Sensors and Materials, Vol. 37, No. 8 (2025) 3447–3464
MYU Tokyo

S & M 4128

Advanced Data Security in Renewable Energy Systems through Lorenz Chaos-based Encryption

Meng-Hui Wang,* Xiang-Ming Shi, and Hong-Wei Sian

Department of Electrical Engineering, National Chin-Yi University of Technology,
No. 57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 411030, Taiwan (R.O.C.)

(Received December 18, 2024; accepted April 21, 2025)

Keywords: Lorenz chaos system, image encryption, data security, signal processing, encryption algorithm

In this study, we developed encryption technologies based on the Lorenz chaotic system to enhance the security of images, data, and signals during transmission. Current encryption methods are vulnerable to statistical analysis and pattern recognition; thus, we used the Lorenz system from chaos theory to generate encryption keys, leveraging its unpredictability and sensitivity to initial conditions. We introduced an innovative encryption mechanism combining the Lorenz system with hash functions. This method effectively encrypts images, data, and signals, ensuring no loss of information during decryption. Experimental results showed the algorithm's accuracy even with added noise and its resistance to statistical analysis attacks. This encryption technology has significant potential in renewable energy systems, where secure data transmission is crucial for operational integrity. In systems such as smart grids and wind or solar energy management, encrypted communication ensures that critical data from real-time metrics to system configurations remains protected against cyber threats. By integrating this robust encryption approach, renewable energy systems can enhance overall security and reliability.

1. Introduction

In today's society, the development of information and communication networks and messaging platforms is highly advanced, with frequent reports of hackers breaching online platforms. Cybersecurity issues have become a critical concern for all sectors. As data transmission volumes experience explosive growth, the importance of encryption technology is undeniable, ranging from protecting personal privacy to safeguarding national security. If confidential or sensitive information related to renewable energy systems were to be stolen by hackers, it could jeopardize the operational safety of these systems.

Particularly in the domains of image and signal transmission, owing to their big data characteristics and wide-ranging application prospects—such as in remote medical diagnosis, satellite image transmission, and personal multimedia data protection—the development of efficient and secure encryption algorithms has become crucial. Therefore, in this study, we propose applying a chaos synchronization system encryption method as a cybersecurity

*Corresponding author: e-mail: wangmh@ncut.edu.tw
https://doi.org/10.18494/SAM5519

ISSN 0914-4935
https://myukk.org/

protection mechanism for intelligent operation and maintenance (O&M) systems in renewable energy.

Chaos synchronization detection methods have been extensively studied across various fields.[1,2] Yang and Chua, and Lia and Tsai proposed the realization of communication encryption using the Lorenz chaotic system theory.[3,4] The primary encryption technique involves modulating and scrambling messages via chaotic systems before transmitting the scrambled data to the receiver. At the receiving end, decryption is performed using a predefined decryption key and a chaos decoding process. Without the proper key, unauthorized parties would only receive scrambled, unintelligible messages.[5]

Traditional encryption methods, such as the Advanced Encryption Standard and Rivest–Shamir–Adleman, face challenges in handling large-scale data owing to computational inefficiency and difficulties in key management. Although chaotic encryption methods theoretically offer high security, practical applications still encounter numerous challenges, such as efficient key generation, the computational cost of the encryption, and the quantifiable evaluation of encryption quality.[6,7]

In this study, we aim to address these issues by referencing chaotic encryption techniques and applying them to the communication encryption methods of intelligent O&M systems for renewable energy.[8–10] By introducing a new encryption framework that integrates chaotic systems with modern encryption technologies, we employed the Lorenz chaotic system to generate dynamic keys and incorporated innovative image processing techniques. The proposed approach seeks to improve encryption efficiency while ensuring quality and security.

Additionally, we conducted extensive performance evaluations of the encrypted data, including noise tolerance, decryption quality, and resilience against various attack strategies, to demonstrate the method's effectiveness and reliability. Through detailed experimental analyses and comparisons, we not only showcase the application potential of the chaotic encryption technology in image and signal encryption, but also provide new directions and insights for future studies.

In summary, the proposed integration of chaos theory and modern encryption technologies presents a novel, efficient, and secure solution for image, numerical, and signal encryption. It is hoped that the outcomes of this research will contribute to the field of information security, particularly for applications requiring the processing of large-scale data.

2. Research System Architecture Design

2.1 Renewable energy system encryption and decryption architecture

We constructed a data information monitoring architecture for the operational status of renewable energy system equipment, primarily focusing on onshore/offshore wind turbines and photovoltaic power generation equipment. The system collects equipment status data through programmable logic controllers and embedded edge computing systems. The proposed encryption technique is then applied to the collected data to ensure data security during transmission.

Once encrypted, the data is transmitted to the central intelligent O&M center via the International Electrotechnical Commission-16850 communication protocol. Upon receiving the encrypted data, the central O&M center employs the proposed decryption technique to decrypt the data, restoring it to its original form. This enables O&M personnel of renewable energy systems to monitor, analyze, and manage the equipment effectively. The overall architecture of the data information monitoring system is illustrated in Fig. 1.

The encryption framework proposed in this study, as illustrated in Fig. 2, is applicable to the encryption and decryption of images, numerical data, and signals. The entire framework processes the original data through encryption algorithms to convert it into encrypted data, which is then restored to decrypted data through decryption algorithms. This framework is

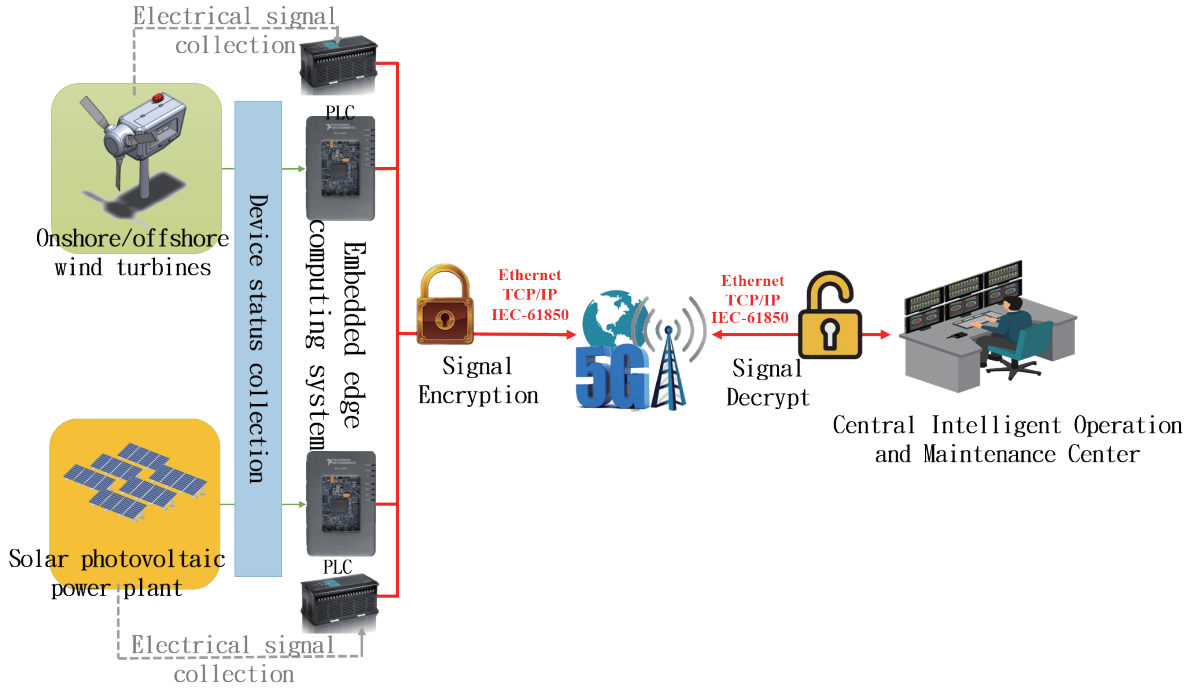

Fig. 1. (Color online) Overall data information monitoring system architecture.

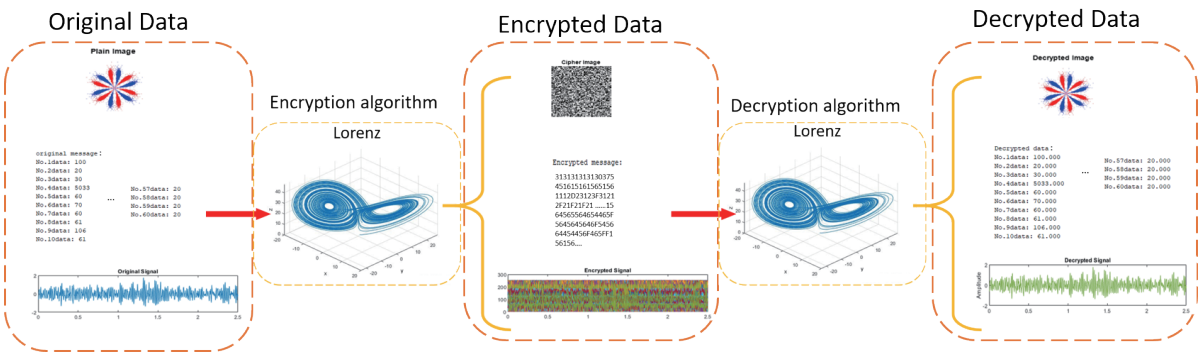

Fig. 2. (Color online) Flowchart of encryption framework.

designed to achieve highly efficient and secure data encryption and decryption operations, making it suitable for renewable energy systems that require remote monitoring and data transmission.

2.2 Design of Lorenz chaotic system for image, data, and signal encryption and decryption methods

2.2.1 SHA-2

Cryptographic encryption methods often employ hash functions in Message Authentication Code (MAC) algorithms, digital signatures, and file integrity verification. Cryptographic hash algorithms exhibit the avalanche effect,[11] where a hash function returns a fixed-length string independent of file size, and the hash value changes entirely when any single unit of the file is altered. The hash functions in the SHA-2 series share similar structural features but differ in terms of message size, block size, security bits, word size, internal operations, and hash size, as shown in Table 1.

The output of a hash function is derived from the input data digest through a two-phase process to compute the hash value. First, the data undergoes preprocessing to ensure that its size is a multiple of the block size, providing an initial hash value. Then, the hash value is calculated through data blocks using constants, functions, words, and logical functions. After a fixed number of iterations, the final hash value is produced, yielding the data digest.

2.2.2 Chaotic system

In the preset key generation phase, a predefined 128-bit hexadecimal key is used to initialize the encryption algorithm. The initial conditions (x_0, y_0, z_0) are utilized to compute the initial values for the Lorenz chaotic system. The initial value of each variable is derived through an XOR operation between the corresponding initial condition and specific key bits. The mathematical equations are shown as follows:

$$x_0 = x_0' + \frac{k_1 \oplus k_2 \oplus k_3 \oplus \ldots \oplus k_{11}}{255}, \tag{1}$$

$$y_0 = y_0' + \frac{k_{12} \oplus k_{13} \oplus k_{14} \oplus \ldots \oplus k_{22}}{255}, \tag{2}$$

$$z_0 = z_0' + \frac{k_{23} \oplus k_{24} \oplus k_{25} \oplus \ldots \oplus k_{32}}{255}. \tag{3}$$

In this study, the Lorenz chaotic system used for cryptography generates chaotic sequences using the Lorenz equations.[12] The parameters are set as $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$, with initial

Table 1
Hash algorithm.

Term	SHA-1	SHA-256	SHA-512
Message digest size	160	256	512
Optimal attack complexity	2^{80}	2^{128}	2^{256}
Message size	$<2^{64}$	$<2^{64}$	$<2^{128}$
Message block size	512	512	1024
Word size	32	32	64
Digest iteration count	80	64	80

conditions $x(1) = 1$, $y(1) = 0$, and $z(1) = 0$. The Lorenz differential equations are solved using the numerical ordinary differential equation solver function ODE45, enabling the generation of chaotic sequences.[13] A portion of the generated chaotic sequence is then extracted as the key sequence for encryption operations. The differential equations are shown in Eq. (4). The discrete form of the Euler method is shown in Eq. (5).

$$\begin{cases} \dfrac{dx}{dt} = \sigma\left(y - x\right) \\ \dfrac{dy}{dt} = x\left(\rho - z\right) - y \\ \dfrac{dz}{dt} = xy - \beta z \end{cases} \tag{4}$$

$$\begin{cases} x(t) = x(t-1) + dt \cdot \sigma\left(y(t-1) - x(t-1)\right) \\ y(t) = y(t-1) + dt \cdot \left(x(t-1)\left(\rho - z(t-1)\right) - y(t-1)\right) \\ z(t) = z(t-1) + dt \cdot \left(x(t-1)\, y(t-1) - \beta z(t-1)\right) \end{cases} \tag{5}$$

3. Methods

3.1 Image encryption and decryption algorithm

First, feature snowflake images from the status monitoring signals of the renewable energy system are captured, and the image size is adjusted to a uniform fixed pixel dimension (64 × 64 pixels). The images are then processed using image processing functions to convert them into grayscale images and further transformed into double-precision floating-point array matrices. This step facilitates subsequent mathematical operations.

Next, the Lorenz chaotic system is used to generate a chaotic sequence, with initial conditions set as $x(1) = 1$, $y(1) = 0$, and $z(1) = 0$ and parameters $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$. By solving the Lorenz differential equations using the numerical ordinary differential equation solver function ODE45, a chaotic sequence is generated. A portion of this sequence is selected as the encryption key.

The chaotic key is then used to perform encryption operations on the image's floating-point array matrix. During the encryption, each pixel value of the floating-point array matrix is sequentially processed using XOR operations or other nonlinear transformations with the chaotic key, resulting in a grayscale encrypted image with irregular, hashed pixels.

Finally, when the central intelligent O&M center receives the encrypted image, the decryption is conducted using the same chaotic key. Inverse operations are applied to the encrypted image to perform decryption, allowing the original image to be restored without distortion.

Figure 3 illustrates the encryption and decryption for the feature images of the renewable energy system's status. As shown in Fig. 3, the decrypted image is identical to the original image, whereas the encrypted image completely loses any correlation with the original image, making it impossible to discern the original image from the encrypted one.

Figure 4 shows the image encryption and decryption histogram. As observed in Fig. 4, the pixel value distribution of the encrypted image appears flatter and more uniform than that of the plain image, indicating that the encryption process effectively randomizes pixel intensity values and enhances resistance against statistical attacks.

Fig. 3. (Color online) Image encryption and decryption.

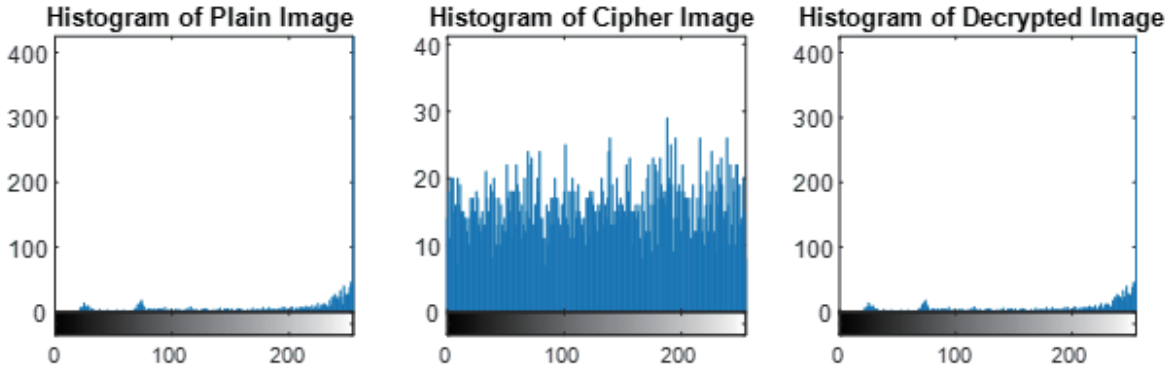

Fig. 4. (Color online) Image encryption and decryption histogram.

3.2 Numerical encryption and decryption algorithm

The numerical data collected from monitoring the status of the renewable energy system is first read and converted into a string format to facilitate character-level encryption operations. Next, the Lorenz chaotic system is used to generate a chaotic sequence, with initial conditions set as $x(1) = 1$, $y(1) = 0$, and $z(1) = 0$ and parameters $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$. The Lorenz differential equations are solved using the numerical ODE solver function ODE45, generating a chaotic sequence. A portion of this sequence is selected as the encryption key.

The generated chaotic key is then applied to perform bitwise operations for the encryption of the numerical string. Specifically, each character in the numerical string is converted into its corresponding ASCII code. The encoded characters are then XORed with the chaotic key, resulting in an unintelligible hexadecimal encrypted string.

When the central intelligent O&M center receives the encrypted string, the decryption is performed using the same chaotic key. The hexadecimal encrypted string undergoes inverse operations, accurately restoring the original numerical string, which is then converted back into a floating-point numerical format.

Figure 5 illustrates the encryption and decryption for numerical data in the renewable energy system. As shown in Fig. 5, the decrypted numerical values are identical to the original ones, with no data loss. The encrypted string, however, appears as an incomprehensible arrangement of values, making it impossible to infer the original numerical data from the encrypted values.

3.3 Signal encryption and decryption algorithm

The electrical monitoring signals measured from the renewable energy system's status are first preprocessed through normalization to scale the signal amplitude range to [−1,1], facilitating subsequent encryption operations for the signal's regularity. Next, a chaotic key is generated using the Lorenz chaotic system, following the same key generation technique as used for image

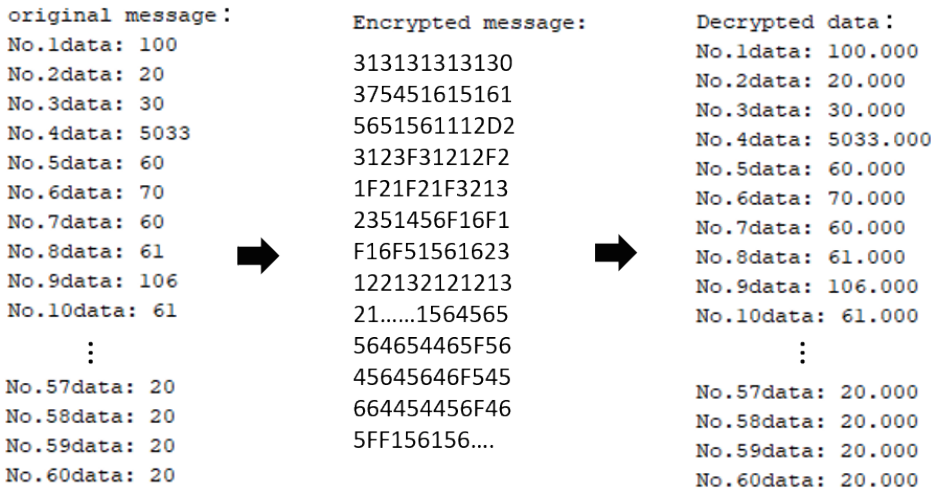

Fig. 5. Numerical encryption and decryption.

and numerical encryption. The normalized signal is then converted into an 8-bit unsigned integer format, and the chaotic key is applied using XOR operations to perform encryption. This process produces an encrypted signal with chaotic and scrambled waveform aliasing.

When the central intelligent O&M center receives the encrypted signal, the decryption is performed using the same chaotic key. The encrypted signal undergoes inverse operations, restoring the waveform of the original signal without any distortion. Finally, the decrypted signal is remapped to its original amplitude range.

Figure 6 illustrates the encryption and decryption for wind turbine vibration electrical signals in the renewable energy system, whereas Fig. 7 demonstrates the process for solar photovoltaic module electrical signals. From Figs. 6 and 7, it is evident that the decrypted signal waveforms are identical to the original waveforms, with no distortion or noise. Additionally, the encrypted signals do not reveal any identifiable features of the original signal waveforms.

4. Simulation Results and Security Analysis

For an image encryption algorithm to be considered highly secure, it must resist various cryptographic attacks such as brute force attacks, statistical attacks, entropy attacks, and differential attacks. To validate the proposed encryption algorithm's effectiveness in terms of image encryption security, we conducted simulation tests and security analyses on five 512 × 512 pixel images. The selected images include wind turbine gearbox tooth-break vibration feature

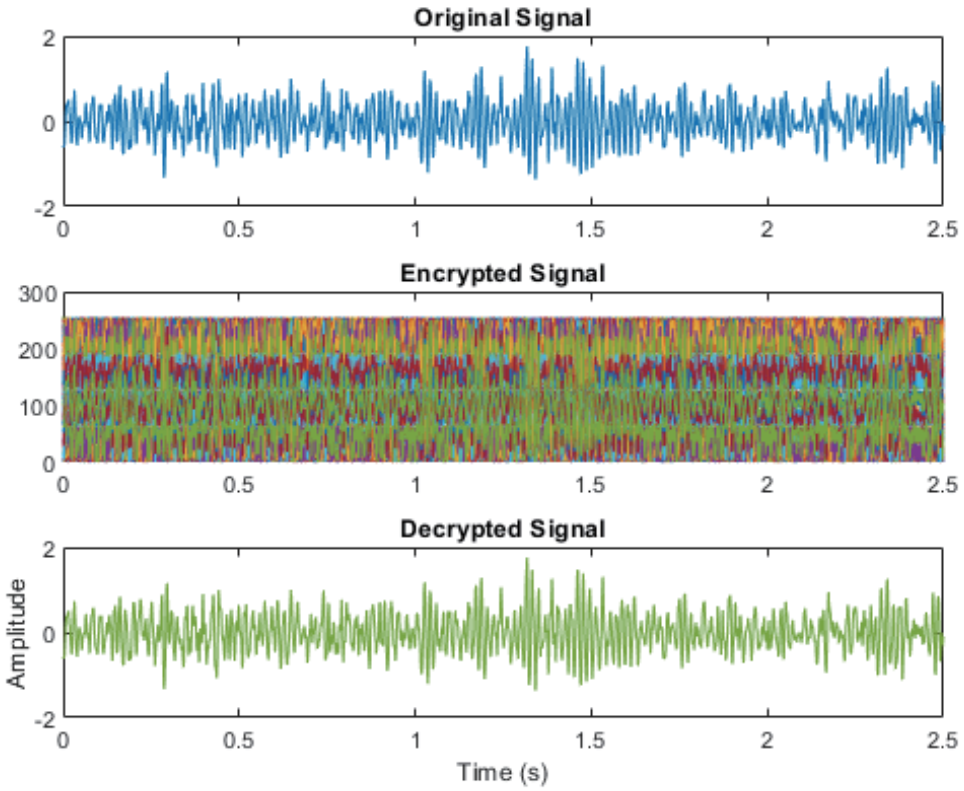

Fig. 6. (Color online) Encryption and decryption for wind turbine vibration electrical signals.

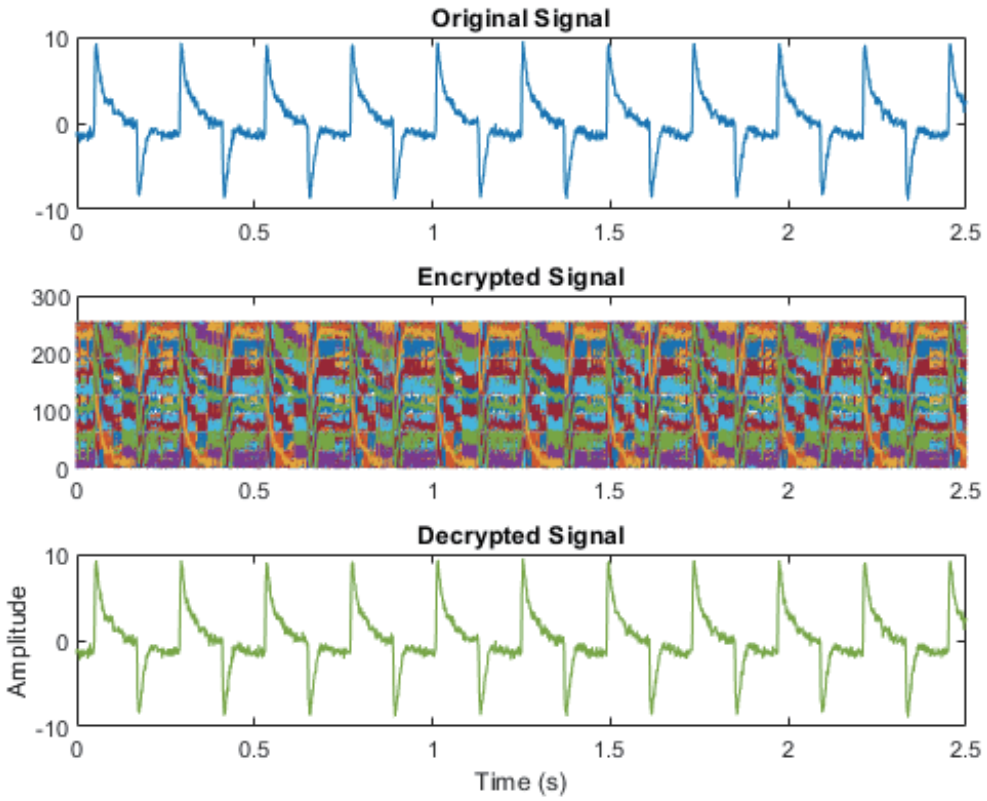

Fig. 7. (Color online) Encryption and decryption for solar photovoltaic module electrical signals.

snowflake image (Types A and B), wind turbine gearbox rust fault vibration feature snowflake image (Type C), pepper image (Type D), and baboon image (Type E). The Lorenz chaotic system was used for the simulations and analyses, with the initial conditions set to $x_0 = 50$, $y_0 = 70$, and $z_0 = 80$.

4.1 Simulation test results for images

In image encryption techniques, the 1-bit and 2-bit tests are important methods for evaluating the robustness and security of encryption algorithms. These tests primarily involve making slight bit changes to the original image and observing the resulting variations in the encrypted image. The following outlines the main reasons and theoretical foundation behind conducting image simulation tests.[14]

4.1.1 Number of pixels change rate (*NPCR*)

NPCR is used to measure the rate of pixel value change in the encrypted image when a single pixel in the original image is altered during encryption. The ideal value is 99.6094%, as shown in Eq. (6).

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \tag{6}$$

Here, $D(i, j)$ represents the difference matrix between two images. If the pixel values at position (i, j) in the two images are not equal, then $D(i, j) = 1$; otherwise, $D(i, j) = 0$.

4.1.2 Unified average changing intensity (*UACI*)

UACI is used to measure the average intensity of changes in the encrypted image when a single pixel in the original image is altered during encryption. The ideal value is approximately 33.4635%, and the calculation formula is shown in Eq. (7).

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{C_1(i,j) - C_2(i,j)}{255}\right| \times 100\% \tag{7}$$

Here, $C_1(i, j)$ and $C_2(i, j)$ represent the pixel values at position (i, j) in the first and second images, respectively.

4.1.3 Information entropy

Information entropy is an important metric for describing the randomness of an image. An information entropy higher than that of the original (unencrypted) image reflects a more chaotic distribution of pixel values in the encrypted image, indicating higher encryption effectiveness. For image encryption, the ideal information entropy for a grayscale image is close to 8, which implies a minimal likelihood of information leakage from the original image. The calculation formula is shown in Eq. (8)

$$H = -\sum_{i=0}^{255} p(m_i) \times \log_2 p(m_i) \tag{8}$$

Here, m_i represents the i-th grayscale pixel value of the image and $p(m_i)$ denotes the probability distribution of the grayscale pixel value m_i.

A. Resistance to differential attack

Differential attack is a method targeting encryption systems, where an attacker attempts to break the encryption algorithm by analyzing how small changes in the input image affect the encrypted image. We evaluated the sensitivity of the proposed encryption algorithm to such minor changes through 1-bit and 2-bit tests, ensuring that the algorithm can effectively resist this type of attack.

B. Testing the diffusion property of the encryption algorithm

Diffusion refers to the property where a small change in the input image should result in a significant change in the encrypted output image. This means that every bit change in the input pixel should affect a large portion of the output pixels. In this study, 1-bit and 2-bit tests are conducted to evaluate whether the proposed encryption algorithm exhibits strong diffusion properties.

C. Security evaluation

We evaluated security tests to quantify the change rate and average intensity variation of encrypted images. These evaluation metrics help assess the encryption algorithm's security, ensuring that it provides sufficient protection to prevent attackers from inferring with the original image content by analyzing the encrypted images.

For image simulation testing, the initial conditions of the Lorenz chaotic system mentioned above were applied to perform experiments on the original images (Types A to E). Specifically, 1-bit or 2-bit pixel modifications were made to evaluate the encryption algorithm's security and stability.

Figure 8 illustrates the 1-bit encryption and decryption for the wind turbine gearbox tooth-break fault vibration feature snowflake image (Type B), whereas Fig. 9 shows the 2-bit

Fig. 8. (Color online) 1-bit encryption and decryption for wind turbine gearbox tooth-break fault vibration feature snowflake image.

Fig. 9. (Color online) 2-bit encryption and decryption for wind turbine gearbox rust fault vibration feature snowflake image.

encryption and decryption for the wind turbine gearbox rust fault vibration feature snowflake image (Type C). From Figs. 8 and 9, it is evident that the encrypted images contain no identifiable features or information from the original images.

To examine whether minor changes in an image affect the encrypted image, we employed entropy, *NPCR*, and *UACI* to quantify the randomness, pixel value change rate, and average intensity variation of the encrypted image. These metrics are instrumental in demonstrating that the proposed encryption algorithm exhibits strong diffusion properties and resistance to differential attacks, thereby enhancing the security of information transmission in renewable energy systems.

Table 2 presents the experimental results of bitwise pixel modifications. The results in Table 2 show that the entropy, *NPCR*, and *UACI* values are all close to their theoretical values, indicating that the proposed encryption algorithm has low leakage and high sensitivity to changes in the original image. This confirms its effectiveness in resisting information entropy and differential attacks.[15]

4.2 Security analysis

Malicious attackers may attempt to disrupt the normal image transmission by tampering or interfering with intercepted encrypted images, with the goal of preventing the successful decryption of the encrypted images. In this study, encrypted images are subjected to cropping and noise attacks to induce a certain degree of damage. The ability to successfully decrypt and recover the original image despite these modifications is observed to analyze the robustness and security of the proposed encryption algorithm.

A. Cropping attack

Cropping attack simulates potential data loss in encrypted images during transmission or storage. This is achieved by setting pixel values in certain regions of the encrypted image to zero, effectively cropping parts of the image. The cropped encrypted image is then decrypted to verify the performance of the proposed encryption algorithm in handling incomplete image data. The peak signal-to-noise ratio (*PSNR*)[16] of the decrypted image is calculated to assess its quality.

The encryption and decryption for Type G and Type H images under cropping attacks are shown in Figs. 10–12. Figure 10 shows that when 25% of the encrypted image data is cropped,

Table 2
Experimental results of bitwise pixel modifications in images.

Image	1-bit pixel modification in images			2-bit pixel modification in images		
	Entropy	*NPCR* (%)	*UACI* (%)	Entropy	*NPCR* (%)	*UACI* (%)
Type A	7.9997	99.59	33.44	7.9997	99.59	33.455
Type B	7.9998	99.609	33.42	7.9998	99.609	33.43
Type C	7.9997	99.66	33.54	7.9997	99.66	33.56
Type D	7.9999	99.52	33.42	7.9999	99.52	33.41
Type E	7.9998	99.601	33.50	7.9998	99.601	33.52

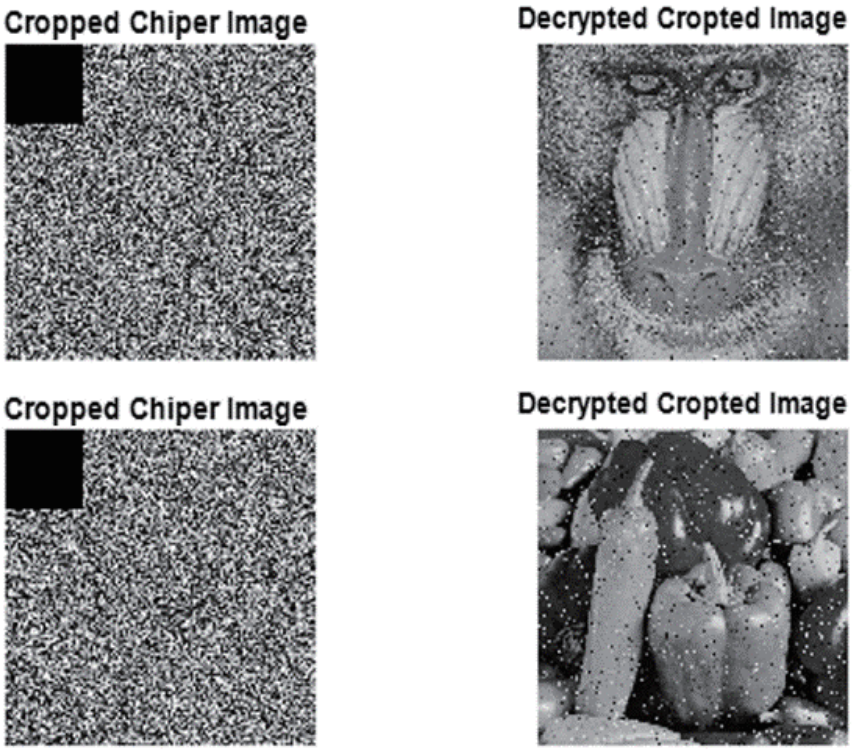

Fig. 10. Encryption and decryption for Type G and Type H images under cropping attack (25%).

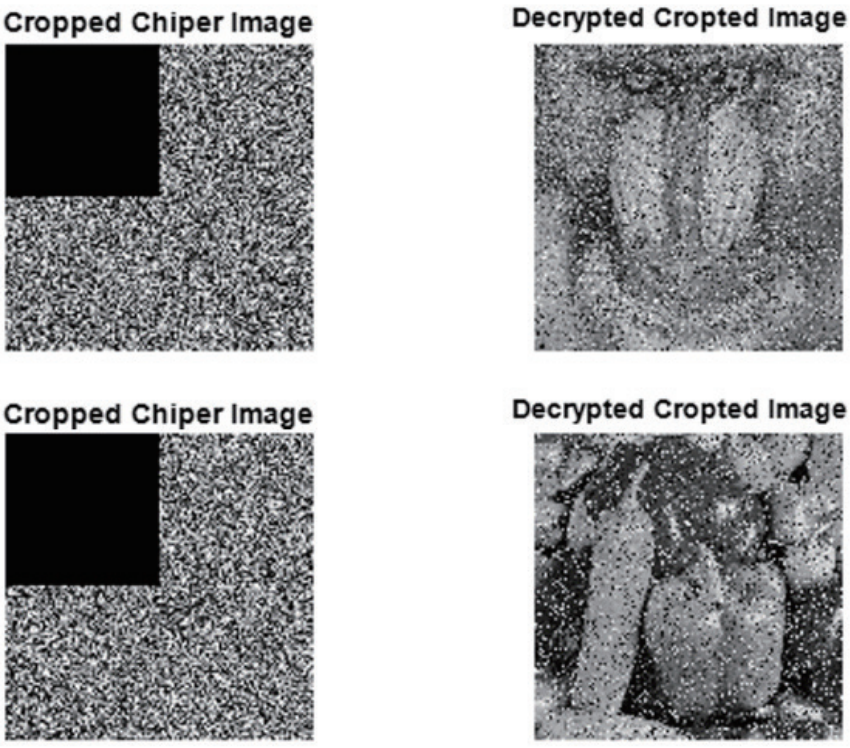

Fig. 11. Encryption and decryption for Type G and Type H images under cropping attack (50%).

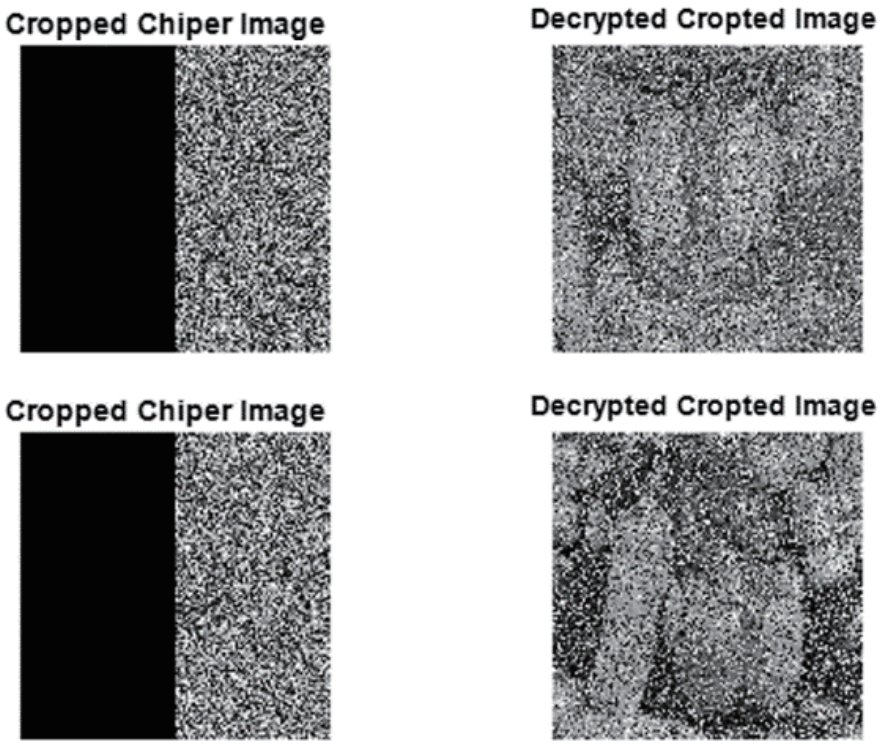

Fig. 12. Encryption and decryption for Type G and Type H images under cropping attack (75%).

Table 3
PSNR values of decrypted images at different cropping ratios.

Cropping ratio (%)	*PSNR* (dB)
25	20.45
50	18.32
75	15.67

the decrypted image does not exhibit severe data loss, achieving a similarity of 95.99% with the original image.

Figure 11 shows that when 50% of the encrypted image data is cropped, the similarity between the decrypted image and the original image is 86.21%, and the decrypted image still retains the key features of the original image.

Figure 12 shows that when 75% of the encrypted image data is cropped, the similarity decreases to 82.93%, resulting in a more blurred decrypted image, although the main features remain faintly recognizable.

Table 3 presents the *PSNR* values of decrypted images at different cropping ratios. The results in Table 3 indicate that as the cropping ratio increases, the *PSNR* value decreases, reflecting a decline in the quality of the decrypted image.

However, even when the encrypted image suffers significant cropping damage, the decrypted image retains a certain level of recognizability. This demonstrates the robustness of the proposed encryption algorithm.

B. Noise attack

Noise attack simulates the interference effects caused by noise on encrypted images during actual transmission. By adding pepper-and-salt noise of varying intensities to the encrypted images, followed by decrypting the noisy encrypted images, we verified the proposed encryption algorithm's decryption performance under data interference. The *PSNR* of the decrypted image is calculated to evaluate its quality.[16]

The encryption and decryption for Type G and Type H images under noise attack are shown in Figs. 13–15. Figure 13 shows that when 1% noise interference is added to the encrypted image, the decrypted image remains clear, achieving a similarity of 96.99% with the original image.

Figure 14 shows that when 5% noise interference is added to the encrypted image, the similarity between the decrypted image and the original image reaches 88.93%. Figure 15 shows that when 10% noise interference is added to the encrypted image, the similarity between the decrypted image and the original image decreases to 85.33%.

Table 4 presents the *PSNR* values of decrypted images at different noise intensities. The results in Table 4 show that the *PSNR* value decreases as the noise intensity increases, indicating a decline in the quality of the decrypted image.

However, even under high noise intensity interference, the decrypted image retains a certain level of recognizability. This demonstrates the proposed encryption algorithm's strong resistance to noise.

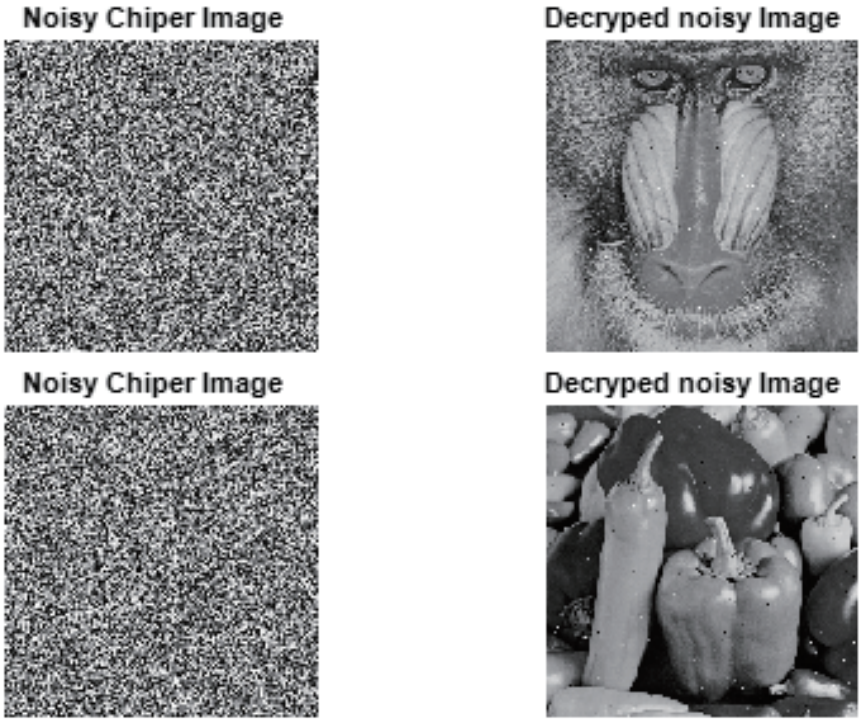

Fig. 13. Encryption and decryption for Type G and Type H images under noise attack (1%).

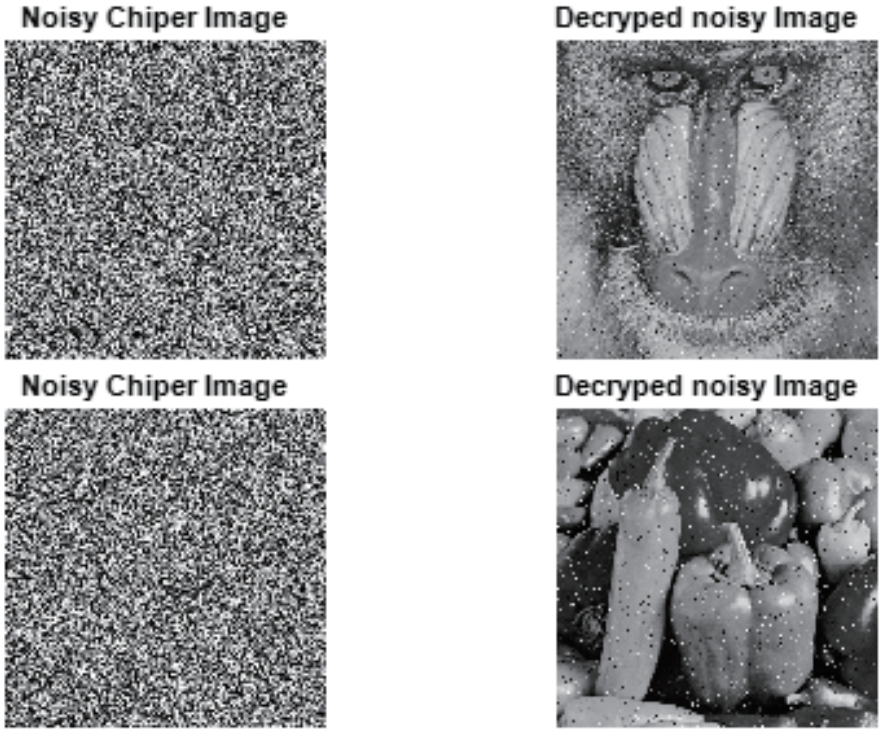

Fig. 14. Encryption and decryption for Type G and Type H images under noise attack (5%).

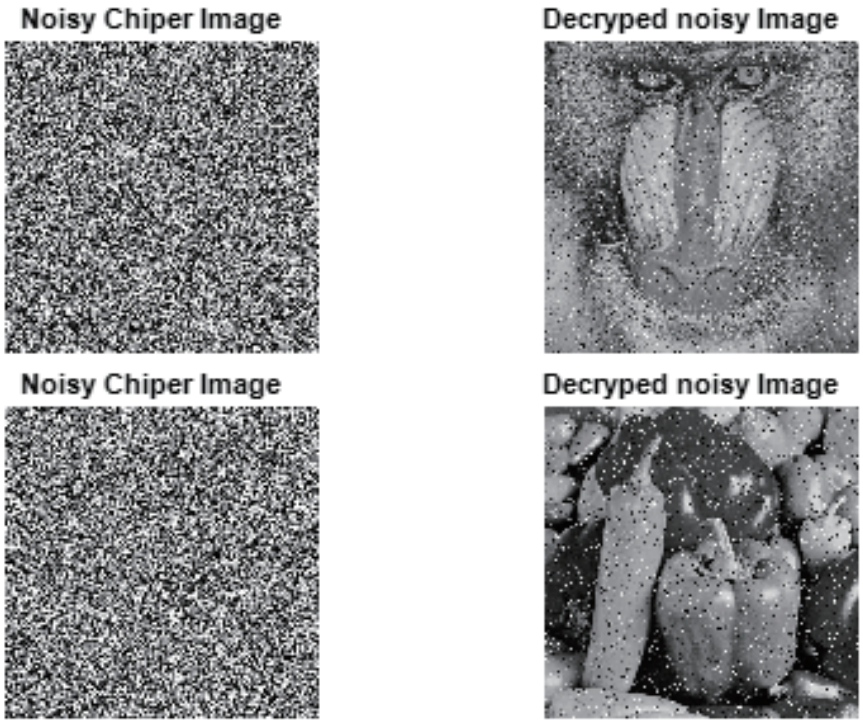

Fig. 15. Encryption and decryption for Type G and Type H images under noise attack (10%).

Table 4
PSNR values of decrypted images at different noise intensities.

Noise level (%)	*PSNR* (dB)
1	22.75
5	19.84
10	17.23

5. Conclusions

In this study, we proposed a novel encryption algorithm based on the Lorenz chaotic system, designed for renewable energy systems. The algorithm is applied to encrypt and decrypt images, numerical data, and signals obtained from renewable energy systems. The proposed encryption algorithm is evaluated through image simulation results and security analysis.

The results demonstrate that the keys generated by the Lorenz chaotic system exhibit excellent secrecy, making the encrypted data highly resistant to decryption attempts. Moreover, the decrypted data closely matches the original data with a high degree of similarity, confirming the accuracy and integrity of the proposed encryption algorithm.

These findings validate the practical utility of the algorithm for providing high-level data protection, making it suitable for data transmission scenarios that require heightened security. It ensures the confidentiality and reliability of transmitted data.

References

1 E. Ott, C. Grebogi, and J. A. Yorke: Phys. Rev. Lett. **64** (1990) 1196. https://doi.org/10.1103/PhysRevLett.64.1196
2 H. Zhang, X. K. Ma, and W. Z. Liu: Chaos, Solitons Fractals **21** (2004) 1249. https://doi.org/10.1016/j.chaos.2003.12.073
3 T. Yang and L. O. Chua: IEEE Trans. Circuits Syst. I Regul. Pap. **44** (IEEE, 1997) 976. https://doi.org/10.1109/81.633887
4 T. L. Liao and S. H. Tsai: Chaos, Solitons Fractals **11** (2000) 1387. https://doi.org/10.1016/S0960-0779(99)00051-X
5 T. Yang, L. B. Yang, and C. M. Yang: IEEE Trans. Circuits Syst. I Regul. Pap. **45** (IEEE, 1998) 1062. https://doi.org/10.1109/81.728860
6 T. Yang, C. W. Wu, and L. O. Chua: IEEE Trans. Circuits Syst. I Regul. Pap. **44** (1997) 469. https://doi.org/10.1109/81.572346
7 J. W. Hong, S. Y. Yoon, D. I. Park, M. J. Choi, E. J. Yoon, and K. Y. Yoo: Inf. Technol. Control **40** (2011) 252. https://doi.org/10.5755/j01.itc.40.3.634
8 H. T. Yau, Y. C. Pu, and S. Li: Inf. Technol. Control **41** (2012) 217. https://doi.org/10.5755/j01.itc.41.3.1137
9. S. Liu, Y. Li, and Z. Jin: Proc. 2023 IEEE 5th Int. Conf. Civil Aviation Safety and Information Technol. (IEEE, 2023) 318. https://doi.org/10.1109/ICCASIT58768.2023.10351719
10 S. A. Nagar and S. Alshamma: Proc. 2012 6th Int. Conf. Sciences of Electronics, Technologies of Information and Telecommunications (IEEE, 2012). https://doi.org/10.1109/SETIT.2012.6481987
11 A. A. Bhadke, S. Kannaiyan, and V. Kamble: Proc. 2018 24th Natinal Conf. Communications (IEEE, 2018) 69. https://doi.org/10.1109/NCC.2018.8600222
12 K. Ramasubramanian and M. Sriram: Physica D **139** (2000) 72. https://doi.org/10.1016/S0167-2789(99)00234-1
13 S. Vega, O. Vega, and E. Ortigoza: Proc. 2022 IEEE Int. Conf. Automation/XXV Congress of the Chilean Association of Automatic Control (IEEE, 2022). https://doi.org/10.1109/ICA-ACCA56767.2022.10005972
14 I. S. Rupa, K. Manideep, N. M. Kamale, and S. Suhasini: Proc. 2022 Int. Conf. Innovative Computing, Intelligent Communication and Smart Electrical Systems (IEEE, 2022). https://doi.org/10.1109/ICSES55317.2022.9914081
15 F. Özkaynak: Proc. 2017 Int. Conf. Computer Science and Engineering (IEEE, 2017). https://doi.org/10.1109/UBMK.2017.8093481
16 D. Tao, S. Di, X. Liang, Z. Chen, and F. Cappello: Proc. 2018 IEEE Int. Conf. Cluster Computing (IEEE, 2018). https://doi.org/10.1109/CLUSTER.2018.00048

About the Authors

Meng-Hui Wang received his M.S. and Ph.D. degrees in electrical engineering in 1990 and 1994, respectively, from National Taiwan University of Science and Technology. He joined National Chin-Yi University of Technology in August 1994 and is now affiliated with the Department of Electrical Engineering as a lifetime distinguished professor. His major areas of research include renewable energy systems, power systems, extension theory, and AI applications. He is a member of the Chinese Association of Artificial Intelligence, the vice president of the Taiwan Education Society of Innovation & Invention, and the chairman of the 6th Intelligent Living Technology Association of Taiwan. He was the general chair of the 1st Intelligent Living Technology Conference (2006) and the honorary co-chair of the 2012 International Symposium on Computer, Consumer, and Control.
(wangmh@ncut.edu.tw)

Shi-Xiang Ming received his B.S. degree from the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan, in 2024. His main research includes wind turbines and fault diagnosis.
(ming900708@gmail.com)

Hong-Wei Sian received his M.S. degree in electrical engineering from National Changhua University of Education, Changhua City, Taiwan, in 2006, and his Ph.D. degree in electrical engineering from National Taiwan University of Science and Technology, Taipei City, Taiwan, in 2024. He is currently an assistant professor in the Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City, Taiwan. His research interests include equipment fault diagnosis, renewable energy systems, programmable logic controller, and automation control application.
(hwsian@ncut.edu.tw)