Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 6661550, 12 pages
https://doi.org/10.1155/2021/6661550

Research Article

Realization of a Secure Visible Light Communication System via Chaos Synchronization

Teh-Lu Liao,[1] **Chih-Yung Chen**,[1,2] **Hsin-Chieh Chen**,[3] **Yung-Yi Chen**,[1] **and Yi-You Hou**[4]

[1]*Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan*
[2]*Department of Computer Science and Information Engineering, Shu-Te University, Kaohsiung, Taiwan*
[3]*Department of Biomedical Engineering, Hungkuang University, Taichung, Taiwan*
[4]*Department of Intelligent Commerce, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan*

Correspondence should be addressed to Yi-You Hou; yyhou@nkust.edu.tw

Received 3 December 2020; Revised 5 January 2021; Accepted 22 January 2021; Published 8 February 2021

Academic Editor: Viet-Thanh Pham

A novel technique for transmission of information through visible light communication (VLC) is developed in this study. A light-emitting diode is used as the light source at the transmitting side to send the encrypted information. At the receiving side, a light sensor, OPT-101, is used to receive the light signals that carry the encrypted information. The Arduino Due microcontroller board is used for digital signal processing at both the transmitting and receiving sides. Furthermore, to prevent the transmitted message from being intercepted, two chaotic systems, a master and a slave, with a synchronization controller are designed to obtain the transmitted audio signals. The design enables not only a VLC system with the light transmission path as a straight line (so that data cannot be stolen) but also the encryption of the audio signals with the chaotic system (Rössler system) to enhance data transmission security. The effectiveness of this system is then experimentally verified.

1. Introduction

Advancements in information technology have enabled the development of fast wired transmission and wireless transmission methods, such as Ethernet, serial communication, Bluetooth, and Wi-Fi, which are now commonly used in daily life. However, regardless of the communication method used, in addition to the requirements of high-speed transmission, low power consumption, strong stability, wide communication range, and other performance parameters, the focus of information transmission has shifted to communication security. Therefore, related encryption methods, such as Rivest–Shamir–Adleman encryption [1], ElGamal encryption, Paillier encryption [2], and the chaos-based encryption (Rossler system) [3], have been proposed.

Visible light communication (VLC) uses light-emitting diodes (LED) to send out high-speed light and dark flashing signals to transmit data, it can reach 500 Mbit/s, and the transmission distance can reach 1 to 2 kilometers, which can be used as a local area network technology. Nowadays, it is used in applications such as unidirectional indoor broadcasting system [4] or indoor positioning [5]. Voice signal transmission over distant places through VLC [6] is a critical topic of research.

For security considerations, in the proposed technique, the signal that carries crucial information is encrypted. A chaotic system that is characterized by a dynamic system, which is very sensitive to the initial value [7] and can only be decrypted after the system is synchronized [8], was used in the proposed system. The proposed system increases communication security. Here, the Rossler system is mainly used for secure communication [3]. The system contains a transmission device and a receiving device, which function as a master and a slave, respectively. A controller is designed to synchronize the master and slave systems and decrypt the encrypted transmitted audio signals. Many synchronization design methods are available for chaotic systems [9–13]. Different from the implementation methods proposed in other documents [14–16], the main purpose of this manuscript is to transmit through VLC. Because of the analog

transmission through the LED, the data is not easy to be stolen. In order to enhance its security, we encrypt it through a chaotic system, design a set of channel modulation methods to enable it to successfully synchronize and decrypt, and strengthen its confidentiality. In this study, we adopted the proportional integral derivative (PID) controller for synchronization [17, 18]. The state error of the master and slave systems is used as the PID input, and suitable PID parameters are used to ensure that the system quickly achieves synchronization to complete the decryption.

2. Research Methods

2.1. Simulation and Synchronization of Chaotic Systems. Because security of information is critical, the transmission signal is encrypted to increase communication security. The Rossler chaotic system is mathematically expressed as follows:

$$\begin{cases} \dfrac{\mathrm{d}x(t)}{\mathrm{d}t} = -y(t) - z(t), \\ \dfrac{\mathrm{d}y(t)}{\mathrm{d}t} = x(t) + ay(t), \\ \dfrac{\mathrm{d}z(t)}{\mathrm{d}t} = b + z(t)(x(t) - c), \\ \text{where } a = b = 0.2, c = 5.7. \end{cases} \tag{1}$$

In the matrix form, it is described as follows:

$$\begin{bmatrix} \dfrac{\mathrm{d}x(t)}{\mathrm{d}t} \\ \dfrac{\mathrm{d}y(t)}{\mathrm{d}t} \\ \dfrac{\mathrm{d}z(t)}{\mathrm{d}t} \end{bmatrix} = A \begin{bmatrix} x(t) \\ y(t) \\ z(t) \end{bmatrix} + B[0.2 + x(t)z(t)], \tag{2}$$

where $A = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ 0 & 0 & -5.7 \end{bmatrix}$ and $B = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

Here, x, y, and z are the three states of the chaotic system. Because these states can be implemented in the transmission system, the chaotic system is then discretized. By applying a sampling time (T) of 25 ms, the discrete time system can be obtained as follows, where k is the time index:

$$G = e^{AT}, \; H = (G - I_3)A^{-1}B, \tag{3}$$

where $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

$$\begin{bmatrix} x^{(k+1)} \\ y^{(k+1)} \\ z^{(k+1)} \end{bmatrix} = G \begin{bmatrix} x^{(k)} \\ y^{(k)} \\ z^{(k)} \end{bmatrix} + H\left[0.2 + x^{(k)}z^{(k)}\right], \tag{4}$$

where $G = \begin{bmatrix} 0.9997 & -0.0251 & -0.0233 \\ 0.0251 & 1.0047 & -0.0003 \\ 0 & 0 & 0.8672 \end{bmatrix}$ and $H = \begin{bmatrix} -2.9815 \times 10^{-4} \\ -2.5171 \times 10^{-6} \\ 0.0233 \end{bmatrix}$.

After successful discretization of the chaotic system, the initial value of the given chaotic system is obtained as $x^{(0)} = 5$, $y^{(0)} = 6$, and $z^{(0)} = 14$ through MATLAB simulation. The chaotic signal characteristics of (x, y), (x, z), (y, z), and (x, y, z) are displayed in Figure 1.

Because chaotic systems are susceptible to initial values, if the initial values at the transmitting and the receiving sides differ, accurate decryption depends on the synchronization controller. In this study, the state variables of the chaotic system at the transmitter are defined as $x_m^{(k)}$, $y_m^{(k)}$, and $z_m^{(k)}$ with the initial value $x_m^{(0)} = 5$, $y_m^{(0)} = 6$, and $z_m^{(0)} = 14$, where k is the time index, and the state variables of the chaotic system at the receiver are defined as $x_s^{(k)}$, $y_s^{(k)}$, and $z_s^{(k)}$ with the initial value $x_s^{(0)} = -4$, $y_s^{(0)} = 7$, and $z_s^{(0)} = 3$, for synchronizing both the transmitter and the receiver with different initial values. Since the chaotic system is easily affected by the initial value and causes the system to be unstable, this manuscript selects the abovementioned initial values that can prevent the system from diverging as the simulation parameters. A PID controller is selected because of its simplicity, convenience, and strong robustness. The proportional controller (K_P) can speed up the response speed of the system, improve the accuracy of the system adjustment, and reduce the system response time. This allows the chaotic system to quickly catch up with the master state when the state error between the master and slave is large. The integral controller (K_I) considers the past error and controls the state to eliminate the steady-state error, but because the steady-state error is less than a certain value when synchronizing, it does not affect subsequent decryption. Furthermore, if the integral control is improper, overshoot may occur. Therefore, integral control was not adopted in the synchronous design. The differential controller (K_D) can consider future errors and achieve advanced control, which can improve system stability, reduce synchronization time, and avoid system overshoot. The state error of the master and slave formula is defined as $e^{(k)} = x_m^{(k)} - x_s^{(k)}$, and the PID controller is $u^{(k)} = K_P e^{(k)} + K_I \sum_{i=1}^{k} e^{(i)} + K_D(\Delta e^{(k)})$, where $K_P = -0.05, K_I = 0$, and $K_D = -0.7$. The control input $u^{(k)}$ is applied in the chaotic system at the receiver, which is expressed in (5). Then, some numerical simulations via MATLAB are performed to demonstrate the system performances. The state relations and errors between the transmitter and the receiver without the controller are displayed in Figures 2 and 3. We then apply the PID controller to synchronize the master and slave systems. The state relations and errors between the transmitter and the receiver with the proposed PID controller are displayed depicted in Figures 4 and 5, which verify the chaotic synchronization is obtained:

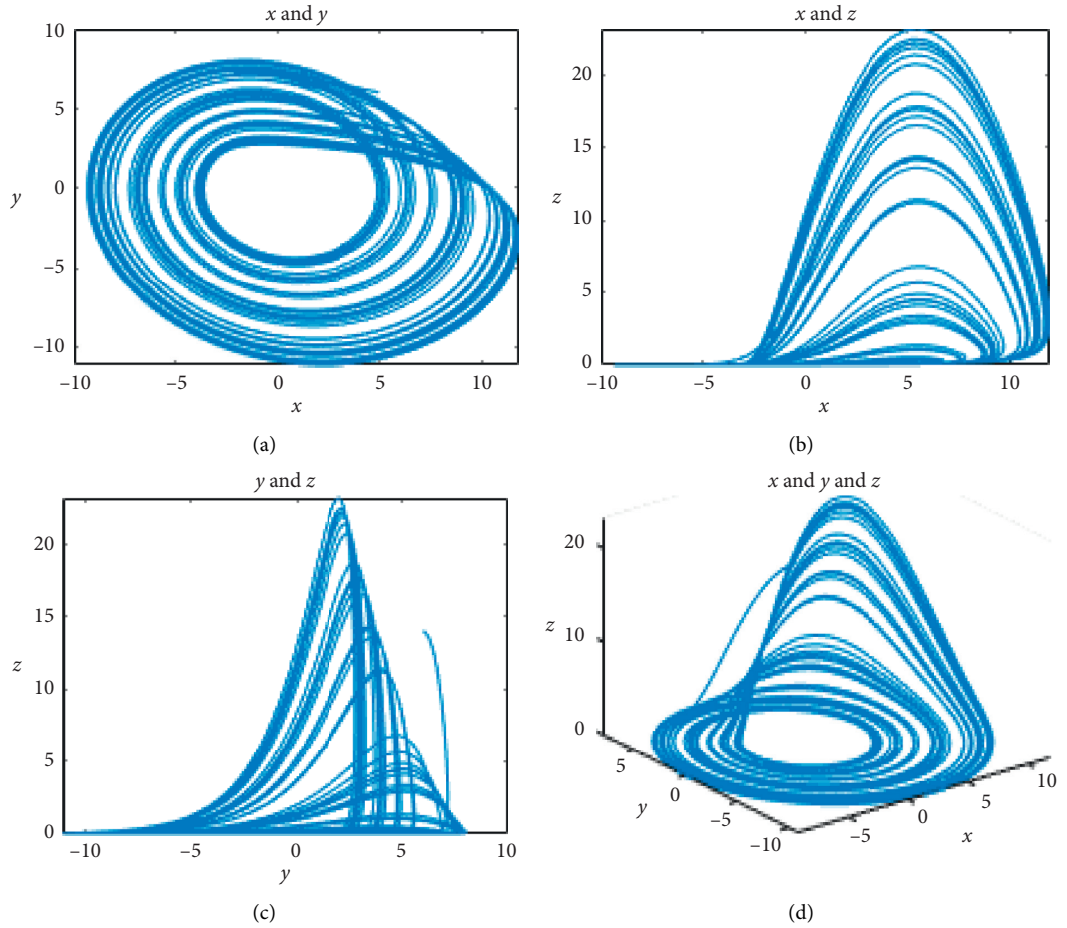

Figure 1: State characteristics of the Rossler chaotic system.

$$\begin{cases} e^{(k)} = x_m^{(k)} - x_s^{(k)}, \\ u^{(k)} = K_P e^{(k)} + K_I \sum_{i=1}^{k} e^{(i)} + K_D\left(\Delta e^{(k)}\right), \\ x_s^{(k+1)} = 0.9997 x_s^{(k)} - 0.0251 y_s^{(k)} - 0.0233 z_s^{(k)} + u^{(k)}. \end{cases} \tag{5}$$

2.2. VLC System Architecture. VLC hardware implementation is divided into two parts: the transmitter and receiver. The Arduino Due microcontroller board is the main control core of the system hardware. As to audio MP3 signals, the sampling frequency should be at least 44.1 MHz. The Arduino Due microcontroller board used in this article has a crystal oscillation frequency of 84 MHz, 12-bit input, high operation speed, and resolution ability, which are sufficient for the audio signal processing. The analog to digital (A/D) and digital to analog (D/A) conversions used in signal processing are processed internally by Arduino Due microcontroller board. The A/D convertor has the fastest conversion rate of 1 MHz, and the D/A processor performance can reach approximately 1.74 MHz, which is sufficient to process and encrypt/decrypt music signals. In the encryption, we add the state of the chaotic system to the audio signal for encryption. In the decryption, after the channel modulation and synchronization, we only need to subtract the state of the chaotic system from the ciphertext, and we can obtain the original signal. To improve the signal strength, the transmitter was combined with PAM8403, and the receiver output was combined with the LM386 amplifier to increase the signal strength. The working voltage of the transmitter is in the range of 2.5–5.5 V. The maximum gain of the system is 24 dB. The working voltage range of the receiver is 4–12 V. A maximum gain of 26 dB can be obtained. The LED is an RGB LED lamp with a diameter of 5 mm with a working voltage range of 2–3.2 V. The power of the LED is 0.06 W. The working voltage of the optical receiver OPT-101 is 2.7–36 V. The receiver converts the intensity of the received light to different voltages. A 1-MΩ feedback resistor with a bandwidth of 14 kHz is placed inside the receiver. The internal resistance of the speaker (horn) is 8 Ω, and its power rating is 0.3 W. System architectures of the transmitter and the receiver of the VLC system are given in Figures 6 and 7, respectively.

3. Experimental Results and Discussion

3.1. Realization of Signal Transmission by Using Visible Light. In this study, an MP3 signal is used as the transmission signal. The transmitter converts the music signal ($m^{(k)}$)

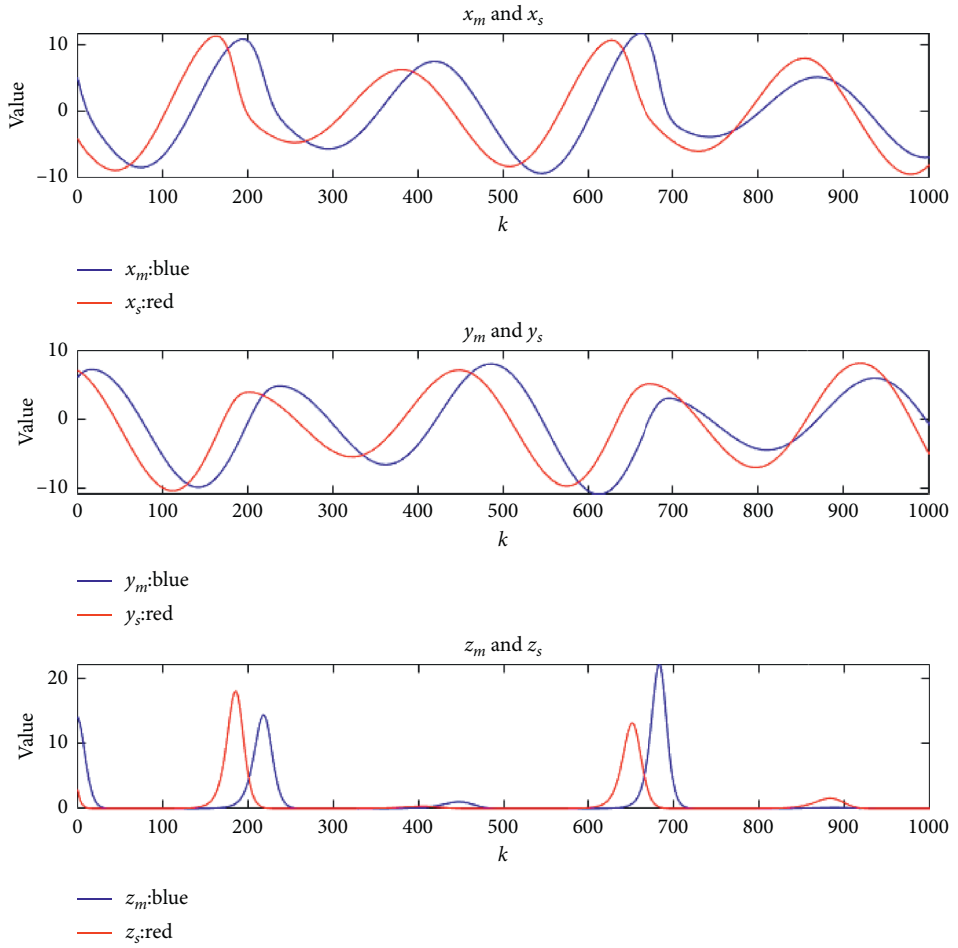

Figure 2: Unsynchronized status at the transmitter and receiver.

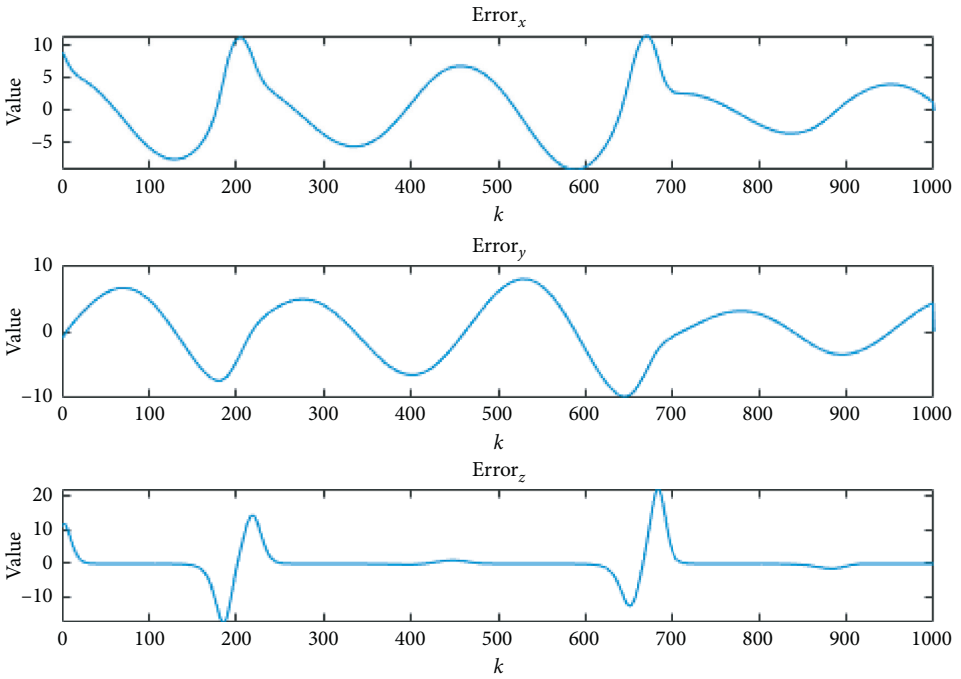

Figure 3: Unsynchronized error of the transmitter and receiver.

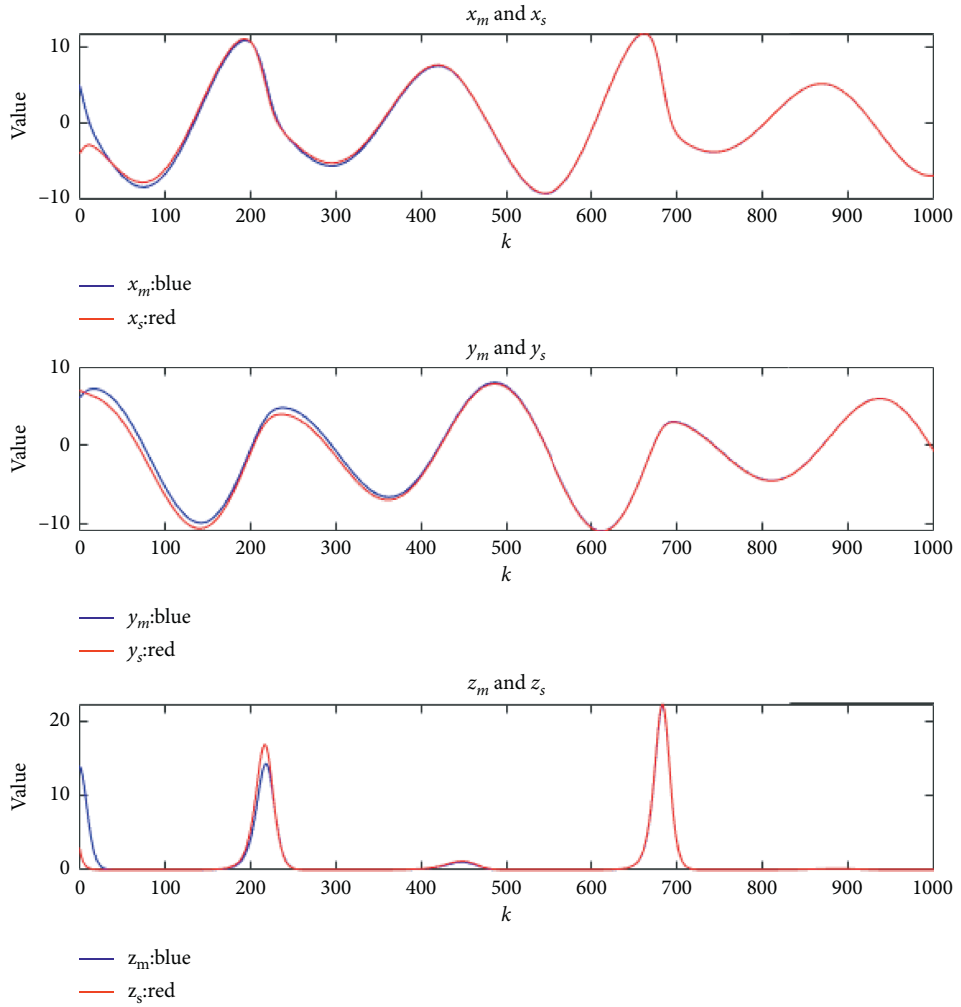

Figure 4: Status of the synchronization process at the transmitter and receiver.

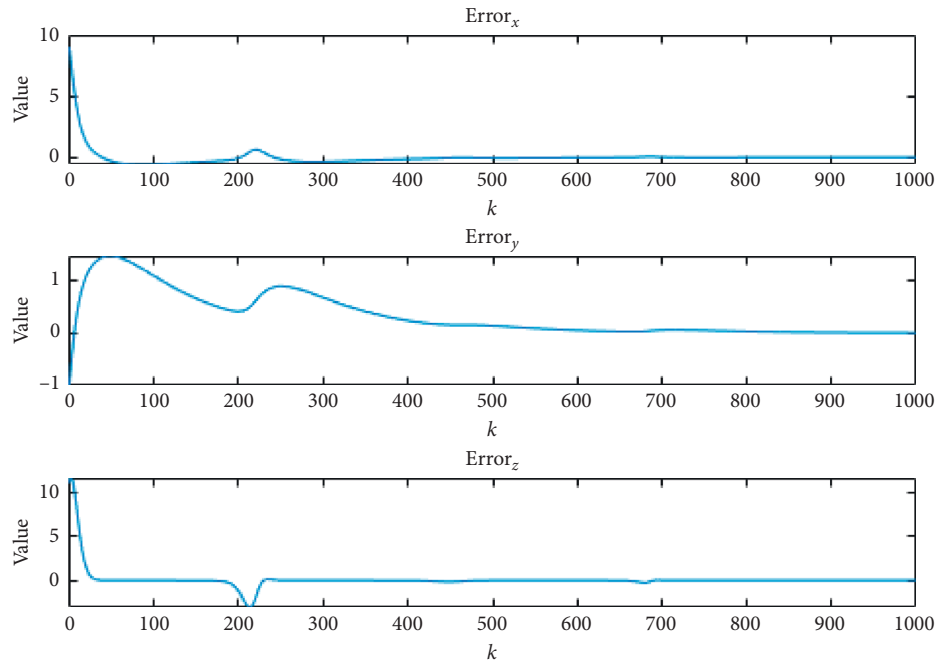

Figure 5: Error trajectory of the synchronization process at the transmitter and receiver.

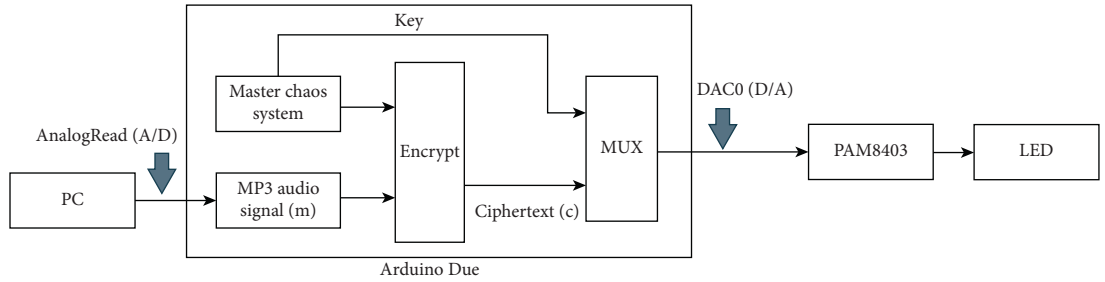

Figure 6: System architecture of the transmitter of the VLC system.

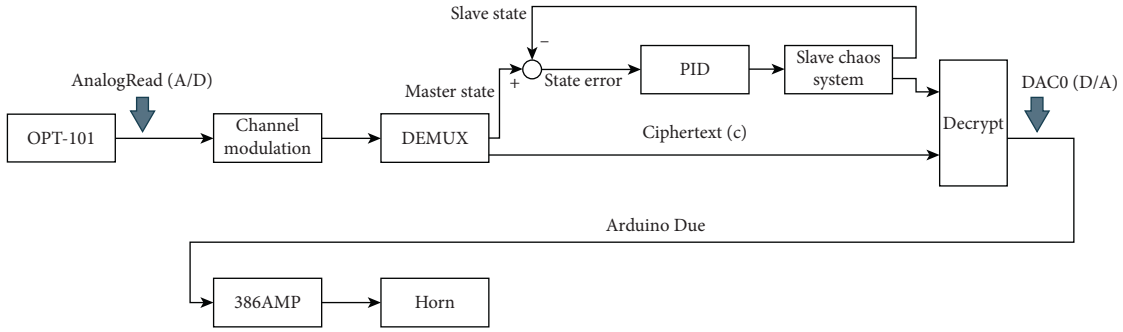

Figure 7: System architecture of the receiver of the VLC system.

played by the computer through the analogRead function of Arduino Due microcontroller board (A/D), where k is the time index. Then, the music signal is converted to an analog signal (D/A) through the analog output pin DAC1. The A/D in Arduino Due microcontroller can withstand a voltage of 5 V and convert it to a 12-bit digital signal, so the numerical resolution range is 0–4095 (unit), and the accuracy of each unit is $5\,\text{V}/4096 = 1.22\,\text{mV}$, and the same is true for D/A. Then, the PAM8403 amplifier is used to drive the LED for transmission, and the MP3 audio signal is transmitted to the receiver, as depicted in Figure 8.

The receiver uses an optical sensor module (OPT-101) to receive the LED signal of the transmitter and then quantize the audio signal. The signal receiver also receives the music signal at the same time through the A/D convertor. After signal processing (as presented in Figure 9), the signal is converted by the D/A convertor, whose output functions as the input to the amplifier (386AMP), and the audio signal is played by the speaker. The actual hardware implementation is displayed in Figure 10. Although VLC was realized using digital signals, the output was analog. At the receiver, the noise caused by external interference factors and channel length modulation can be removed using a filter.

3.2. Ensuring Security of Data Transmission. To ensure the security of data transmission, a chaotic synchronization control system is used to encrypt and decrypt transmitted data. To avoid data breach, the difference between the frequency band of the transmitted data and the frequency band of the chaotic system is minimized. The fast Fourier transform (FFT) is used to observe the frequency band distribution. As displayed in Figure 11, a suitable chaotic system is used to ensure security of transmission data. The fast Fourier analysis of the chaotic signal is displayed in Figure 12. With this design, even if the data are stolen at the transmitter, the data cannot be easily decrypted, which strengthens the system security.

3.3. Function of Audio and Chaotic Signals. The 12-bit ADC resolution from analogRead function between value 0 and 4095 (unit) of Arduino Due microcontroller is used in the signal transmitter to read the audio signal ($m^{(k)}$) played by the computer to complete the A/D conversion, and then, the audio signal is encrypted by the chaotic system into a ciphertext ($c^{(k)}$) according to (6). Figure 13 displays the encrypted signal. Furthermore, the ciphertext is converted from the digital to analog signal, and then the amplifier is used to improve the signal strength to drive the LEDs for transmission. The receiver receives the ciphertext signal ($C^{(k)}$) through the OPT101 module, as displayed in Figure 14. The signal receiver receives the encrypted signal ($C^{(k)}$) through OPT-101 and transmits it to Arduino Due microcontroller through analogRead:

$$c^{(k)} = m^{(k)} + 50x_m^{(k)}. \tag{6}$$

Considering channel modulation, the relationship between the value of the ciphertext at the transmitter ($c^{(k)}$) and the value of the ciphertext signal at the receiver ($C^{(k)}$) is established under conditions to avoid external interference, as displayed in Table 1. To decrypt the received signal, the receiver value is converted into original information:

$$c'^{(k)} = 500 + 2.5\left(C^{(k)} - 2200\right), \tag{7}$$

where $c'^{(k)} = c^{(k)}$.

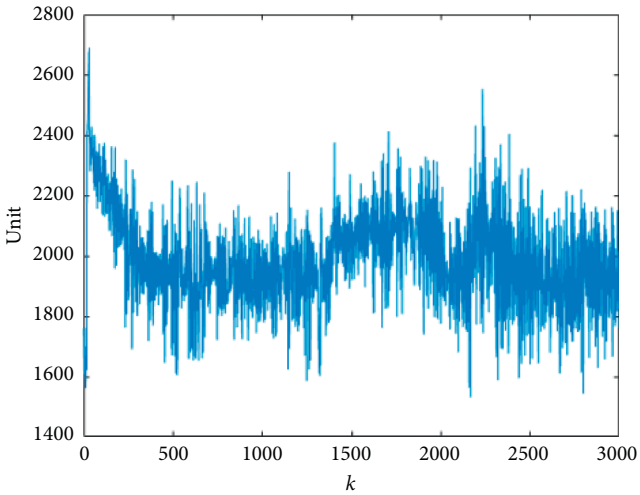

Figure 8: MP3 audio signal processing at the output of the signal transmitter.

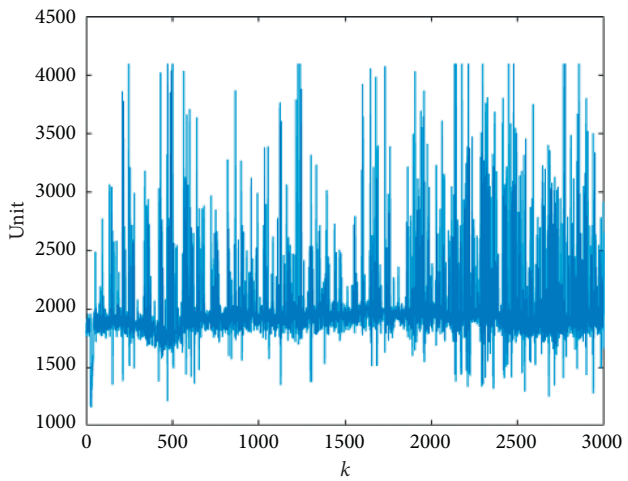

Figure 9: Signal receiver output display.

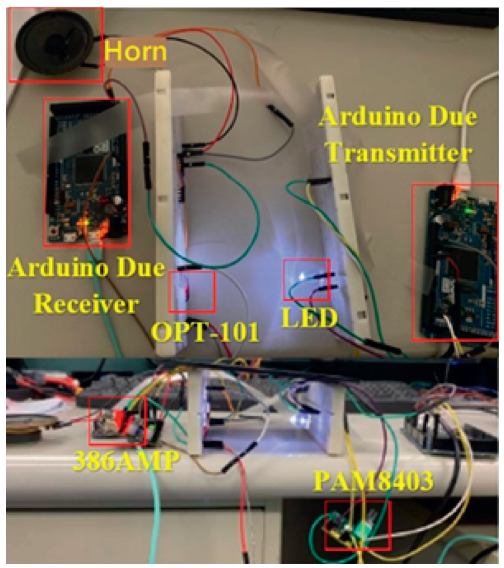

Figure 10: VLC system prototype and hardware.

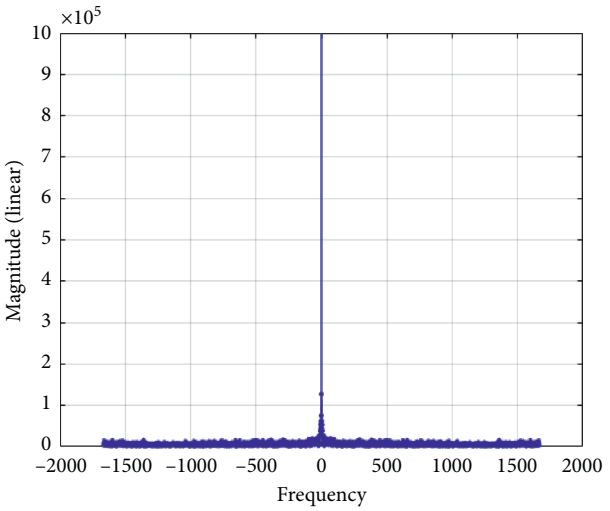

Figure 11: Analysis of audio signals by using FFT.

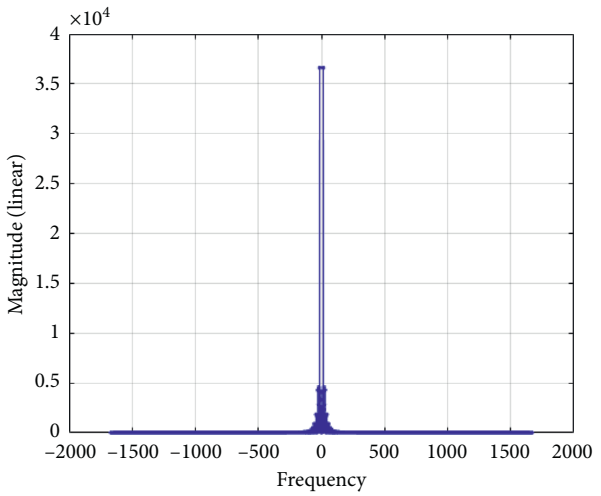

Figure 12: Analysis of chaotic signals by using FFT.

Immediately after converting the value back to the original information, the ciphertext was decrypted using the chaotic signal that is synchronized with the transmitter, as expressed in (8). Thus, the original music is obtained. Figures 15 and 16 display the results of the decryption of the unmodulated signal and the modulated signal, respectively.

To ensure the feasibility of the channel modulation and decryption proposed in this manuscript, we transmit some data through VLC, and the value is shown in Figure 17. And, then, we observe the received data; it can be found in Figure 18 that the value before channel modulation has a large error with the original data. Figure 19 shows that the value after channel modulation is very similar to the original data. The error between the original data and the data before channel modulation is shown in Figure 20. And, the error between the original data and the data after channel modulation is shown in Figure 21:

$$m^{(k)} = c'^{(k)} - 50x_s^{(k)}. \quad (8)$$

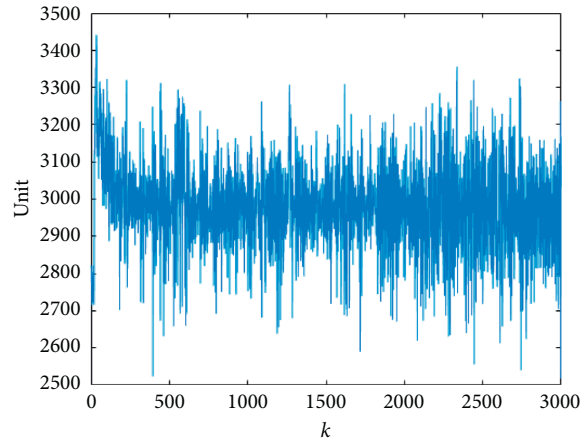

Figure 13: Schematic of the ciphertext signal after the signal transmitter encrypts the audio signal.

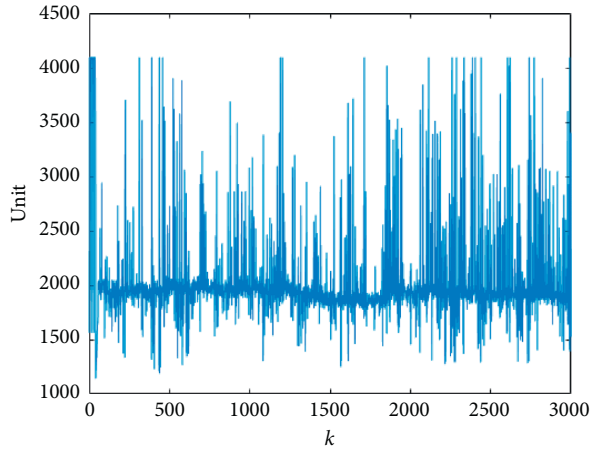

Figure 14: Schematic of the ciphertext signal received by the signal receiver.

Table 1: Numerical relationship between the transmitter and receiver.

Resolution	12-bit ADC values between 0 and 4095 (unit)	
	Transmitter	Receiver
—	100	1900
	500	2200
	1000	2400
	1500	2600

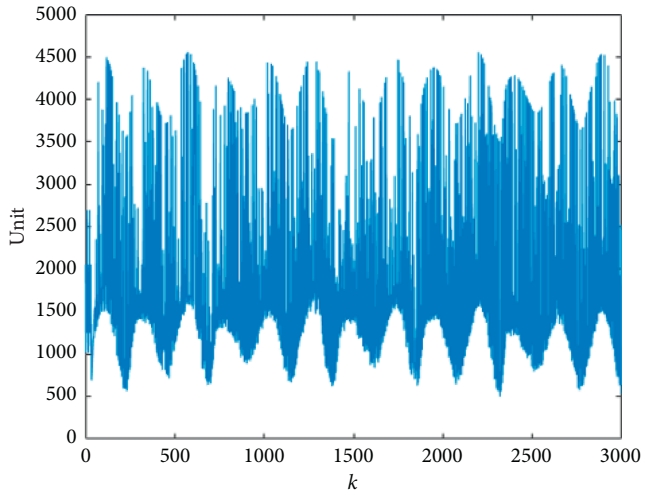

Figure 15: Unmodulated signal decryption results.

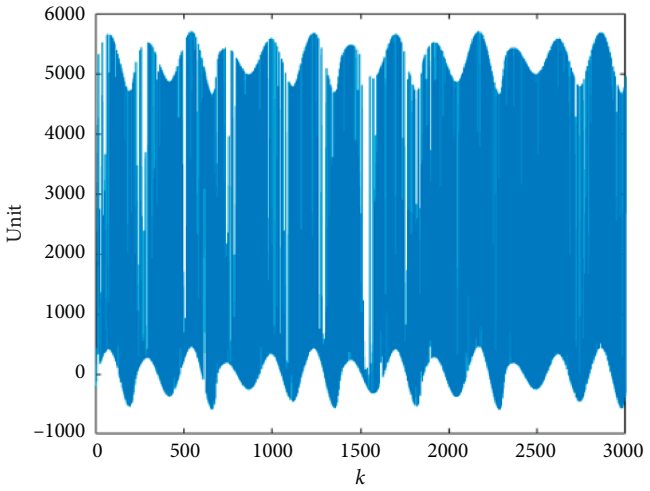

Figure 16: Demodulated signal decryption results.

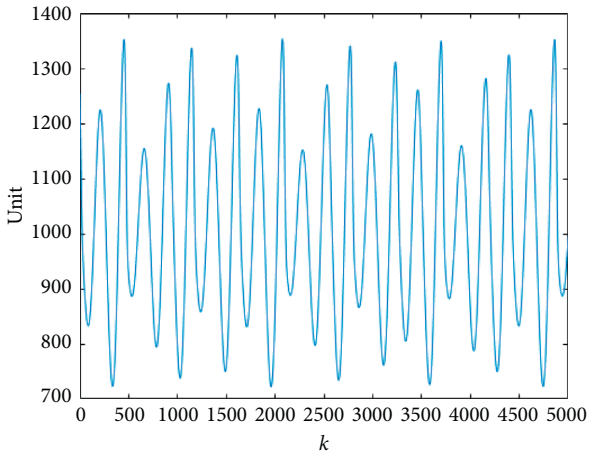

Figure 17: The data of the transmitter.

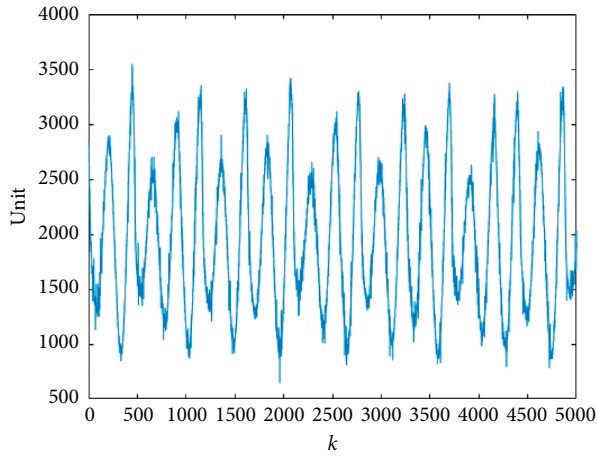

Figure 18: The data of the receiver before channel modulation.

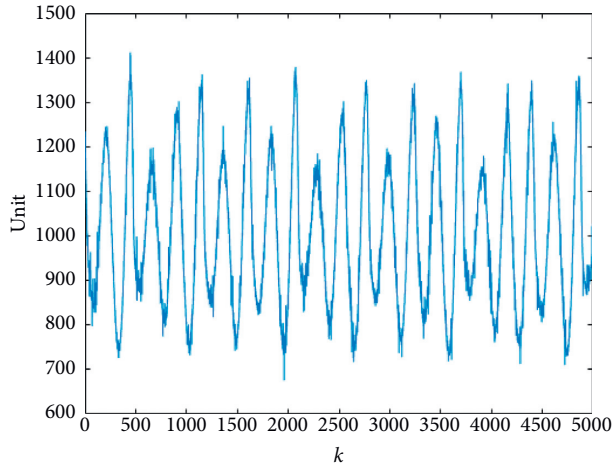

Figure 19: The data of the receiver after channel modulation.

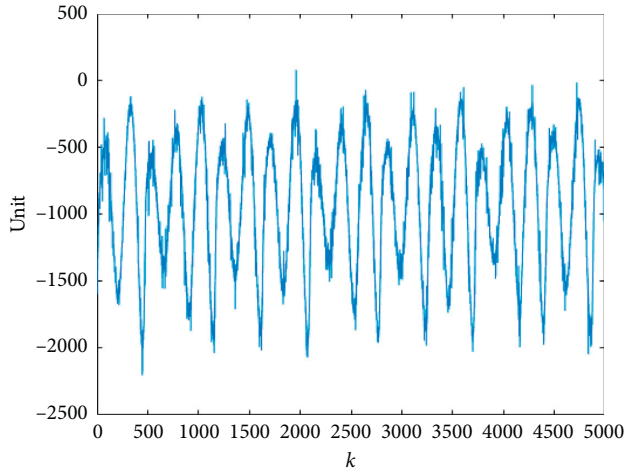

Figure 20: The error between the transmitter and receiver before channel modulation.

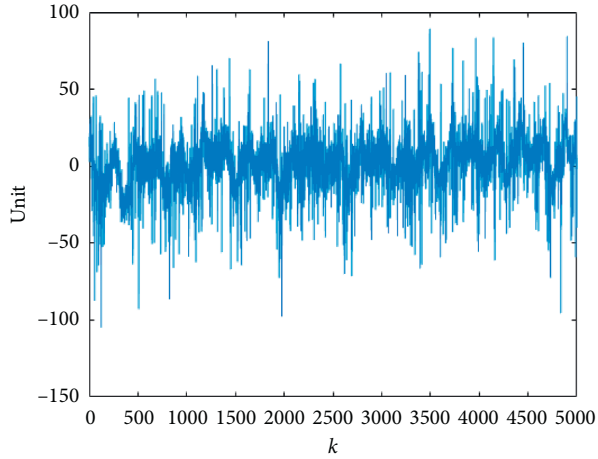

Figure 21: The error between the transmitter and receiver after channel modulation.

4. Conclusion

A novel VLC system integrated with a chaotic system has been proposed in the study to enhance the security of data transmission. The Arduino Due microcontroller is used in the proposed VLC system. LEDs are used as light sources to transmit information, and a light-sensing OPT-101 module is used to receive the light signal. A synchronization controller is used to reduce the state error and synchronize the master and slave mechanism. Some numerical simulations are conducted to verify the effectiveness of the proposed PID controller and analyze the signal. Furthermore, a chaotic system is used for encryption. The design has improved the resolution of optical communication transmission and accelerated the synchronization of the chaotic system. Most of the interference of external light sources was removed using appropriate filters. In addition, this manuscript is different from digital transmission, and we use VLC to transmit data, which proposes channel modulation methods to solve the shortcomings of analog transmission that is susceptible to external environmental interference. The experimental results of the prototype visible light information communication system can be used as the basis for the improvement of the next generation of communication technology.

Data Availability

The data used to support the findings of the study are cited in the references within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was supported in part by the Ministry of Science and Technology, Taiwan, under Grant nos. MOST 108-2221-E-992-094, MOST 108-2221-E-006-214-MY2, and MOST 109-2221-E-366-004.

References

[1] M. Calderbank, *The RSA Cryptosystem: History, Algorithm, Primes*, University of Chicago, Chicago, IL, USA, 2007.

[2] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology-EUROCRYPT'99*, pp. 223–238, Springer, Berlin, Germany, 1999.

[3] B. Paul and F. Marcus, "The rossler attractor in 3D," 2002, http://paulbourke.net/fractals/rossler/.

[4] Y. T. Chang, "A CDMA-based indoor visible light communications system for message broadcasting," Thesis, National Chiao Tung University Institute of Computer Science and Engineering, Hsinchu, Taiwan, 2013.

[5] Z. Y. Chen, "VLC-based indoor positioning system using smartphone," Thesis, National Yunlin University of Science and Technology Electronic Engineering, Douliu, Taiwan, 2017.

[6] C. H. Shih, "Application of remote voice control system for visible light communication," Thesis, National Chung Hsing University Electronic Engineering, Taichung, Taiwan, 2015.

[7] P. C. Chiang, "The electronic circuit realization and nonlinear analysis of synchronization between Lorenz and Rössler chaotic systems," Thesis, Department of Physics National Kaohsiung Normal University, Kaohsiung, Taiwan, 2018.

[8] K. L. Wu, "Synchronization of chaotic systems and its application," Thesis, I-SHOU University Department of Civil and Ecological Engineering, Kaohsiung, Taiwan, 2006.

[9] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, p. 821, 1990.

[10] C. S. Carroll, "Synchronous control of chaotic systems and its development in wireless digital image/audio secure communication," Thesis, National Kaohsiung Marine University, Kaohsiung, Taiwan, 2015.

[11] A. Ouannas, A. A. Khennaoui, S. Momani, V.-T. Pham, and R. El-Khazali, "Hidden attractors in a new fractional–order discrete system: chaos, complexity, entropy, and control," *Chinese Physics B*, vol. 29, no. 5, Article ID 050504, 2020.

[12] A. Ouannas, A. A. Khennaoui, S. Momani, G. Grassi, and V.-T. Pham, "Chaos and control of a three-dimensional fractional order discrete-time system with no equilibrium and its synchronization," *AIP Advances*, vol. 10, no. 4, Article ID 045310, 2020.

[13] A. Ouannas, A. A. Khennaoui, S. Momani, and V.-T. Pham, "The discrete fractional duffing system: chaos, 0–1 test, C 0 complexity, entropy, and control," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 30, no. 8, Article ID 083131, 2020.

[14] C. Sánchez-López, "An experimental synthesis methodology of fractional-order chaotic attractors," *Nonlinear Dynamics*, vol. 100, no. 4, pp. 3907–3923, 2020.

[15] A. D. Pano-Azucena, J. de Jesus Rangel-Magdaleno, E. Tlelo-Cuautle, and A. de Jesus Quintas-Valles, "Arduino-based chaotic secure communication system using multi-directional multi-scroll chaotic oscillators," *Nonlinear Dynamics*, vol. 87, no. 4, pp. 2203–2217, 2017.

[16] M. Zapateiro De la Hoz, L. Acho, and Y. Vidal, "An experimental realization of a chaos-based secure communication using arduino microcontrollers," *The Scientific World Journal*, vol. 2015, Article ID 123080, 10 pages, 2015.

[17] M. L. Hung, J. S. Lin, J. J. Yan, and T. L. Liao, "Optimal PID control design for synchronization of delayed discrete chaotic systems," *Chaos, Solitons and Fractals*, vol. 35, no. 4, pp. 781–785, 2008.

[18] G. Wen, Q.-G. Wang, C. Lin, G. Li, and X. Han, "Chaos synchronization via multivariable PID control," *International Journal of Bifurcation and Chaos*, vol. 17, no. 5, pp. 1753–1758, 2007.