Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5585079, 7 pages
https://doi.org/10.1155/2021/5585079

Research Article

Design of a Cryptographic System for Communication Security using Chaotic Signals

Jai-Houng Leu,[1] **Jung-Kang Sun**,[2] **Ho-Sheng Chen**,[3] **Chong-Lin Huang**,[3] **Dong-Kai Qiao**,[3] **Tian-Syung Lan**,[3] **Yu-Chih Chen**,[4] **and Ay Su**[2]

[1]*Shandong Polytechnic, No.23000 Jin Ten East Road, Jinan, Shandong Province, China*
[2]*Department of Mechanical Engineering, Yuan Ze University, Taoyuan 32003, Taiwan*
[3]*College of Mechatronic Engineering, Guangdong University of Petrochemical Technology, Maoming, Guangdong 525000, China*
[4]*Aerospace Science and Technology Research Center, National Cheng Kung University, Tainan, Taiwan*

Correspondence should be addressed to Ho-Sheng Chen; hschen98.tw@gmail.com

Received 12 February 2021; Revised 6 April 2021; Accepted 12 May 2021; Published 27 May 2021

Academic Editor: Teen-Hang Meen

Disturbance or corresponding errors of the transmission of information affect the ability of error detection. The chaotic encryption system prevents errors and secures the transmission system safely. The security assures by updating chaotic signals with the parameters of the chaotic circuits which are frequently changed. The data decipher and the encryption by the chaotic signaling system renews and changes the initial condition of a chaotic electric circuit. When most of the decimal portions are less than the threshold, the transmission is accepted, and all the noninteger numbers are rounded to their nearest integers. The criterion allows the error-detection function in the security system that is proposed in this paper. The chaotic encryption system for information is applied to public channels by the authorized individual. Three pictorial examples transmitted in the proposed system successfully demonstrate the security and performance. The new system provides high efficiency in the satellite communication network.

1. Introduction

Communication via satellite has been a common way for information exchange since the twentieth century. New ways of communication such as distance education and video conferencing with mobile devices need satellite networks. Despite the easy and convenient transmission of the information, there is always a problem of protecting private and secret information. Illegal eavesdropping or wiretapping causes considerable loss of the users. As transmitted messages through the satellite are easily interfered with and tampered with, important data of the defense navigation or business messages may not be delivered appropriately. Therefore, communication security in satellite networks has been attracting increasing interest from industry and academia. In general, the encryption system adopts public (secret) key [1–4] or private key cryptography [5–7]. The former was introduced by Diffie and Hellman [1]. They designed a cryptosystem that uses the same private key for encrypting and decrypting. That is, two terminals share the same identification code for encrypting the cryptography of the private key by designing an encryption algorithm in the system as a data encryption standard (DES) [5]. The private-key cryptosystem provides strong security for public-key cryptosystem whose speed of authentication is slower than that of the private-key cryptosystem. Systems using satellite communication such as mobile devices and communication platforms for video conferencing usually use public (secret) keys.

Thus, how to protect important information in private key in the transmission is critical. Therefore, a new cryptographic technology for network security for satellite communication is required.

This research aims to propose a new system for the security of the satellite communication network by using a chaotic signal as a carrier and the Haar wavelets for multiplexing and demultiplexing. The proposed system is different from the conventional encryption algorithm as the

chaotic encryption system used for this study has a noncycle and complex time behavior. The new nonlinear method that uses the initial condition of a chaotic system as a private key masks the information-bearing signals by chaotic signals in the system (Figure 1). Then, the information is decrypted based on the carrier after it is accepted at the end of the transmission channel. The chaotic system transforms the private key of the system and the Haar wavelet by multiplexing and decrypts the key by the demultiplexing (Figure 2) [8]. This process finds out the transmission error easily and prevents the interception of information from the public channel. Thus, an effective way of satellite communication is obtained. The proposed system proves the effect of the divergence of a chaotic system which is suppressed according to the behavior of a nonlinear system in the new encryption scheme. The system provides a new security system of satellite communication network and protects the data and messages from various cyber attacks.

2. Methods

2.1. System Design. There are different projects that encode the public key since the public-key-encrypted project arose. Its safety always sets up the most complex mathematics problems. The encrypted key and cracked key in the symmetric encryption system are the same key. The major problem is that how the sender transmits the encrypted key to the receiver in safety after the information was encrypted, and let both share the secret key to decode it. If we use the key list in a trusted Internet, maybe we can solve this problem [9].

Through the encryption algorithm, we can do every kind of replacement to plaintext, and the input to encryption algorithm is the secret key. The key is unrelated data to plaintext; we use the key not only to encrypt the plaintext but also to crack the ciphertext. That is, we use the same secret key to encrypt or crack the text in the symmetric encryption system, so the transceiver must own the same key. Therefore, how to transmit the key to the receiver validly and guard the information against hackers is an important problem. [10, 11].

Everyone has a public key and private key in the asymmetric encryption system. The private key must be kept by an individual carefully. Under the asymmetric encryption system, every participator can get everyone's public key and own his own private key, so the private key does not need be transmitted in the net. If the public key encrypted one message, then it must be cracked by the private key, and vice versa.[12].

The state trajectory of a chaotic system is indeterminable. Thus, the divergence of nearby trajectories causes any small error to be magnified as the equations are integrated with the specified initial conditions. Even a small effect affects the system in a long term. The sensitivity of the system depends on initial conditions in the chaotic behavior of the system. The effect of the divergence of a chaotic system is suppressed in a nonlinear system where a message of plain texts is converted into a Haar wavelet form by the encoder matrix. It gives not only an encrypted message but also a transmitted error checking [13]. The Haar wavelets signal can be carried by one state of the chaotic signals (Figure 3). Then, it is sent to a public channel, decrypted at the receiving end, and demultiplexed by using the decoder matrix. The method uses the initial conditions of a chaotic system as a private key in addition to the Haar wavelet transform for multiplexing and demultiplexing to form the nonlinear system. The messages are securely encrypted, and its transmission errors are easily detected. No one can decrypt the intercepted messages from a public channel without the private key. The Haar wavelet of information in Chua's circuit is transmitted to a public channel as it is decoded at the end of communication by a demultiplexer. The process is presented in Figure 3. The security of the system is decided by the initial condition of the chaotic signal of the information. The original information is transformed by the Haar wavelet by the encoder matrix.

2.2. Encryption. Encrypting the chaotic cryptosystem is carried out according to the following steps:

(1) First, both the transmitter and the receiver are assigned to have the same private key that contains the chaotic parameters (α,β, a, b), the initial conditions (x_0, y_0, z_0), and the rank of the encoder matrices $\boldsymbol{H}_{\mathbf{n}}$

(2) The transmitter obtains the plaintext data **[C]** and calculates $[\mathbf{m}] = [\mathbf{C}] * \mathbf{H}_n$

(3) It generates the signal states of (**X** or **Y** or **Z**) on a fixed time interval in x, y, and z channels in Chua's circuit using the parameters in step 1

(4) When $\hat{\mathbf{Z}} = Z + [\mathrm{m}]$, a chaotic signal of chaotic masking denotes and transmits $\hat{\mathbf{Z}}$ to the receiver

(5) The transmitter calculates the new chaotic parameters as follows:

$$\begin{cases} \alpha' = f(\alpha), \\ \beta' = f(\beta), \\ a' = f(a), \\ b' = f(b), \\ x_0' = f(x_0), \\ y_0' = f(y_0), \\ z_0' = f(z_0), \end{cases} \tag{1}$$

where $f()$ is a collision-free one-way function [7, 14] for both ends of the transmitter and receiver

For example,

$$f(x) = \left(a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_1 x + a_0\right) \bmod p. \tag{2}$$

If the transmitter sends the next frame message, steps 2~6 should be repeated. The receiver obtains the encrypted messages $\hat{\mathbf{Z}}$ from the public channel and uses the following procedures for decryption.

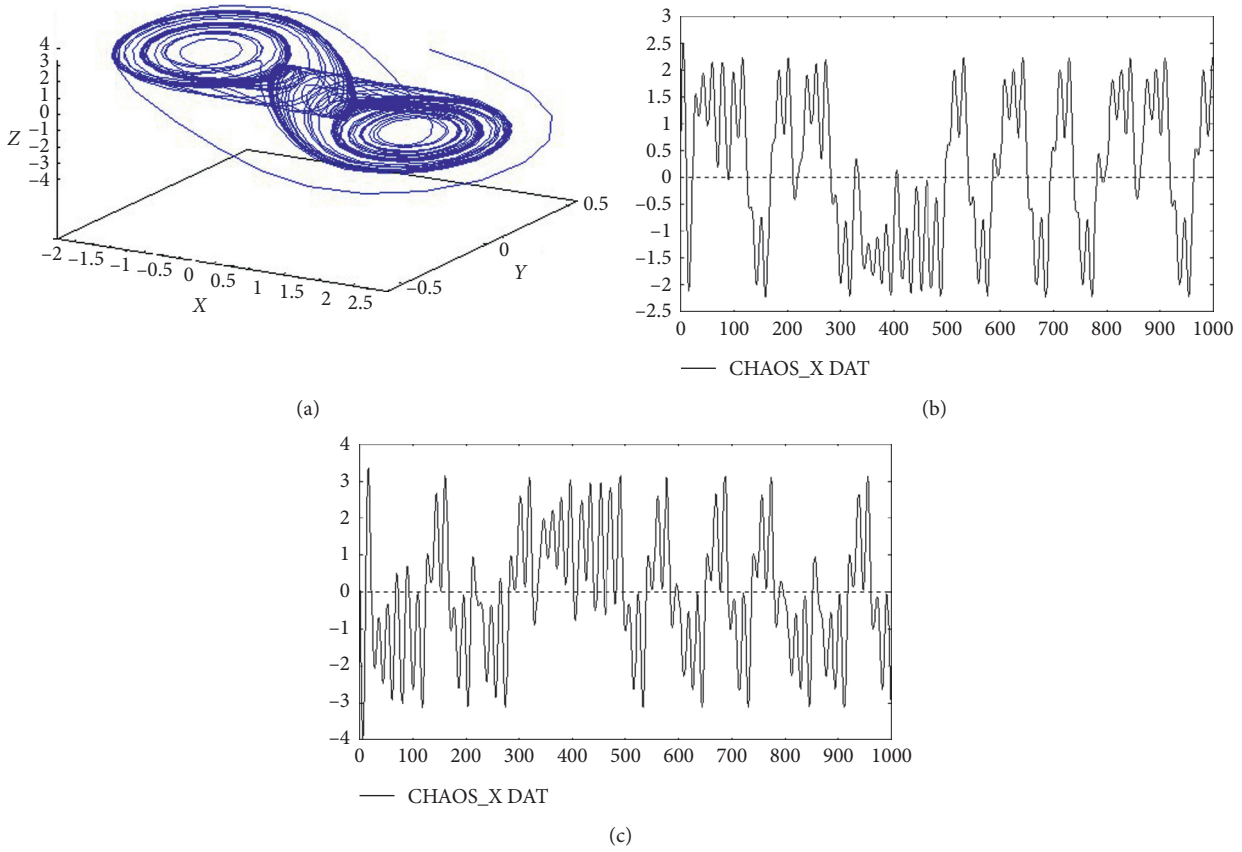


Figure 1: Information-bearing signals with chaotic signals. (a) Double scroll chaotic signal. (b) X channel. (c) Z channel.

2.3. Decryption

(1) $\hat{\mathbf{Z}}$ arrives at the receiver.

(2) The receiver generates a state variable Z by using the same parameters as in step 1.

(3) The ciphertext $[\mathrm{m}] = \hat{\mathbf{Z}} - Z$ is calculated.

(4) $[\mathrm{C}] = [\mathrm{m}]\mathrm{H}^{-1}{}_{\mathrm{n}}$ is defined.

(5) If this cipher message $[C]$ contains noninteger numbers and the difference between the noninteger numbers to their nearest integers is larger than a threshold, then the transmitted message may have been interfered with by noise disturbances or communication error. In this case, the receiver requests the transmitter to send the message again. Otherwise, the transmission is considered to be successful.

(6) The receiver calculates the chaotic parameters as in equation (1).

The Haar wavelet transform is carried by one of the chaotic signal states ($x(t)$, y(t), or z(t)) in Chua's circuit (Figure 4). Then, it is sent to a public channel, decrypted at the receiver, and demultiplexed by using the decoder matrix. The changing private key alters the transmitted messages in the public channel and contains the parameters of Chua's circuit and the rank of the encoder matrix. As the plaintext data $[C]_n$ and the encoder matrix H_n are both integers, the ciphertext [m] contains only integer numbers. This property allows a convenient detection of redundancy when the masked message Z is corrupted during transmission. For example, network disturbances in computers of heavy load and frequent on-off operations and external electromagnetic fields may contaminate the messages.

3. Results and Discussion

We use the seven chaotic parameters (α, β, a, b, x_0, y_0, and z_0) and the dimension of matrix n as the "encryption keys." The cyber attacker cannot decrypt the encrypted message unless the chaotic behavior is understood as the original signals are carried by the chaotic signals during transmission. The control parameters of chaotic behavior constantly change in the collision-free one-way function. As a result, the security property results in a high sensitivity of synchronization with the parameter change. Therefore, understanding the chaotic behavior of the chaotic parameters that change in each transmission is required for decryption. In other words, the system is secured as long as the first chaotic parameters are kept secret. To decrypt the encrypted data, the encryption key of the system is demanded to synchronize the signal [14].

In the other words, the modulation-demodulation requires the system to spend much time, and the message is not decrypted without a correct key. For updating other parameters such as the encoder matrix order, initial

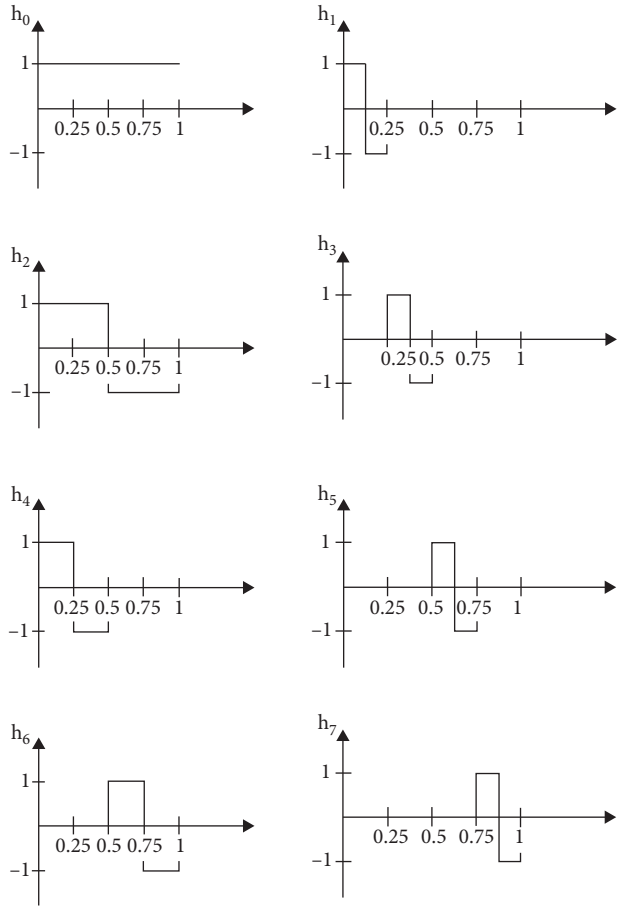


Figure 2: The Haar wavelet transform.

conditions of chaotic circuits, coefficients, and prime number in equation (1), communication security needs enhancement, which is realized in this research. Besides the safety of secret messages, this system also enhances communication efficiency and improved performance for the secured communication. For any disturbance or communication error, the received message contains noninteger numbers that are easily detected, which improves the capability for error detection. It is important to exactly estimate the unknown parameters of chaotic systems in chaos control and synchronization. Hu et al. presented a method for estimating a one-dimensional discrete chaotic system based on the mean value method (MVM) by exploiting the ergodic and synchronization features of the chaos. This research proposed a method that estimates the parameter value more accurately than the MVM [15].

The suggested chaotic parameters can be any integers between −32767 and 32767, and the possible combination of keys is $(32767)^7 \times 2^7 \times [(I+1)!-1]$. As it takes 10^{-9} seconds for one calculation, this is beyond the capability of the existing supercomputers. The total time needed for solving the message is up to 2.83×10^{22} years. The number of keyspace reaches 1.88×10^{39} if the rank of encoder/decoder matrix is set to be eight including seven independent variables and one dependent function. The variables are chaotic parameters (α, β, a, and b), the initial conditions (x_0, y_0, and z_0) on which the rank of the encoder matrices is based. This private key that contains the parameters of Chua's circuit and the rank of the encoder matrix changes constantly to alter the appearances of the transmitted messages in the public channel. As integers, the plaintext data $[C]_n$ and the encoder matrix H_n result in ciphertext **[m]** of only integer numbers. This property offers a convenient way to detect whether the masked messages **Z** are corrupted during transmission. JAVA codes of the proposed algorithm were tested successfully on two remote machines. Of course, the ideal encryption should be robust so that the transmitted messages in the public channel are not decrypted by an unauthorized person.

The results are shown in Figure 5 based on JAVA codes of the proposed algorithm. Heavy-loaded computer networks, on-off operations of computers, and external electromagnetic fields cause disturbances to corrupt messages. If the disturbances are large, the messages decrypted by the receiver contain nonintegers. The receiver then becomes aware of obtaining a corrupted message and requests retransmission immediately. However, decrypted messages with nonintegers need caution; they are false transmissions. In the algorithm, the chaotic signals with nonintegers of floating parts can be introduced during the masking and unmasking. Also, when computers or the operating systems of the transmitter and the receiver are not the same, this

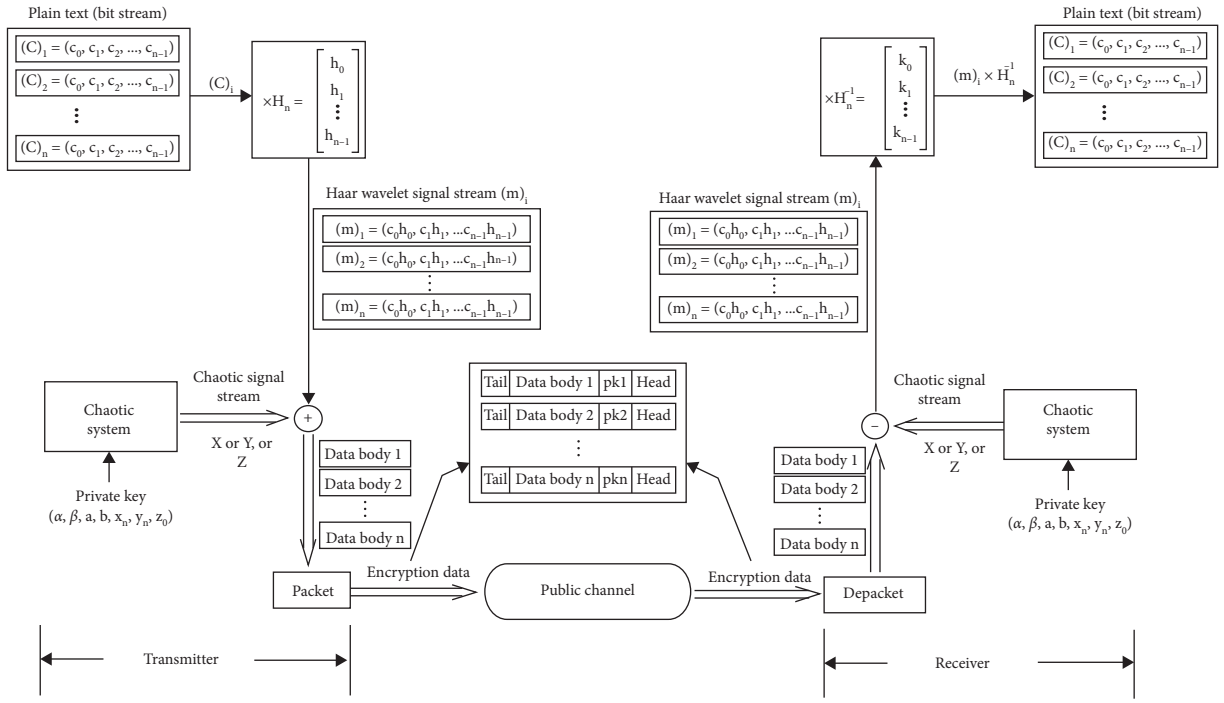


Figure 3: The diagram of a chaotic cryptosystem.

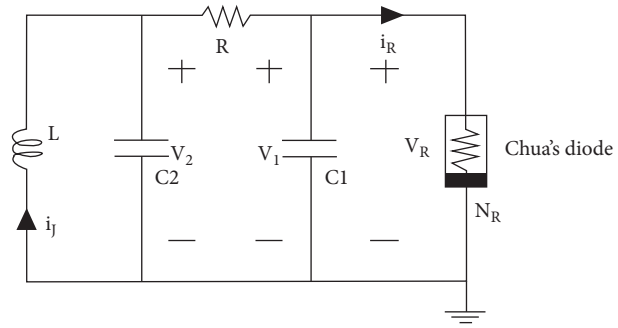
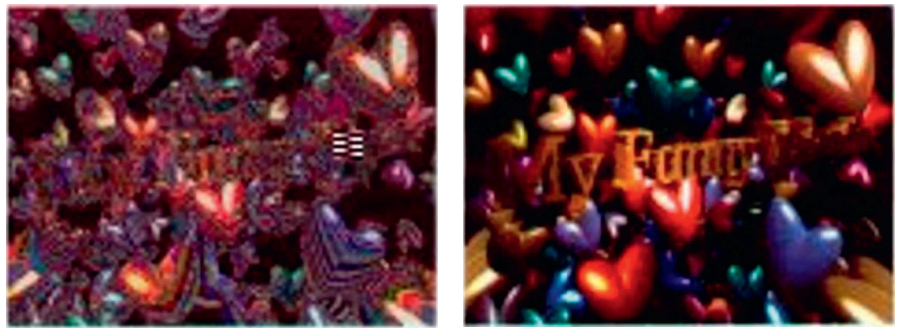


Figure 4: Chua's circuit.

(a) (b)

Figure 5: Continued.



(c) (d)

Figure 5: The results of "many hearts" signals transmitted by chaotic parameters. (a) Original signal, (b) chaotic signal, (c) encryption signal, (d) recovery signal.

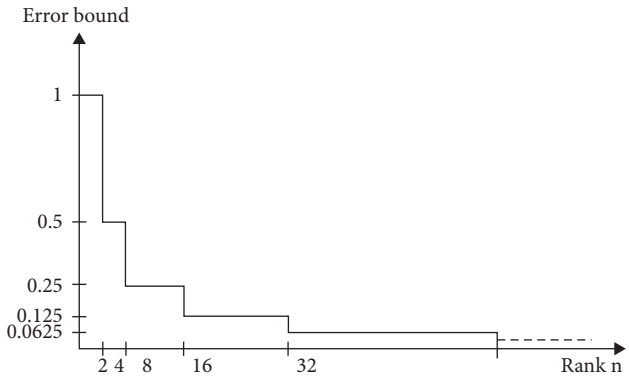


Figure 6: Threshold of the error bound (the x-axis) and the rank of the encoder matrix (the y-axis).

creates decimal parts. Therefore, to remedy the possible situation for misinterpreting, a threshold regarding the magnitude of the decimal part is required for error detection.

The behavior of the Haar wavelet form is aperiodic. It is not complex like a random signal or a noise that needs time and an algorithm to distinguish signals and noises. The plaintext message is converted into a Haar wavelet form by the encoder matrix and sets the criterion for filtering. That is, there is a convenient criterion from the Haar wavelets to check and filter the transmitted error. Since a fitting error of approximating any function by the Haar wavelet form is a reciprocal of the highest-order Haar function, we selected a threshold (or an error bound) as the reciprocal of the rank of the encoder matrix. In this way, the transmission becomes acceptable and all the noninteger numbers are rounded to their nearest integers if most of the decimal parts are less than the threshold. With this simple criterion, the error-detection function in the proposed system is established. In this case, the threshold is equal to $1/n$ as shown in Figure 6.

4. Conclusions

The importance of communication security is becoming critical as the number of satellites is increasing. Thus, preventing transferred information from eavesdropping or wiretapping has been attracting much interest. New cryptographic technology for the security of the satellite communication network is proposed by using a chaotic signal as a carrier and the Haar wavelets for multiplexing and demultiplexing. The proposed system allows secure encryption of messages and easy detection of errors. Three pictorial examples were tested in the system, and the result validated the performance and security of the system. The system has the following four advantages: (1) simplicity and low cost as it runs on PCs by implementing the algorithm, (2) high security, (3) secure authentication, and (4) easy detection of transmission errors. The JAVA code of the proposed algorithm was also tested and operated successfully on two remote machines. The result shows that the proposed system is available for individual, academic, or industrial purposes conveniently. The result of the system leads to further research on the encryption and decryption of messages including plaintexts, voice, pictures, or their combination for multimedia purposes.

Data Availability

The data used to support the findings of this study are restricted by Jai-Houng Leu in order to protect PATIENT PRIVACY. Data are available from Jai-Houng Leu (jahonleu@yahoo.com.tw) for researchers who meet the criteria for access to confidential data.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] T. E. Gamal, "Design of universal test sequences for VLSI," *IEEE Trans. Inf. Theory*, vol. 31, p. 469, 1985.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[4] M. O. Rabin, MIT Laboratory of Computer Science, Technical Report MIT/LCS/TR-212, 1979, https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=45711.
[5] E. L. Richardson, E. O. Vetter, B. Ancker-Johnson, and E. Ambler, Data Encryption Standard. FIPS PUB National Bureau of Standards, Washington D.C., 1977, https://csrc.nist.gov/CSRC/media/Publications/fips/46/archive/1977-01-15/documents/NBS.FIPS.46.pdf.
[6] W. M. Daley and R. G. Krammer, *Data Encryption Standard (DES)*, National Institute of Standards and Technology, Gaithersburg, Maryland, 1999, https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf.
[7] X. Lai and J. L. Massey, *Proc*, Advances in Cryptology Eurocrypt, 1992, https://link.springer.com/chapter/10.1007/3-540-47555-9_5.
[8] A. Haar, "Zur Theorie der orthogonalen Funktionensysteme," *Mathematische Annalen*, vol. 69, no. 3, pp. 331–371, 1910.
[9] Zhang Chengxin, 1997, https://www.elsevier.com/books/computer-and-information-security-handbook/vacca/978-0-12-803843-7.
[10] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 67, no. 3, p. 644, 1976.
[11] W. Diffie and M. Hellman, "New directions in cryptography," *IIEEE Transactions on Information Theory*, vol. 22, no. 6, p. 654, 1976.
[12] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[13] K.-S. Hwang, "Long-yeu chung, isaac yuchih chen , reducing the cost of spacecraft ground systems and operations," *Part of the Space Technology Proceedings Book Series*, vol. 3, p. 421, 1988.
[14] Y. Zhery, T. Matsumoto, and H. Imai, "Impossibility and optimality results on constructing pseudorandom permutations," *Lecture Notes in Computer Science,Advances in Cryptology-EUROCRYPT*, vol. 89, pp. 412–422, 1990.
[15] J. Hu, H. Li, and J. Li, "Parameter Estimation of a Class One-Dimensional Discrete Chaotic System," *Discrete Dynamics in Nature and Society*, vol. 2011, Article ID 696017, 9 pages, 2011.