystem involves the use of the same keys, which are private, for both encryption and decryption of information, while the asymmetric cryptosystem uses a public key for encryption and a private key for decryption.

Citation: Adeyemi, Vincent Ademola & Nuñez-Perez, Jose Cruz (2022). Chaos-Based Information Security: A Novel Approach to Securing the Cyberspace. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

LORENZ SYSTEM

Edward Norton Lorenz, a Meteorologist and Mathematician, invented a nonlinear dynamical system in 1963 for weather forecast research [8]. The Lorenz system displays sensitivity to the initial conditions, and hence, it is a chaotic system. The three-dimensional model consists of coupled ordinary differential equations as shown in the next equation:

$$\begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = x(r - z) - y, \\ \dot{z} = xy - bz, \end{cases} \quad (1)$$

Where
x, y, and z are the state variables

While σ, r, and b are constant parameters.

For example, the Lorenz system (1) generate chaos when $\sigma = 10$, $b = 8/3$, and $r = 28$, with the initial conditions $(x_0, y_0, z_0) = (0.1, 0.1, 0.1)$. The phase space of the model is presented in Figure 1, showing chaotic strange attractor as $x(t)$, $y(t)$, and $z(t)$ evolve against time.

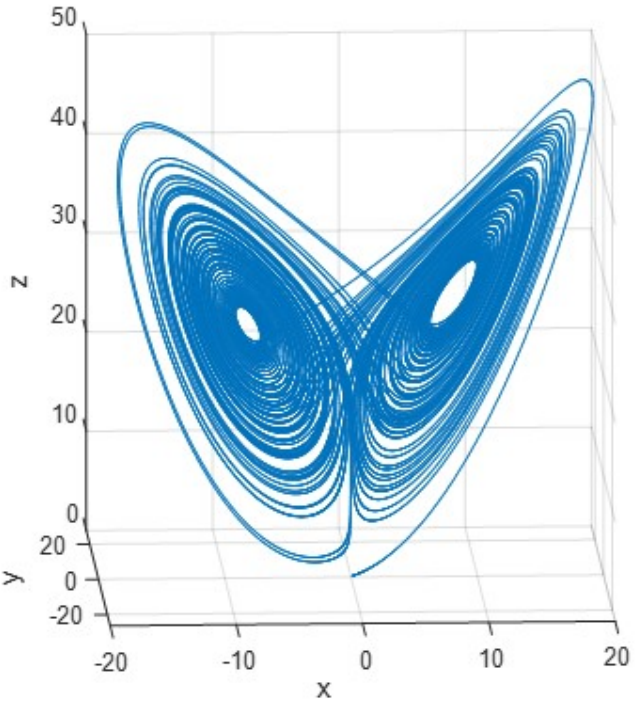

Figure 1: Chaotic strange attractor of the Lorenz system (1) on 3D plane.

Chaos-based Cryptosystem

The properties of chaotic nonlinear dynamic systems, such as ergodicity and sensitivity to initial conditions and system parameters, can be exploited to design cryptosystems for securing information in the cyberspace. In the proposed cyber security system, a sender utilizes chaos-based encryption algorithm (CBE) to encrypt information of any type, such as image, text, video, or audio, while the receiver also uses chaos-based decryption (CBD) algorithm to decrypt the encrypted information. In Figure 2 is found the decryption of the cyber security system implemented with chaos. The cryptosystem is based on the chaotic sequences of the Lorenz system (1), generated by the three state variables *x*, *y*, and *z*. The chaos-based cryptosystem is symmetric, meaning that the encryption and decryption keys are the same and private. In all, there are a total of six private keys, consisting of the three system parameters and the three initial conditions.

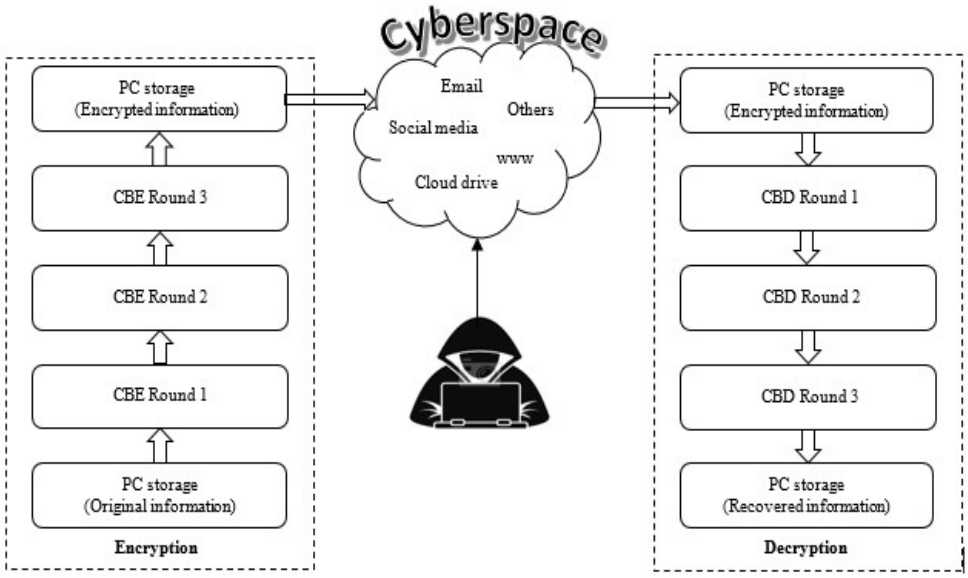

Figure 2: Architecture of the chaos-based cyber security.

As shown in Figure 2, a sender applies the encryption algorithm, which involves three rounds of CBE using each chaotic state of the Lorenz system, on the original information and generates the final ciphered information after the third round.

The encryption is achieved by performing exclusive-or operation between the original information and the chaotic sequence. For the ciphered information to get to the receiver, it must pass through the cyberspace, which can be via different means such as the email, social media, cloud drive, and so on, and with a potential of being intercepted by hackers. At the receiver, the user applies the decryption algorithm, which also involves three rounds of CBD in a reverse order using the same chaotic states, on the ciphered information and generates the final deciphered information after the third round.

RESULTS AND DISCUSSION

The implementation of the chaos-based cryptosystem was done in MATLAB, and it consists of two separate modules, namely Module 1 and Module 2. The Module 1 is the encryption system on the sender's computer while the Module 2 is the decryption system on the receiver's computer. To demonstrate this chaos-based cyber security, grayscale image of size 640x480 and 8-bit depth was used. Figure 3 shows the original image, encrypted image by chaos, and recovered image by chaos. Table 1 presents the statistical analysis by correlation coefficient to examine the results.

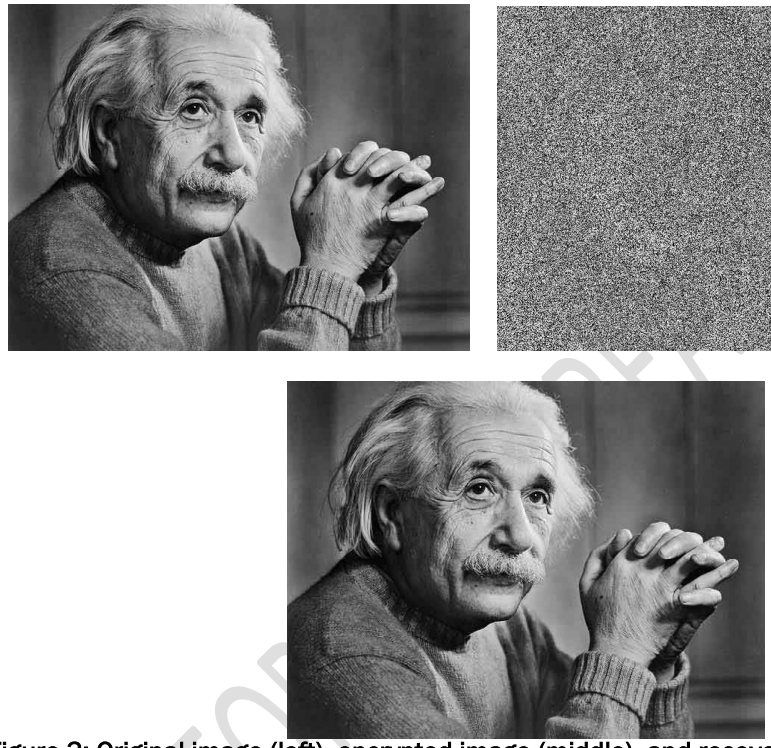

Figure 3: Original image (left), encrypted image (middle), and recovered image (right).

Table 1: Statistical analysis of the cryptosystem by correlation coefficient.

Images	Correlation
Original and encrypted	-0.0495
Original and recovered	1

In Figure 3, it is seen that the encrypted image totally differs from the original image because of the encryption performed with the chaos from the Lorenz system (1). This was confirmed by the correlation coefficient of approximately 0 between the original and encrypted images in Table 1. On the other hand, the original and recovered images are the same because there was no loss of quality. This was confirmed by the correlation coefficient of 1 between the two images as shown in Table 1.

Now, let's assume a case whereby the encrypted image was intercepted by a hacker while in the cyberspace. Considering that the keys are private, and the Lorenz system (1) is sensitive to initial conditions and the parameters, if any of the private keys has a change in value, it will affect the recovery of the information.

To demonstrate this key sensitivity, the initial conditions in the Lorenz system (1) were changed to (x_0, y_0, z_0) = (0.5, 0.5, 0.5) for the decryption algorithm. The result is presented in Figure 4, whereby it is seen that the original image could not be recovered.

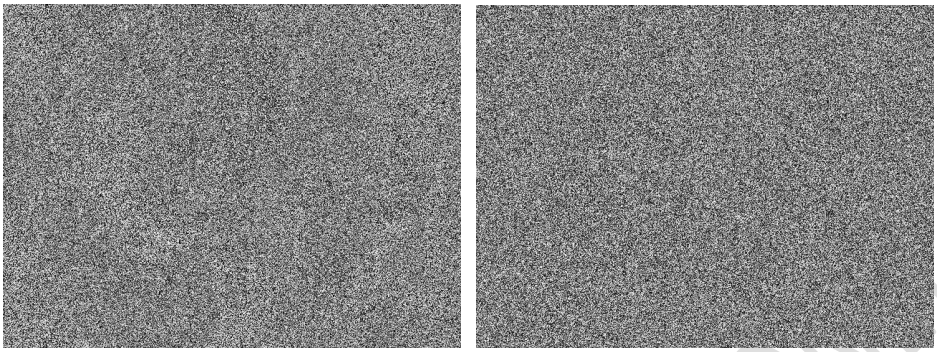

Figure 4: Key sensitivity result showing the encrypted image (left) and recovered image (right).

With a considerable precision for the fractional part of the secret keys, the total size of the secret key space will be very high, making the cryptosystem to be very robust.

CONCLUSION

This paper showcases the application of chaos in the security of information in the cyberspace. The underlying chaotic system for the developed cryptosystem, which consists of a chaos-based encryption module and a chaos-based decryption module with private keys, was the Lorenz system. The cryptosystem was demonstrated to encrypt a grayscale image and decrypt the encrypted image, and the results were analyzed statistically using correlation coefficient. It was also shown that even if the encrypted information, image in this case, is intercepted by a hacker on the Internet, the original information would not be recovered due to the sensitivity of the system to the secret keys of the chaotic system. The cryptosystem is applicable to data in other forms, such as video, text, and audio, and it does not suffer from low-level efficiency Hence, chaos-based information security is proven to be a reliable method for protecting information in the cyberspace.

REFERENCES

[1] I. Agrafiotis, J.R.C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, Vol. 4, No. 1, Oct. 2018, Art. No. tyy006.

[2] A. Singh, V.K. Sharma, and S. Chauhan, "A hybrid model for cyberspace security," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 1595-1600, doi: 10.1109/I-SMAC52330.2021.9640951.

[3] J. Srinivas, A.K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, Vol. 92, pp. 178-188, March 2019.

[4] Z. Guo, L. Tang, T. Guo, K. Yu, M. Alazab, and A. Shalaginov, "Deep graph neural network-based spammer detection under the perspective of heterogeneous cyberspace," *Future Generation Computer Systems*, Vol. 117, pp. 205-218, April 2021.

[5] J.C. Nuñez-Perez, V.A. Adeyemi, Y. Sandoval-Ibarra, F.J. Pérez-Pinal, and E. Tlelo-Cuautle, "FPGA Realization of Spherical Chaotic System with Application in Image Transmission," *Mathematical Problems in Engineering*, Vol. 2021, No. 2, April 2021, Art. No. 5532106.

[6] V.R. Folifack Signing, G.A. Gakam Tegue, M. Kountchou, Z.T. Njitacke, N. Tsafack, J.D.D. Nkapkop, C.M. Lessouga Etoundi, and J. Kengne, "A cryptosystem based on a chameleon chaotic system and dynamic DNA coding," *Chaos, Solitons & Fractals*, Vol. 155, Feb. 2022, doi.org/10.1016/j.chaos.2021.111777.
[7] R. Montero-Canela, E. Zambrano-Serrano, E.I. Tamariz-Flores, J.M. Muñoz-Pacheco, R. Torrealba-Meléndez, "Fractional Chaos-Based Cryptosystem for Generating Encryption Keys in Ad Hoc Networks," *Ad Hoc Networks*, Vol. 97, Feb. 2020, Art. No. 102005.
[8] E.N. Lorenz, "Deterministic Nonperiodic Flow," *Journal of Atmospheric Sciences*, Vol. 20, No. 2, pp. 130-141, March 1963.