Hindawi
Scientific Programming
Volume 2022, Article ID 2308825, 10 pages
https://doi.org/10.1155/2022/2308825

Research Article

Wireless Sensor Network Security Based on Improved Identity Encryption

Hao Zhou[1] **and Haochang Bi**[2]

[1]*Computer Department, Anhui Post and Telecommunication College, Hefei 230031, China*
[2]*Anhui Vocational College of Electronics & Information Technology, Anhui, Bengbu 233030, China*

Correspondence should be addressed to Haochang Bi; 2000100018@ahdy.edu.cn

Received 24 January 2022; Revised 18 February 2022; Accepted 12 March 2022; Published 1 April 2022

Academic Editor: Hangjun Che

Copyright © 2022 Hao Zhou and Haochang Bi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to protect network information security and improve the security of wireless sensor networks, based on chaotic systems, we propose a wireless sensor algorithm based on improved identity encryption. First, the basic principle of chaotic system mapping is specifically analyzed; the two chaotic mapping systems are rectified to obtain the hybrid chaotic mapping system according to the demand of wireless sensing network. After that, an encryption framework and key are designed and the hybrid mapping system is applied to the encryption framework to encrypt the data. In this way, the length of the encryption algorithm is lengthened and the defensibility of the encrypted content is improved. Finally, the performance of the proposed encryption algorithm is tested in terms of information entropy, statistical methods, and ciphertext randomness. The test results show that compared with other encryption algorithms, the running speed of the encryption algorithm proposed in this paper is only 18.51 ms, which is faster than that of other encryption algorithms, and the memory consumption is only 27%, which is much lower than that of other algorithms. It can be seen that the proposed encryption algorithm has strong encryption effect and superior algorithm performance for data encryption in wireless sensor networks.

1. Introduction

With the continuous improvement of Internet technology, computers, cell phones, and many other computer devices are widely used and have become essential products for daily life, enhancing information exchange and enriching people's entertainment. However, the widespread popularity and application of devices such as wireless sensors in computers have also brought about information security problems, and the security of people's information on the network has been seriously threatened. Therefore, encryption technology was born. The current market research on wireless sensor network security mainly includes encryption algorithms and authentication schemes, which serve to guarantee data security and legitimacy. However, the complex node resources and small memory of wireless sensor networks lead to the low computational accuracy and poor results of the existing encryption algorithms for wireless sensor networks. Among them, chaotic system has the characteristics of sensitivity to initial value, ergodicity, pseudo-randomness, etc., which meets the characteristics of diffusion and obfuscation in encryption algorithms and achieves preliminary application results in information security. For network information encryption, scholars and experts have conducted in-depth research. Maram et al. proposed a dynamic S-box approach to process Unicode text data [1]. Ahmad et al. proposed to use the Diffie–Hellman technique to exchange the encryption key generated by TTI algorithm with another party as a way to improve the security of sensitive information transmission [2]. Liang et al. proposed a dynamic key encryption-decryption neural network chaotic algorithm, and the results showed that the encryption-decryption speed and anti-decryption ability of the method had a great improvement [3]. Chaotic encryption algorithm was widely used, for example, Deng and Xiao applied the chaotic algorithm to the encrypted transmission of RFID, and the

results showed that the algorithm can meet the security requirements of object RFID [4]. Zhang et al. applied chaos algorithm to video transmission encryption to encrypt the differential components of motion vectors in horizontal and vertical directions as well as DC transform coefficients, respectively, and achieved good results [5]. Ge et al. proposed an encryption method for images based on cross-diffusion of logistic mapping and Chebyshev mapping by combining chaos algorithm. The results indicated that the encryption algorithm had high security [6]. Wu et al. proposed a chaotic compressed sensing algorithm for OFDM-PON networks, with results showing that the method can save bandwidth and improve the security of OFDM-PON networks [7]. The above studies show that chaotic algorithm is widely used in the field of data transmission [8–17]. Therefore, this study proposes an improved chaos-based encryption algorithm for wireless networks based on the characteristics of chaos algorithm and verifies the feasibility of the proposed algorithm.

2. Basic Methods

In the field of network information security, chaotic systems possess sensitivity, ergodicity, and unpredictability that have led to smaller applications in information security. Chaotic mappings are mainly divided into logistic mappings and cubic mappings.

Logistic mapping is in one-dimensional form in chaotic systems and can be expressed as

$$x_{n+1} = \mu x_n(1 - x_n), \mu \in (0, 4), x_n \in [0, 1], \tag{1}$$

where μ is a parameter and when $\mu \in (3.57, 4)$, the logistic mapping exhibits chaotic properties.

The cubic mapping is calculated as

$$x_{n+1} = ax_n^3 - bx_n, x_n \in [-1, 1], \tag{2}$$

where both **a** and b are parameters, the output range of Cubic mapping is shown in Figure 1, and the mapping range becomes progressively smaller with increasing parameter **a**.

As shown in Figure 2, a bifurcation point will occur when the parameter b is higher than 2.3, and the chaotic system is in a chaotic state at this time. To obtain better pseudo-randomness, a is set to 4 and b is set to 3. The cubic mapping expression is obtained as follows:

$$x_{n+1} = 4x_n^3 - 3x_n, x_n \in [-1, 1]. \tag{3}$$

In wireless sensor networks, chaotic systems cannot perform complex calculations on the network due to the problems of small network memory and poor computational power. To apply chaotic systems to wireless sensor network encryption, the chaotic system needs to be rectified.

The logistic mapping can also be expressed as

$$x_{n+1} = 1 - \lambda x_n^2, \lambda \in [0, 2], x_n \in [-1, 1], \tag{4}$$

where λ is a parameter. The logistic mapping integerization in chaotic systems consists of three main steps, as follows:

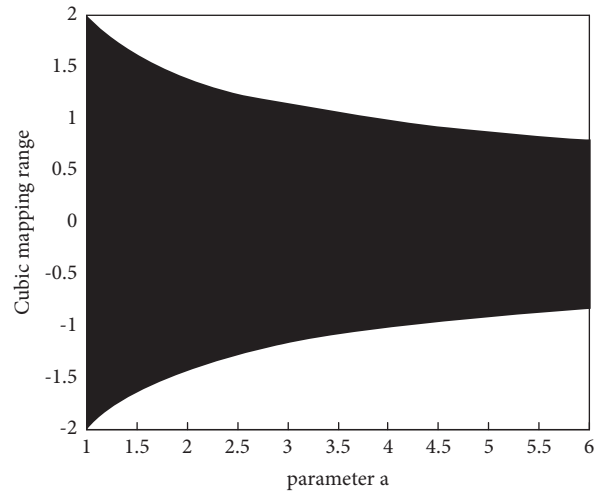

Figure 1: Trend of the range of cubic mapping with parameter a.

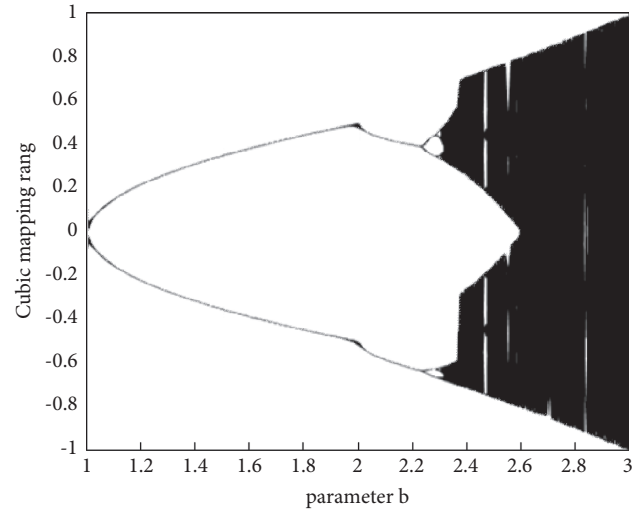

Figure 2: Trend of the range of cubic mapping with parameter b.

(1) Multiply both sides of equation (4) by $m^2 = (m \neq 0)$ at the same time and obtain the following equation

$$m^2 x_{n+1} = m^2 - \lambda(mx_n)^2. \tag{5}$$

(2) Construct an equation:

$$z_n = mx_n + m. \tag{6}$$

After a simple treatment of equation (6), equation (7) is calculated as follows:

$$\begin{cases} x_n = \dfrac{z_n}{m} - 1 \\ \\ x_{n+1} = \dfrac{z_{n+1}}{m} - 1 \end{cases}. \tag{7}$$

(3) Substitute equation (7) into equation (5) and set the parameter λ to 2. The final integer logistic mapping equation is obtained as

$$z_{n+1} = 4z_n - \frac{2}{m}z_n^2. \quad (8)$$

In equation (6), x_n interval is [−1, 1]; z_n interval is [0, 2m]; if z_n are integers, then $m = 2^{L-1}$, thus obtaining the z_n interval as $[0,2^L]$.

Equation (8) contains two zeros, $z_n = 0$ and $z_n = 2m$. If the initial iteration value is 0 or $2m$, the value of all subsequent iterations will be 0. To prevent the above situation, equation (8) will be optimized:

$$\begin{cases} z_{n+1} = 4z_n - \frac{2}{m}z_n^2 - 1, z_n = 0 \text{ or } 2m \\ \\ z_{n+1} = 4z_n - \frac{2}{m}z_n^2 - 1, \text{others} \end{cases}. \quad (9)$$

There are no zeros in equation (9) so that all iteration values will not be 0.

According to the cubic mapping of equation (3), it is integerized as follows:

(1) Construct the following equation:

$$\begin{cases} x_n = \frac{y_n}{c} - 1 \\ \\ x_{n+1} = \frac{y_{n+1}}{c} - 1 \end{cases}. \quad (10)$$

(2) Substitute equation (10) into equation (3) to obtain the following equation:

$$y_{n+1} = \frac{4}{c^2}y_n^3 - \frac{12}{c}y_n^2 + 9y_n. \quad (11)$$

In equation (10), the x_n interval is [−1,1], and the y_n interval is obtained as [0, 2c]. If the y_n values are all integers, then $c = 2^{L-1}$, and the y_n interval is $[0, 2^L]$.

Equation (11) contains several zeros, $y_n = 0$, $y_n = 1.5c$, and $y_n = c$. If the initial iteration value is 0, $1.5c$, or c, then all subsequent iterations have a value of 0. Thus, equation (11) is optimized to obtain the following equation:

$$y_{n+1} = \begin{cases} \frac{4}{c^2}y_n^3 - \frac{12}{c}y_n^2 + 9y_n + 1, y_n = 0 \text{ or } \frac{3}{2}c \\ \\ \frac{4}{c^2}y_n^3 - \frac{12}{c}y_n^2 + 9y_n, \text{others} \end{cases}. \quad (12)$$

There are no zeros in equation (12), and the iterative value of 0 does not occur when iterating.

3. Improved Identity Encryption Algorithm

3.1. Cryptographic Framework. The chaotic algorithm after integer is computed by Feistel cryptographic framework as shown in Figure 3, and the encryption process is as follows:

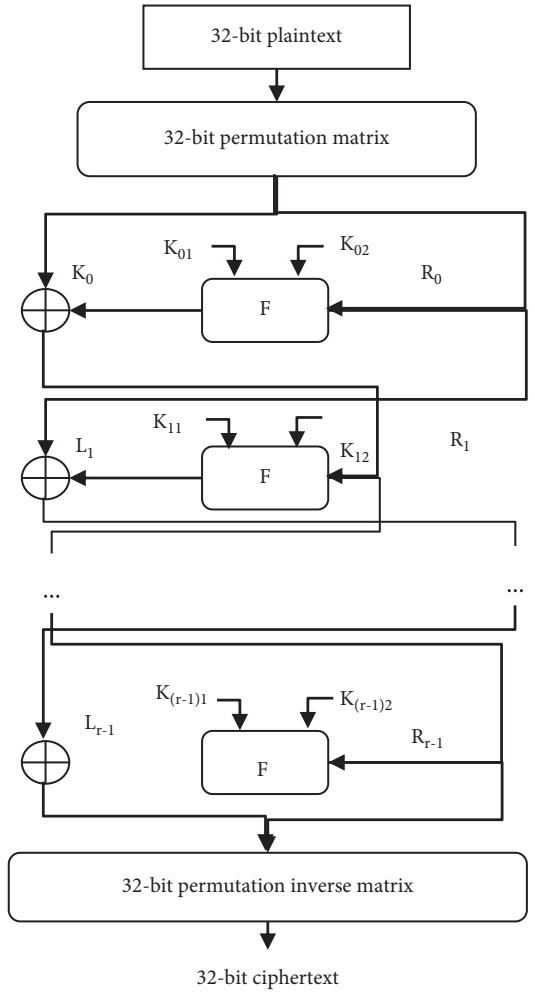

Figure 3: Cryptographic framework.

$$\begin{cases} R_{i+1}L_i \oplus F(K_i, R_i) \\ L_{i+1} = R_i \end{cases}. \quad (13)$$

The Feistel structure belongs to a symmetric cryptographic framework in which the round function F has an important impact on the performance of the algorithm. The main details of the round function F are shown in Figure 4.

In Figure 4, ⊕ is the XOR operation. The round function encryption process is divided into three main steps, as follows.

(1) First a 32-bit plaintext is divided into two parts of equal length, each side of length 16; then, a part is divided into two parts of equal length, of length 8.

(2) The two 8-bit plaintexts are followed by the number "0" to bring their length to 16 bits.

(3) The round key will be XOR operated on the 16-bit plaintext separately, followed by the logistic and cubic mappings, and then the XOR operation will be performed. Finally, the XOR value is passed through a 16-bit permutation matrix to obtain the output.

The algorithm encrypts a total of 4 rounds, i.e., $r = 4$.

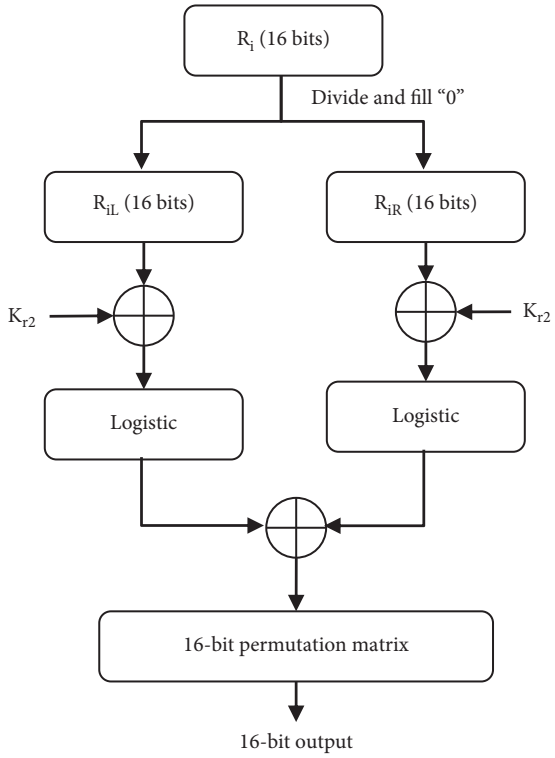

Figure 4: Round function F.

3.2. Generation of Round Key. In the above, the performance of the two chaotic systems degrades gradually after the integerization, which leads to the reduction of their sequence randomness. Therefore, to solve the above problem, the two chaotic systems are mapped together to obtain one hybrid chaotic system.

Also, this part generates the initial values of the hybrid chaotic system by a linear congruential generator. The linear congruential generator expression is given by [18, 19]

$$y(n+1) = \left(16807 \times y(n) \bmod \left(2^{31} - 1\right)\right). \quad (14)$$

With the addition of a linear congruential generator to the hybrid chaotic system, the period of the sequence generated by the hybrid chaotic system is extended to 2^{31}–1. The specific flow of generating chaotic sequences is shown in Figure 5.

The autocorrelation of integer logistic mapping and integer cubic mapping in a 16-bit processor is shown in Figures 6 and 7.

From Figures 6 and 7, it can be seen that the autocorrelation of logistic and cubic chaotic mappings is poor, which affects their encryption effect. Therefore, the study will use the quantization operation method to enhance the autocorrelation of the two chaotic systems. The autocorrelation of the sequences generated by the quantized hybrid chaotic system is shown in Figure 8, from which it can be found that the autocorrelation image is mainly in the form of impulse function, which indicates that the sequences generated by the quantized hybrid chaotic system have better autocorrelation and can achieve better encryption effect.

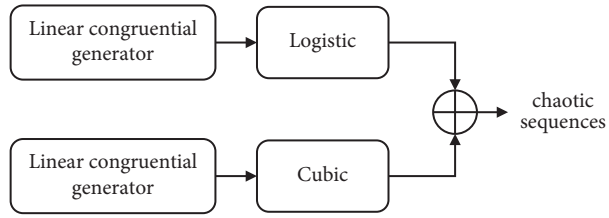

Figure 5: Generation of chaotic sequences.

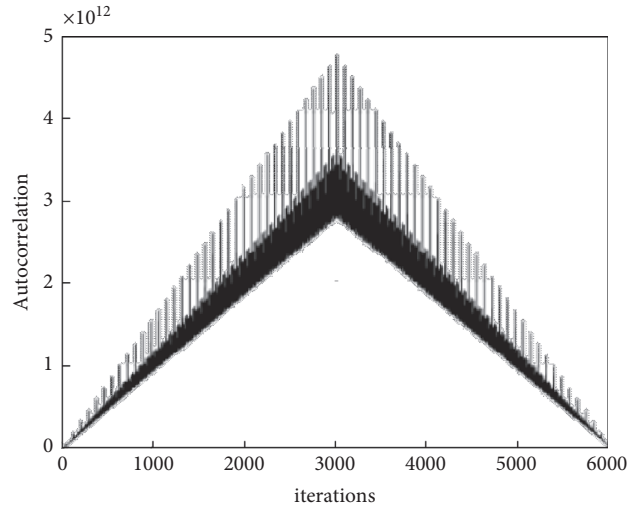

Figure 6: Integer logistic mapping.

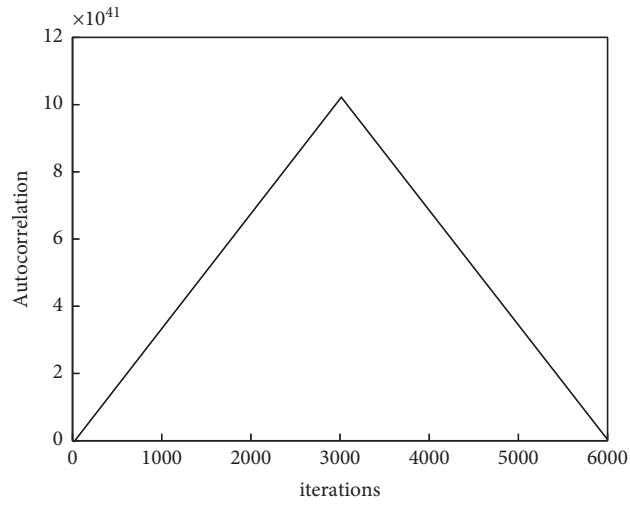

Figure 7: Integer cubic mapping autocorrelation.

An arbitrary 32-bit sequence is selected from the sequence generated by the hybrid chaotic system and divided into two parts of equal length, labeled k_1 and k_2, respectively [20, 21].

As shown in Figure 9, k_1 and k_2 are used as the initial values for generating the round key, the process of which is divided into three main steps, as follows.

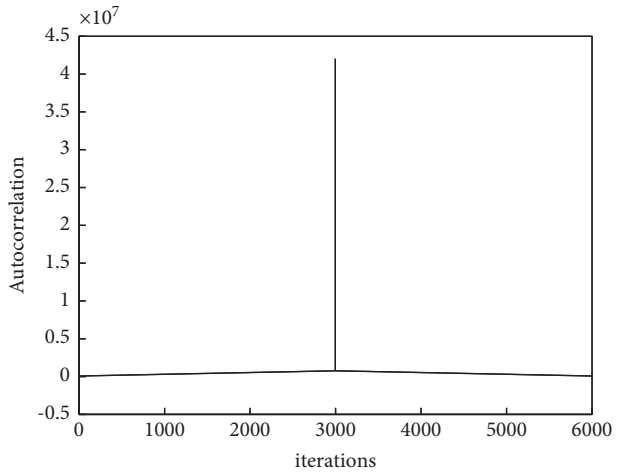

Figure 8: Autocorrelation of chaotic sequences.

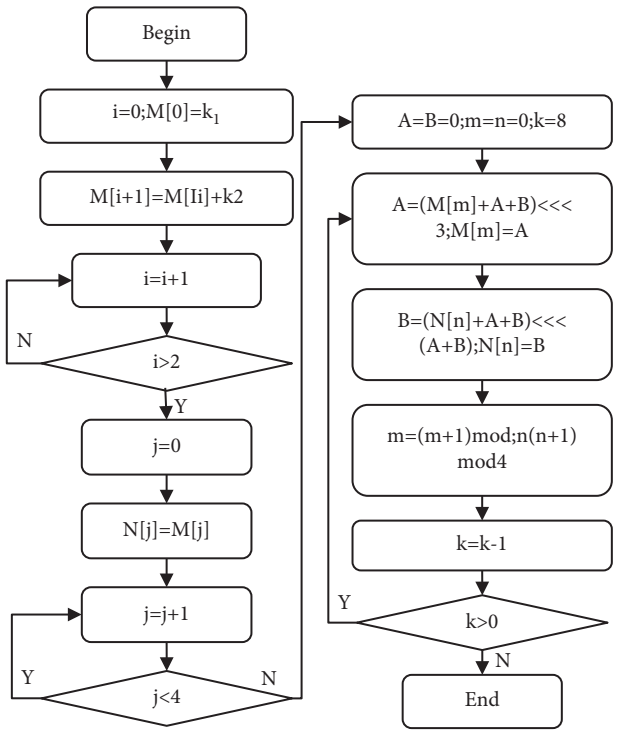

Figure 9: The generation of round key.

(1) The initialization matrix M is generated by k_1 and k_2.

(2) Loop the value of matrix M twice and assign all of them to matrix N afterwards.

(3) Eight shift operations are performed on the matrix and the values in the matrix to obtain the eight round keys needed for encryption.

3.3. Permutation Matrix. In cryptography, the permutation operation is a typical practice whose main function is to complicate the relationship between plaintext and ciphertext. In the chaotic encryption algorithm, the study will be represented by a permutation matrix P:

$$P = \begin{bmatrix} 10 & 7 & 12 & 9 \\ 11 & 5 & 1 & 15 \\ 26 & 23 & 28 & 25 \\ 27 & 21 & 17 & 31 \\ 16 & 13 & 3 & 14 \\ 4 & 6 & 8 & 2 \\ 32 & 29 & 19 & 30 \\ 20 & 22 & 24 & 18 \end{bmatrix}. \tag{15}$$

In the matrix, each parameter is the position of the input sequence. The parameter "10" means that when the input sequence passes through the permutation matrix, the parameter at the tenth position becomes the parameter at the first position of the output sequence. This can be expressed as follows:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{P} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}. \tag{16}$$

3.4. Decryption. From the above cryptographic framework, it is clear that the Feistel structure is a symmetric state and the decryption and encryption steps are roughly the same. The difference lies in the order of using the round keys, such as the order in encryption K_1, K_2, K_3, K_4; conversely, the decryption round key is the reverse of the encryption round key K_4, K_3, K_2, K_1. The decryption is calculated as in equation (15) [22–24]:

$$\begin{cases} L_i = R_{i+1} \oplus F(K_i, R_i), \\ R_i = L_{i+1}. \end{cases} \tag{17}$$

Meanwhile, the substitution inverse matrix P^{-1} can be expressed as

$$P^{-1} = \begin{bmatrix} 11 & 16 & 7 & 13 & 10 & 14 & 2 & 15 \\ 4 & 1 & 9 & 3 & 6 & 8 & 12 & 5 \\ 37 & 32 & 23 & 29 & 26 & 30 & 18 & 31 \\ 20 & 17 & 25 & 19 & 22 & 24 & 28 & 21 \end{bmatrix}. \tag{18}$$

From P^{-1} matrix, we can see that the element in the first position of the input sequence becomes the element in the eleventh position of the output sequence after permutation; if we want to restore the element in the eleventh position of the output sequence to the first position of the input sequence again through the permutation inverse matrix, we need to set the first value of the permutation inverse matrix to 11, and so on, to obtain the permutation inverse matrix.

4. Experimental Results and Analysis

4.1. Experimental Environment. To verify the effectiveness of the proposed algorithm performance, this experiment will be implemented using C program and the algorithm will be applied to the ZigBee platform, which contains 128 KB of ROM, 4 KB of RAM, and a CC2530 microprocessor.

4.2. Algorithm Evaluation Index

4.2.1. Information Entropy. In order to test the performance of hybrid chaotic systems, i.e., to test the system complexity and security, the experiment will use information entropy to verify the performance of chaotic systems. The higher the value of information entropy, the stronger the complexity of the system. That is, the information entropy can effectively measure the system. If the length of the ciphertext is 8 bits, the information entropy is taken to be about 8 for better encryption. The expression of information entropy is as follows [25]:

$$H(x) = \sum_{x} P(x)\log_2 \frac{1}{p(x)}. \tag{19}$$

The entropy of various ciphertext information of different lengths is shown in Table 1.

From Table 1, we can visually see that the ciphertext length is extended from 16000 to 800000, and its information entropy is increased from 7.9642 to 7.9999, which is very close to the standard value of 8. This shows that the ciphertext has strong randomness and also proves that the system has better performance, complexity, and security and can effectively avoid external attacks on network information.

4.2.2. Confusion and Diffusion. In encryption algorithms, confusion and diffusion are the two basic principles that must be followed. Confusion serves to complicate the relationship between the plaintext and the ciphertext, and diffusion, i.e., the maximum impact on the ciphertext through the plaintext, further enhances the security of the ciphertext.

In order to verify the confusion and diffusion effect of the encryption algorithm and to evaluate and assess the performance of the encryption algorithm more objectively, the degree of completeness, degree of avalanche, and degree of strict avalanche are used as evaluation indexes in this experiment.

If an encryption algorithm encrypts a plaintext of n bits into a ciphertext of m bits, the performance of the encryption algorithm is measured using the above three criteria. Completeness represents the existence of correlation between each bit of the plaintext and all bits of the ciphertext species, and the completeness expression is as follows:

$$\mathrm{d}_c = -1\frac{1}{nm}\#\left\{(i, j)|a_{ij} = 0\right\}. \tag{20}$$

The avalanche degree represents that each change of one bit in the plaintext will change at least nearly half of the bits of all ciphertexts, and the avalanche degree expression is as in equation (18):

$$\mathrm{d}_a = 1 - \frac{2}{\#X * nm}\sum_{i=1}^{n}\left|\sum_{j=1}^{m} jb_{ij} - \frac{m}{2}\#X\right|. \tag{21}$$

Table 1: Ciphertext information entropy.

Ciphertext length (bytes)	Information entropy
160.000	7.9642
320.000	7.9765
480.000	7.9835
640.000	7.9926
800.000	7.9999

The strict avalanche degree is the probability that for each bit changed in the plaintext, each bit in the ciphertext is changed at least 50%, which is expressed as follows [26–28]:

$$\mathrm{d}_{sa} = 1 - \frac{2}{\#X * nm}\sum_{i=1}^{n}\sum_{j=1}^{m}\left|a_{ij} - \frac{1}{2}\#X\right|. \tag{22}$$

In the above equation, a_{ij} denotes the i-th row and j-th column element inside the dependency matrix a containing $n*m$ elements, i takes values in the range (1, n), and j takes values in the range (1, m). If the i-th element of the plaintext is changed, the j-th element of the ciphertext changes; then $a_{ij} = 1$; otherwise $a_{ij} = 0.b_{\mathrm{ij}}$ denotes the i-th row and $j + 1$-th column element inside the distance matrix B containing $n*(m + 1)$ elements, i takes values in the range (0, n), and j takes values in the range(0, m). If the i-th element of the plaintext is changed, the plaintext is changed by j bits, and then $b_{ij} = 1$. The symbol X represents the total number of bits in the plaintext; # indicates the summation symbol.

If the values of d_{c}, d_{a}, and d_{sa} meet the criteria of equation (20), it means that the proposed algorithm possesses good results in confusion and diffusion.

$$\mathrm{d}_c = 1, \mathrm{d}_a \approx 1, \mathrm{d}_{sa} \approx 1. \tag{23}$$

The trends of the above three evaluation indexes under different encryption rounds are shown in Figures 10–12.

The change curves of d_{c}, d_{a}, and d_{sa} indicators from Figures 10–12 show that when the number of encryption rounds is 4, d_{a} and d_{sa} show stable trends with no significant change. The optimal number of encryption rounds can be determined to be 4, thus minimizing the resource loss of wireless sensors and ensuring the security of encrypted information.

To further verify the superiority of the proposed encryption algorithm based on hybrid chaotic system, this experiment compares the designed algorithm with the traditional two encryption algorithms of RC5 and RC6 for wireless sensor network for confusion and diffusion, and the comparison results obtained are shown in Table 2.

From the above table, the d_{c} values of all three algorithms are 1, which indicates that the completeness of all three algorithms is good. d_{a} and d_{sa} of the proposed algorithm are 0.998 and 0.999, respectively, which are both higher than those of the other two algorithms, by (0.005, 0.12) and (0.007, 0.009), respectively, compared to the RC5 and RC6 encryption algorithms. This shows that the proposed algorithm is more effective in confusion and diffusion, and the algorithm performs better than the traditional encryption algorithm.

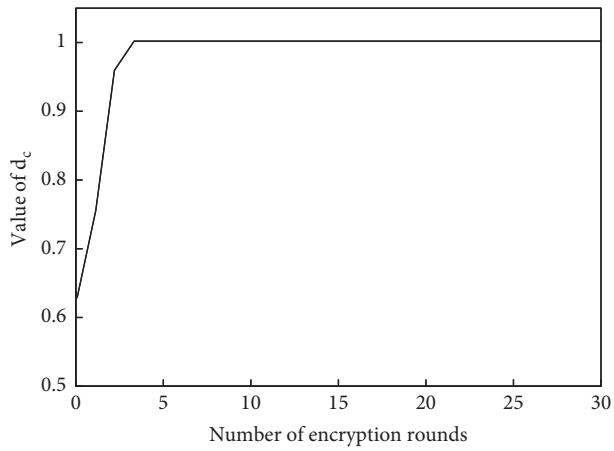

Figure 10: Value of d_c for different number of encryption rounds.

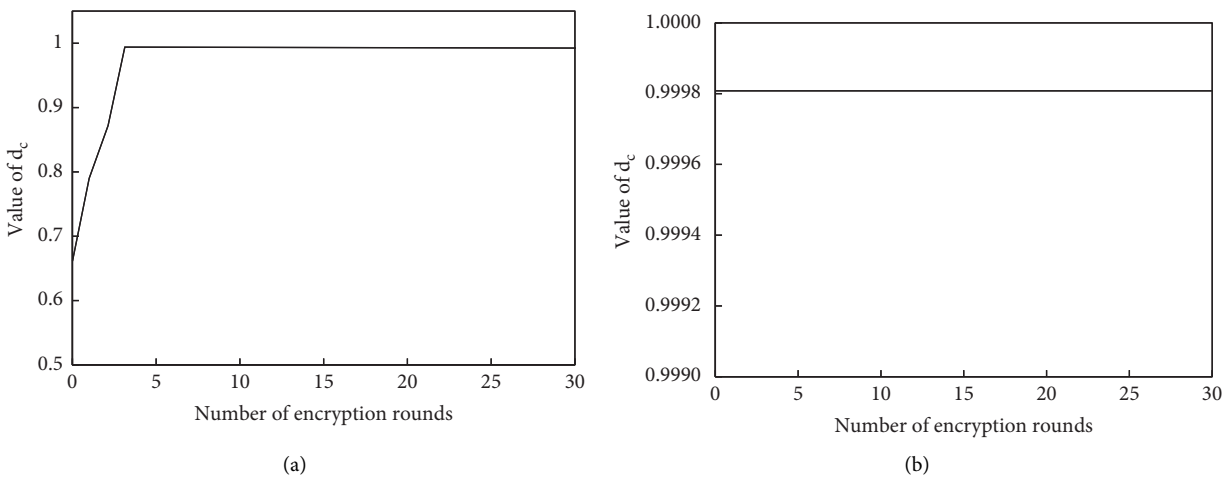

Figure 11: Value of d_a. (a) Encryption from round 1 to round 30. (b) Encryption from round 4 to round 30.

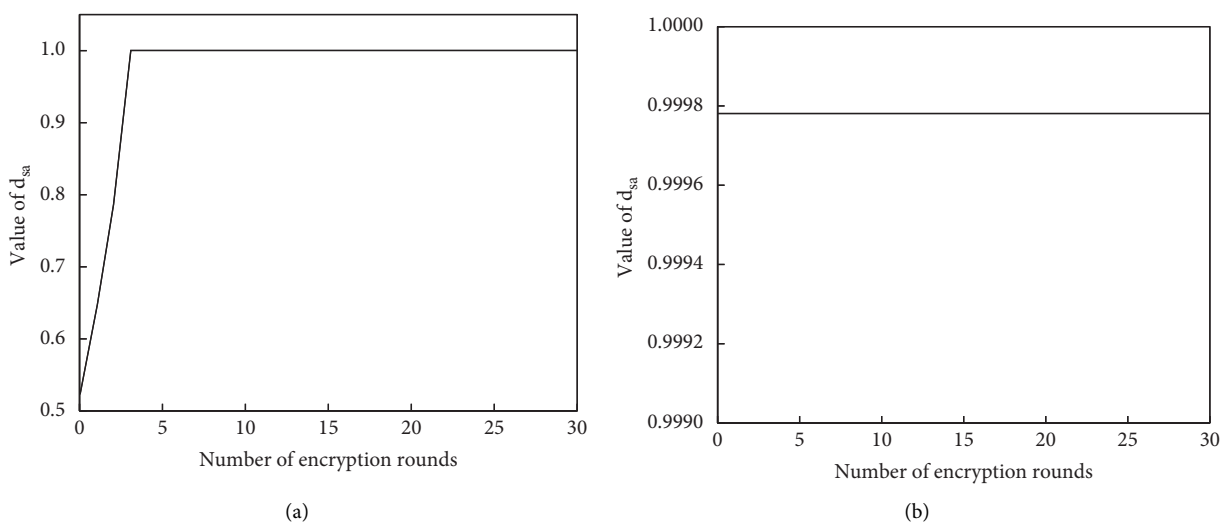

Figure 12: Value of d_{sa}. (a) Encryption from round 1 to round 30. (b) Encryption from round 4 to round 30.

Table 2: Performance comparison of the proposed encryption algorithm and traditional encryption algorithm.

Algorithm	d_c	d_a	d_{sa}
RC5 [29]	1.000000	0.999786	0.999770
RC6 [29]	1.000000	0.999779	0.999799
The algorithm designed in this paper	1.000000	0.999812	0.999772

Table 3: Statistical analysis of "0" and "1."

Length of ciphertext n	Number of "0" k_1	Number of "1" k_2	k_1/n	K_2/n
1,280,000 bits	631,923	648.077	49.369%	50.631%
2,560,000 bits	1,282,425	1,277,575	50.095%	49.905%
3,840,000 bits	1,924.163	1,915,837	50.108%	49.892%
5,120,000 bits	2,557,439	2,562,561	49.950%	50.050%
6,400,000 bits	3,199,671	3,200,329	49.995%	50.005%

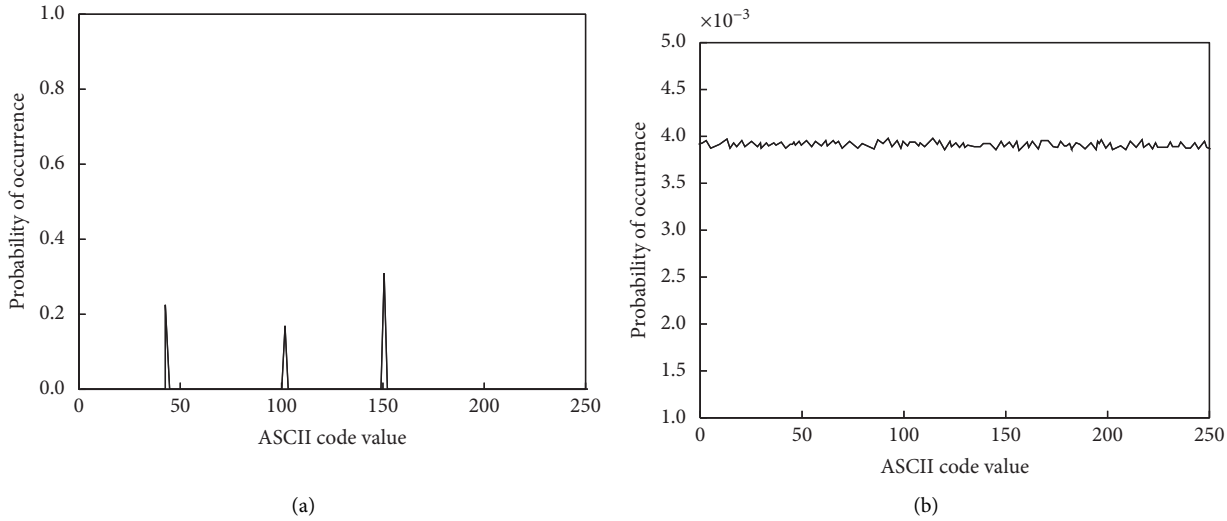

Figure 13: ASCII distributions. (a) Plaintext. (b) Ciphertext.

4.3. Statistical Analysis. In order to verify the randomness of the ciphertext after performing the encryption algorithm, this experiment will perform a statistical analysis of the length of the ciphertext, with 0 and 1 as the criteria, and the number of ciphertexts is 0 or 1, indicating that they are roughly the same. The statistical analysis table is shown in Table 3.

From the above table, it can be seen that after encryption by encryption algorithm, ciphertext of different lengths can be obtained. The number of "0" and "1" in the ciphertext is very close to each other and gets closer after increasing the length continuously, indicating that the ciphertext data achieve the 0-1 balance objective.

In the plaintext, the ASCII distribution is uneven. After encryption, the ASCII distribution gradually tends to be homogeneous, which means that the encryption algorithm can effectively defend against probabilistic attacks. The ASCII distributions of both are shown in Figure 13.

As can be seen from the above graph, the plaintext ASCII distribution shows a large undulating peak at 50, 100, and 150, indicating a higher probability of aggressiveness and a lower defensibility in the plaintext, which makes it vulnerable to external intrusion and threats. After encrypting the plaintext, the ASCII code values shown in Figure 13(b) are obtained. It can be seen that the probability of ASCII code values is all around 40%, which indicates that they are very evenly distributed and further proves that the encrypted ciphertext is more defensive and less likely to be attacked.

4.4. SP 800-22 Test. In order to test whether the ciphertext sequence is secure after using the encryption algorithm, this experiment is conducted to test 15 information security items of SP800-22. There are 1 million bytes in this ciphertext, and it is divided into 400 copies equally. The test results of this information are as follows. If all the P values in the table are more than 0.01, it indicates that the ciphertext sequence information meets the criteria.

As can be seen from Table 4, the P values of the ciphertext sequences are all above 0.01, with the lowest being 0.012351 and the highest being 0.943113. The experimental results show that all the above sequences meet the standard

Table 4: SP 800-22 test.

Statistical test	P value	Result
Frequency	0.403216	PASS
Block frequency	0.943113	PASS
Cumulative sums (forward)	0.409276	PASS
Cumulative sums (reverse)	0.545923	PASS
Runs	0635289	PASS
Longest run	0.246932	PASS
Rank	0.513486	PASS
FFT	0.160782	PASS
Nonoverlapping template	0.172193	PASS
Overlapping template	0.194653	PASS
Universal	0.775S69	PASS
Approximate entropy	0.764231	PASS
Random excursions	0.812351	PASS
Random excursions variant	0 797955	PASS
Serial (P value1)	0.667959	PASS
Serial (P value2)	0.791328	PASS
Linear complexity	0.401947	PASS

Table 5: Comparison results of running speed and memory consumption of the three algorithms.

Encryption algorithm	Speed (byte/ms)	Memory (bytes) consumption
RC5 [29]	12.82	268
CWSN [30]	16.58	160
The algorithm designed in this paper	18.51	96

and satisfy the requirements of wireless sensor information security protection.

4.5. Running Speed and Memory Consumption. In order to test the suitability of the designed encryption algorithm in wireless sensor networks, the experiment will test the algorithm in terms of its running time and memory consumption and compare the algorithm with the traditional encryption algorithms RC5, SKIPJACK, and CWSN to obtain the following results.

It is obvious from Table 5 that the designed algorithm runs at 18.51byte/ms, which is 5.7, 7.28, and 1.93 higher than that of the other three algorithms, respectively, indicating that the algorithm runs faster; the memory consumption of the proposed algorithm is 96, and that of the other three algorithms is 268, 356, and 160, which exceeds that of the algorithm proposed in the study by 172, 260, and 64. After comprehensive analysis, it is shown that the proposed algorithm runs the fastest and takes up the least memory in wireless sensor networks and is very suitable for the operation of wireless sensor network.

5. Conclusion

In summary, the proposed identity encryption algorithm for hybrid chaotic systems can be applied to wireless sensor network security protection, which can solve the problems of complex node resources and small memory of wireless sensor networks, and the algorithm can further enhance the defense capability of ciphertext and reduce the attack probability. The experimental results suggest that with different ciphertext lengths, the ciphertext information entropy is close to 8 after using the improved encryption algorithm, the ciphertext randomness is significantly improved, and the performance of the hybrid chaotic system is enhanced. With the number of ciphertext encryption rounds close to 4, the resource loss of the wireless sensor network is minimized, thus simplifying the network nodes, reducing the computational cost, and improving the network security. Finally, after comparing the proposed algorithm with the traditional encryption algorithm, it is found that the improved algorithm has better confusion and diffusion effects than the traditional algorithm, and the algorithm has better performance. The operation speed is faster than that of other algorithms, and the memory consumption is smaller. Comprehensively, it can be seen that the proposed algorithm can be applied and promoted in wireless sensing networks. However, due to the experimental conditions and insufficient research experience, this experiment only encrypted text information, and the proposed algorithm cannot encrypt images and other types of information well, and thus there are certain limitations, and in the future, we will start from this aspect and apply the algorithm to information such as images and videos to improve the performance and applicability of the algorithm.

Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] B. Maram, J. M. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for UNICODE data privacy and security in IOT," *Service Oriented Computing and Applications*, vol. 13, no. 1, pp. 3–15, 2019.

[2] A. Ahmad, N. A. Muhammad, M. Zeyad, and A. Bareeq, "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 1, pp. 65–81, 2019.

[3] C. Liang, Q. Zhang, J. Ma, and K. Li, "Research on neural network chaotic encryption algorithm in wireless network security communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–10, 2019.

[4] A. P. Deng and B. Xiao, "Application of chaotic encryption algorithm in RFID secure mechanism," *Advanced Materials Research*, vol. 532-533, no. 532-533, pp. 1695–1699, 2012.

[5] X. Zhang, S. Yu, P. Chen, J. Lü, J. He, and Z. Lin, "Design and ARM-embedded implementation of a chaotic secure communication scheme based on H.264 selective encryption," *Nonlinear Dynamics*, vol. 89, no. 3, pp. 1949–1965, 2017.

[6] J. Ge, Z. Sheng, L. Lang, and Z. Yi, "Hybrid chaotic encryption algorithm for securing DICOM systems," *International Journal of Performability Engineering*, vol. 15, no. 5, pp. 1436–1444, 2019.

[7] T. Wu, C. Zhang, Y. Chen et al., "Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission," *Optics express*, vol. 29, no. 3, pp. 3669–3684, 2021.

[8] Z. Zhang and S. Yu, "On the security of a Latin-bit cube-based image chaotic encryption algorithm," *Entropy*, vol. 21, no. 9, p. 888, 2019.

[9] M. Noor, K. Majid, J. S. Sajjad, and M. H. Mohammad, "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map," *Mathematics and Computers in Simulation*, vol. 190, pp. 826–836, 2021.

[10] G. Qiu, C. Wang, S. Luo, and W. Xu, "A dual dynamic key chaotic encryption system for industrial cyber-physical systems:LETTER," *IEICE Electronics Express*, vol. 17, no. 24, p. 20200389, 2020.

[11] Q.-y. Zhang, Y.-z. Li, and Y. jie Hu, "A retrieval algorithm for encrypted speech based on convolutional neural network and deep hashing," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 1201–1221, 2020.

[12] F. Wang, B. Zhu, K. Wang, M. Zhao, L. Zhao, and J. Yu, "Physical layer encryption in DMT based on digital multi-scroll chaotic system," *IEEE Photonics Technology Letters*, vol. 32, no. 20, pp. 1303–1306, 2020.

[13] L. Yin and N. Hassan, "Multi-level encryption algorithm for user-related information across social networks," *Open Physics*, vol. 16, no. 1, pp. 989–999, 2018.

[14] X. Wang and S. Chen, "Chaotic image encryption algorithm based on dynamic spiral scrambling transform and deoxyribonucleic acid encoding operation," *IEEE ACCESS*, vol. 8, pp. 160897–160914, 2020.

[15] M. Wang, X. Wang, Y. Zhang, and Z. Gao, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models," *Optics & Laser Technology*, vol. 108, pp. 558–573, 2018.

[16] Yi Kang, L. Zhang, and D. Zhang, "Study of an encryption system based on compressive temporal ghost imaging with a chaotic laser," *Optics Communications*, vol. 426, pp. 535–540, 2018.

[17] Y. Xiao, J. Cao, Z. Wang, and C. Long, "Polar coded optical OFDM system with chaotic encryption for physical-layer security," *Optics Communications*, vol. 433, pp. 231–235, 2018.

[18] L. Kraleva, V. Rijmen, and N. L. Manev, "Correlation Distribution Analysis of a Two-Round Key-Alternating Block Cipher," *Tatra Mountains Mathematical Publications*, vol. 73, no. 1, pp. 109–130, 2019.

[19] C.-S. Chen, X. Yu, Y. X. Xiang, X. Li, and T. Li, "An improved DPA attack on DES with forth and back random round algorithm," *International Journal on Network Security*, vol. 19, no. 2, pp. 285–294, 2017.

[20] J. Wang, H. Xu, and M. Yao, "Improvement of the round key generation of AES," *International Journal of Communications, Network and System Sciences*, vol. 05, no. 12, pp. 850–853, 2012.

[21] Y. Luo, D. Zhang, and J. Liu, "A chaotic block cryptographic system resistant to power analysis attack," *International Journal of Bifurcation and Chaos*, vol. 29, no. 8, p. 13, 2019.

[22] H. Mai, E. E. Rabaie, M. E. Ibrahim, and F. E. Samie, "3-D image encryption based on rubik's cube and RC6 algorithm," *3D Research*, vol. 8, no. 4, 2017.

[23] E. B. Villanueva, B. G. Gerardo, and R. P. Medina, "Implementation and performance assessment of the enhanced RC5 (ERC5) algorithm based on addition-then-append key expansion technique[J]," *IOP Conference Series: Materials Science and Engineering*, vol. 482, no. 1, 2019.

[24] A. Abidi, C. Guyeux, and M. Machhout, "Statistical analysis and security evaluation of chaotic RC5-CBC symmetric key block cipher algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 10, 2019.

[25] S. Kumar, K. Patidar, R. Kushwah, and S. Chouhan, "Text data partitioning and image based RC5 encryption with block based key generation," *International Journal of Advanced Technology and Engineering Exploration (IJATEE)*, vol. 4, no. 31, 2017.

[26] V. Manikandan and R. Amirtharajan, "On Dual Encryption with RC6 and Combined Logistic Tent Map for Grayscale and DICOM," *Multimedia Tools and Applications*, vol. 80, pp. 1–30, 2021.

[27] A. I. Sallam, E.-S. M. El-Rabaie, and O. S. Faragallah, "CABAC-based selective encryption for HEVC using RC6 in different operation modes," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28395–28416, 2018.

[28] R. Rajoriya, K. Patidar, and S. Chouhan, "An efficient image encryption algorithm based on RK-RC6," *ACCENTS Transactions on Information Security (TIS)*, vol. 3, no. 9, 2018.

[29] Y. Chen, S. Su, H. Yin et al., "Optimized non-cooperative spectrum sensing algorithm in cognitive wireless sensor networks," *Sensors (Basel, Switzerland)*, vol. 19, no. 9, p. 2174, 2019.

[30] P. S. Chatterjee and M. Roy, "Maximum match filtering algorithm to defend spectrum-sensing data falsification attack in CWSN," *International Journal of Wireless and Mobile Computing*, vol. 15, no. 2, pp. 113–122, 2018.