Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7203237, 14 pages
https://doi.org/10.1155/2022/7203237

Research Article

Encryption Management of Accounting Data Based on DES Algorithm of Wireless Sensor Network

Zixin Lu

School of Business, Shandong Normal University, Jinan, 250358 Shandong, China

Correspondence should be addressed to Zixin Lu; lzx@sdnu.edu.cn

Received 27 October 2021; Revised 28 November 2021; Accepted 8 December 2021; Published 4 January 2022

Academic Editor: Haibin Lv

The emergence of wireless sensor networks connects the physical world with the information world and changes the way humans interact with nature. With the rapid development of modern information technology, accounting information systems (AIS) have emerged at the historic moment. Under the information environment, accounting data exists in paper or paperless form. The use of information technology not only brings convenient and efficient services to enterprises but also has a huge impact on the internal control of the enterprise. Because the network is open and unstable, the system is vulnerable to illegal intrusion and viruses. Based on the above background, the research content of this article is to use DES algorithm to encrypt accounting data. DES (Data Encryption Standard) encryption algorithm is a symmetric password encryption method. It has the advantages of fast encryption speed, simple and practical algorithm, and consideration of both security and efficiency requirements. This paper discusses the application of DES encryption technology to accounting data processing. To achieve data security management goals. Therefore, this paper proposes a DES algorithm based on the logistic chaotic system. Through experimental simulation, the results show that the chaotic discrete model has initial value sensitivity and iterative nonrepetition. The resulting key space is independent and random. In the application, you can perform random key input according to the performance of software and hardware, which is flexible; there is only one “1186828” in the initial DES algorithm encryption process, but each set of plain text in the improved DES algorithm corresponds to a corresponding set of keys and independence. The test results show that they are maintained between 5 and 6.6. It is proved that using the initial value sensitivity of the logistic system and using the initial value as the key can realize the secure management of accounting data on the premise of ensuring efficiency.

1. Introduction

With the rapid development of wireless Internet technology, wireless sensor networks have been widely used in various fields of society. The emergence of wireless sensor networks connects the physical world with the information world and changes the way humans interact with nature. The security goal of data fusion is to ensure that users or base stations can obtain the final data fusion results and at the same time to ensure that these data fusion results are accurate and can be received by users, which requires the application of corresponding security data fusion solutions to be effective. It resists different types of attacks and can accomplish various security goals under limited resources and environmental conditions. With the development of network information technology, the production and operation activities of enterprises have undergone tremendous changes. In recent years, with the rapid development of the Internet, companies have gradually launched e-commerce business; transactions using the Internet have become an irreplaceable development trend. Enterprise accounting has also undergone tremendous changes. Under the network environment, accounting goals, accounting functions, accounting operation methods, and accounting supervision are all changing and developing in the direction of adapting to the new network economy. A wireless sensor network is a form of network formed by freely organizing and combining tens of thousands of sensor nodes through wireless communication technology. The units constituting the sensor node are as follows: a data acquisition unit, a data transmission unit, a data processing unit, and an energy supply unit.

With the development of the network, the users of accounting information have become more extensive, and the accounting operation methods and supervision methods have become more advanced. Based on this situation, network accounting emerged at the historic moment [1–4]. The emergence of network accounting first changed the way of accounting operation; accounting changed from manual operation stage to computer operation [5, 6]. The emergence of financial software has changed the state of separation of finance and business in the manual mode and realized integrated management and coordination of financial operations [7–9]. Finally, in the network environment, the accounting information of enterprises is no longer like the information island [2, 10] form of accounting information under manual accounting [11, 12]. Its accounting information system is closely connected with the internal and external as a whole, and information users can obtain their required accounting information through the network [13, 14]. However, the development of network technology has brought convenience and risks to corporate accounting. Due to the risk of the network environment, the security of accounting information has become increasingly important [15, 16]. Considering the current status of accounting data security, in the data encryption algorithm, the DES algorithm has certain advantages, so it has certain research value [17–19].

Encryption has become a necessity of life, especially in the field of exchanging and transmitting data through transmission media. Serwe introduced two formal models of the Data Encryption Standard (DES) [20, 21], the first using the international standard LOTOS and the second using the latest process to calculate LNT. Both models encode DES in the form of asynchronous circuits; that is, the data stream blocks of the DES algorithm are represented by processes that communicate through rendezvous points. In order to ensure the correctness of the model, Serwe applied a variety of techniques, including model checking, equivalence checking, and comparing the results generated by the prototype automatically generated by the formal model with the existing implementation of DES to verify the correctness of the model [22, 23]. His research in DES is very in-depth, but if combined with the application of wireless sensor networks in DES, the value of this article is higher. Aiming at the security problems of the typical shielded Data Encryption Standard (DES) implementation, Wenqing et al. introduced a correlation power analysis (CPA) method that combines the last two rounds of the DES algorithm and selects the discrete bits of the intermediate data as the objective function. Using the Hamming Weight (HW) model, it guesses the 16th round of DES keys and calculates the correlation between data and hardware. By sorting the related values, it can destroy the masked DES key. The experimental result of using the shielded software to attack the smart card is DES, indicating that CPA can successfully crack the 64-bit DES key [24, 25]. Template security is a crucial issue in biometric recognition systems. The existing technology uses hand vein and palm vein patterns to build fuzzy libraries for multibiometric recognition. However, the security involved in converting feature points to vault is not satisfactory. Lalithamani et al. used a combination of AES (Advanced Encryption Standard) and DES (Data Encryption Standard) for this. First, use the AES algorithm to encrypt the characteristic points of the palm and hand vein, then provide the private key generated by AES algorithm to DES algorithm for encryption, and finally use multimode biometric template and key to generate fuzzy library [26]. The comparison of the results with traditional techniques shows that the technique proposed by Lalithamani et al. achieves better results when the GAR reaches 90% in the absence of noise and noise. Lalithamani et al.'s technology provides good security for pattern-based biometrics [27–29]. All of the above references are related to DES and wireless sensor networks. Although the two technologies are not combined and applied, they still have a certain reference value for this article.

Based on the background and significance of accounting data security, this paper analyzes the research status of DES algorithm and the research status of chaos. Based on the characteristics of DES and chaos, it studies the related content of DES algorithm and logistic chaotic system. Based on the above content, this paper proposes a DES key generation algorithm based on the logistic chaotic system. The improved principle and method of generating DES key by logistic chaotic system are given. The feasibility of the algorithm is verified on Matlab, and the improvement of the algorithm is summarized. The experimental results show that using the initial value sensitivity of the logistic system and using the initial value as the key can increase the difficulty of malicious deciphering, so the security of the encryption system is significantly improved, and the performance of the DES algorithm during the encryption/decryption process is avoided. The shortcomings and some improvements have been achieved in the security of the DES algorithm. Although the DES key has very powerful encryption and decryption capabilities, it requires a lot of calculations to maintain the continuity of its algorithm and requires very high computational processing capabilities.

2. Proposed Method

2.1. Data Encryption Technology Processing Classification. The so-called data encryption technology refers to the conversion of an information through an encryption key and an encryption function into a meaningless ciphertext, and the receiver restores the ciphertext into plaintext through a decryption function and decryption key. Encryption technology is the cornerstone of network security technology.

(1) Symmetric key encryption technology: the encryption algorithms of the symmetric cryptosystem mainly have two basic algorithms: block cipher and sequence cipher. Among them, block without cipher is mainly for 64-bit data, and the 64-bit plain text data is encrypted. There are no restrictions on the

data flow of plaintext and ciphertext in the sequence cipher algorithm.

(2) Asymmetric key encryption technology: asymmetric key encryption technology is a public key encryption system. That is, anyone can deliver the letter from the entrance of the mailbox, but only the legal person who has the correct key can get the letter. The entrance to the letter is the public key, and the key to the mailbox is the private key. The encryption process of this algorithm is one-way. Even if the data is intercepted during transmission, because the intruder does not have the private key, the plaintext information of the data will not be obtained. The advantage of the RSA algorithm is that the principle is simple and easy to use. Even if it communicates secretly with multiple users, it does not need to remember too many keys. RSA can be used for data encryption and digital signatures because it uses keys that can vary in length. The disadvantage is that the implementation of the RSA algorithm has a lot to do with the speed of the computer, and the overall efficiency is relatively low.

(3) Hybrid encryption technology: although symmetric key algorithms have advantages such as high efficiency and high strength, the management of keys is too complicated and insecure; asymmetric key encryption algorithms have advantages in key management, but they are extremely inefficient and difficult to analyze. Bulk data encryption. In practical applications, the two encryption algorithms are often used in combination, so that the security of the asymmetric key encryption system and the high efficiency of the symmetric key system are obtained at the same time.

(4) Zero-key encryption technology: zero-key encryption technology is also called random key encryption technology. The two parties of communication do not use a fixed password but generate a key randomly every time, and the key is used only once. It does not have a key, but does not have a key transmission, which greatly reduces the risk of the key being leaked, and also saves the management and transmission costs of the key. The disadvantage is that the algorithm design is difficult, and at least three to four encryption and decryption operations are required.

2.2. DES Algorithm. Symmetric cryptography represented by DES is an important cryptosystem in the field of information security. In the symmetric encryption algorithm, the data sender processes the plaintext (original data) and the encryption key together with a special encryption algorithm to make it a complex encrypted ciphertext and send it out. After receiving the ciphertext, if the recipient wants to interpret the original text, it needs to decrypt the ciphertext with the used encryption key and the inverse algorithm of the same algorithm to restore it to a readable plaintext. Compared with public key cryptography, symmetric cryptography has low computational cost and relatively simple algorithm, so it has been widely used in the industry. The DES algorithm has also been improved to an algorithm. The speed of encrypting each block of information with three different sets of keys is reduced by one-third, and the new ciphertext block is connected with the previous ciphertext block and then encrypted, which has very good effect. Since the DES algorithm is completely open, its security completely depends on the protection of the key. Therefore, it is not suitable to be used alone in a network environment. By regularly switching to new ones at the source and destination ends of the communication network at the same time, the confidentiality of data can be further improved, which is the current popular practice in financial transaction networks. Through the analysis of the encryption process and specific implementation steps of the DES algorithm and the long-term attacks on the DES algorithm, it can be seen that the internal structure and design of the DES algorithm are almost perfect and will not cause the DES algorithm to be insecure. For online analysis of DES algorithm, there are

$$F_{\chi} \geq \frac{1}{m}\sum_{i=1}^{N}\sum_{e=0}^{i=1}\left(1-\frac{it}{m}\right)^{e+1}, \tag{1}$$

$$F_{\chi}^{\mathrm{all}} \geq 1-\left(1-\frac{1}{m}\sum_{i=1}^{n}\sum_{e=0}^{i=1}\left(1-\frac{it}{m}\right)^{e+1}\right)^{i}. \tag{2}$$

t represents the number, and n represents the number of rows. With the increase of m and t, the success rate does not increase year-on-year. The trend is to increase faster in the low success rate stage. When two nodes collide, they form a chain merger. Calculate this merger probability; then, there is

$$\begin{gathered} F_c = 1-\prod_{i=1}^{t}\left(1-\frac{N_i}{m}\right), \\ f_i(e) = e_i(F_e(f)). \end{gathered} \tag{3}$$

When $n_i = n_1$, the maximum expected success rate can be expressed as

$$F_{\max} = 1-\left(1-\frac{n_{\max}}{m}\right)^{i} \approx 1-e^{-i(n_{\max}/m)} \approx 1-e^{-2i}. \tag{4}$$

The above formula conforms to the situation that it is almost impossible to generate a loop in the chain, which can reduce the space waste caused by storing duplicate nodes, which is expressed by the formula as

$$Q_{xy} = g\left(Q_{x,y-1}\right) = E\left(P_{ax,j-1}(R_0)\right)(1 \leq y \leq t), \tag{5}$$

$$P\left(Q_{ax,y-1}(R_0)\right) = \left(Q_{ax,y-1}(R_0)+y-1\right) \bmod M, \tag{6}$$

$$p_h = \frac{N_{x-h+1}}{m}\left(\prod_{x=r=h+2}^{i}\left(1-\frac{n_i}{M}\right)\right). \tag{7}$$

Assuming that the number of iterations is less than $t(t-1)/2$, the number of y substitutions is always less than or equal to t, the expected number of iterations is calculated, and the formula is expressed as

$$T = \sum_{h=1}^{i}\frac{n_{x-h+1}}{M}\left(\prod_{x=1-h+2}^{i}\left(1-\frac{n_i}{M}\right)\left(\frac{h(h-1)}{2}\right)\right), \tag{8}$$

$$T(p_{h-1}) \leq \sum_{i=1}^{n}\sum_{e=1}^{h-1}\left(\frac{e}{M}\right) = \frac{nh(h-1)}{2M}. \tag{9}$$

p_{h-1} is the upper limit of the probability of occurrence of the event. According to the different chain e, the number of false alarms is calculated; then, there is

$$T(p_h) \leq R(P_{h-1}) + \frac{1}{\delta}\sum_{i=1}^{\delta=1} I \quad (i-1), \tag{10}$$

$$E = \sum_{i=1}^{n}\sum_{r-1}^{h-1}\left(\frac{r}{M}\right) + \frac{\delta-1}{2} = \frac{nh(h-1)+M(\delta-1)}{2M}. \tag{11}$$

For the case of multiple tables of the same scale, the depth-first search method is $\delta - 1/2$, and the probability of each table is the same and equal to r/M, and the encryption process can be expressed as

$$F_i = U_{i-1} \oplus (F(U_{i-1}, L_{i-1})) = U_{i-1} \oplus (P(F(U_{i-1}, L_i \oplus (R(F_{i-1}))))), \tag{12}$$

$$a(0+1) = \cos\,(a(m)), \quad -1 \leq a(0) \leq l_1, \tag{13}$$

$$w(a,b) = \begin{cases} (2a, \delta y), & 0 \leq a \leq 0.1, \\ (2a-1, \delta y + 0.1), & 0.1 \leq y \leq 0.2. \end{cases} \tag{14}$$

Transform and fold the plane area into a δy matrix, and enter the uniform distribution value a. At this time, the system is far from the initial state, and a real-valued chaotic sequence is established to represent it as a discrete chaotic system:

$$a_{m+1} = \beta A_m (1 - a_m), \tag{15}$$

$$V(a) = \sum_{i=1}^{2^{\beta}-1} g(a_i)\log\frac{1}{g(a_1)}\phi, \tag{16}$$

$$g(b) = \sum_{i=m^o}^{l_{\max}} g(m=h)\left(1-j^{(h-1)(h-2)/1}\right)^h\Bigg). \tag{17}$$

$l_{\max}$ is the largest scale. Any node collects data and divides it into $2^{\beta}-1$ parts. The probability of data being affected is

$$\beta_i = x_i a_i + s_i m, \phi_i = L(\beta_i|h|t\beta_i|\phi_i), \tag{18}$$

$$\phi_i = \prod_{i=1}^{t} b_i = \delta^{-n} \otimes \delta^{n-1} \bmod i^2, \tag{19}$$

$$\frac{A_t - A_{t-1}}{i_t} = \frac{i_t \otimes A_{t-1}(n-1)}{i_t} = n_t. \tag{20}$$

The above formula is a recursive algorithm, A is the collection of all node data, and ϕ_i implements algorithm decryption. Each node of the wireless network sensor uses data fusion technology to perform ciphertext strategy attributes on it. This process can be expressed as

$$G(l_{i,o}^2) = \iint (u^2+v^2) f(u,v) lulv = a^2 f(a,\eta) ala\eta, \tag{21}$$

$$G(l^2) = f\int_{\eta=0}^{2\pi} a - \sqrt{a_{i-1} = o, a^3\eta} = \frac{f}{2\pi}\frac{A^4}{2l^2}, \tag{22}$$

$$G(L) = dE_{\text{elec}} + dE\int\frac{1}{2\pi}\frac{a}{h}. \tag{23}$$

The density function of the inner node distribution is $l_{i,o}$. In this area, the average distribution of all nodes is expressed as (u, v); the energy consumption control of the nodes is calculated as

$$l_i = \sum_{a\neq 1}\sqrt{(u_a-u)^2+(v_a-v)^2} \otimes \sum_{a\neq 1} l_{uv}, \tag{24}$$

$$u_a(o+1) = a^{1-i}(o+1)a\frac{u_{i-1}(i)-a(i)}{\|\eta(u-v)\|}. \tag{25}$$

l_i is the radius of the decision domain; o is the actual position of the beacon node.

2.2.1. Principle Analysis of DES Algorithm. DES is a kind of mathematical operation designed for binary coded data, which can password protect computer data. DES makes the relationship between the statistical properties of the ciphertext and the value of the key as complicated as possible, so that the dependence between the key, the plaintext, and the ciphertext is unavailable to the cryptanalyst. The way to implement the DES algorithm includes software implementation of software installed on the host computer and hardware implementation in related communication devices. Its structure is shown in Figure 1.

The input of the DES algorithm includes 64-bit input (Data), 56-bit key (Key), and working mode (Mode). Data is the plain text that needs to be encrypted or ciphertext that needs to be processed; Mode is the working mode of DES: encryption and decryption. When Mode is encrypted, Data is plain text, and it is encrypted with key to generate the corresponding ciphertext as the output result. When Mode is decrypted, Data is ciphertext, and it is decrypted with Key to generate the corresponding Plain text as the result of the

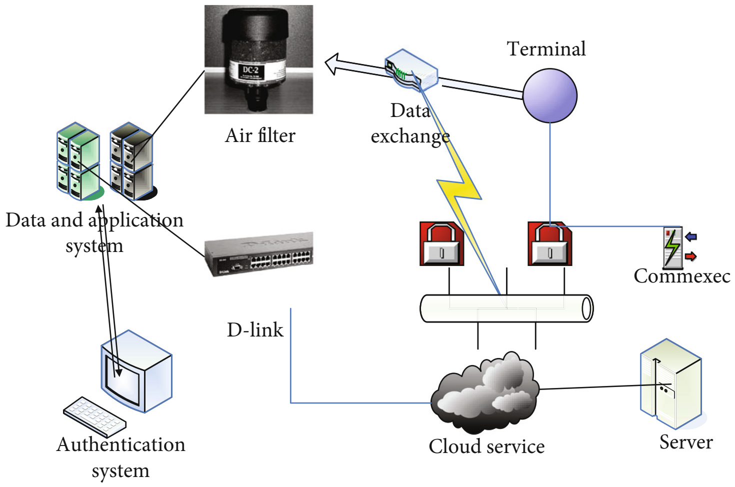

Figure 1: DES algorithm structure diagram.

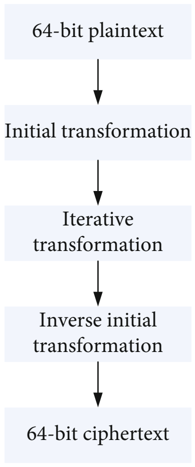

Figure 2: The structure of DES algorithm.

output. The structure of the DES algorithm is shown in Figure 2.

As shown in Figure 2, the DES algorithm first divides the plaintext encoding into several 64-bit packets. The algorithm takes one packet as plaintext input at a time and divides the plaintext into left (L0) 32-bit and right (R0) 32-bit through initial permutation (IP). And then there are 16 rounds of iterative operations. The key of DES encryption is 64 bits, but because there are 8 bits as parity bits, it can be ignored. In the iterative operation, the 56-bit key is used to generate a 48-bit subkey through the key generation system. The data is combined with the subkey to perform the F-function operation. After 16 rounds of iterative operations, the left and right parts are combined and then the reverse initial replacement (IP); output a 64bit ciphertext packet. The 16-round iterative transformation operation principle is shown in Figure 3.

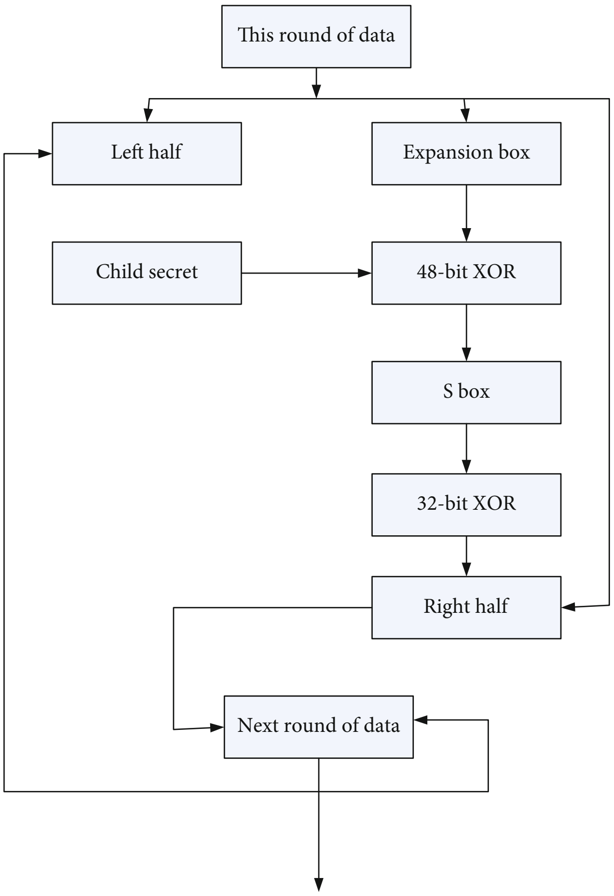

Figure 3: The schematic of a single iteration.

In each round of operation, the key generator generates a 48-bit subkey Ki from the 56-bit key. The right half of the data is expanded to 48 bits by an extended permutation, and the subkey is then XORed with the right half of the bit. Then, using the eight S-boxes, the 48-bit XOR result is converted into 32-bit, and then output after 32-bit permutation operation. These four steps constitute function. Then, through another XOR operation, the output of the function is combined with the left half, and the result becomes the new right half. The calculation formula for each round is

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i). \tag{26}$$

The original right half becomes the new left half. Repeating this operation 16 times, 16 rounds of iterative operations of DES are realized.

2.2.2. Initial Sequence Transformation. The main purpose of the initial replacement is to make it easier to put the plaintext and ciphertext data into the DES iterative operation according to the size of 64-bit bytes. The input 64-bit packet plaintext (Data) is initialized by an algorithm (IP replacement). Convert Data to IP-Data, and allocate IP-Data left and right: L0 = the first 32-bit data, and R0 = the last 32-bit data. The position of the table is exchanged with the bits of the original data according to the initial value; until each bit of the packet plaintext (Data) is replaced.

2.2.3. Generation of Subkeys. The core of the DES encryption algorithm is to believe that complex iterative operations can produce chaotic effects. So 16 rounds of iterative operation in DES algorithm is very important. Since each iteration operation is participated by the subkey generated by the original key, the subkey generated by the original key and the process of generating the subkey are very important to the entire system. According to the key generator in the DES algorithm design, each original key will generate 16 corresponding subkeys, that is, k1, k2, k3, ⋯, k16. Each subkey has a length of 48 bits. After replacement, selection was formed by a shift operation. For a 64-bit original key, if it is divided into 8 groups of 8-bit key blocks, the last byte of each packet can be regarded as a parity byte. Therefore, for a 64-bit original key, it is believed that only 56 bits are actually involved in the encryption process. The 64-bit original key is numbered, from left to right, which are l to 64 bytes; then according to the above, the number of the check bit is $i \times 8$, $i = 1, 2, 3, 4, 5, 6, 7, 8$. The specific calculation steps for the subkey are as follows:

(1) Excluding the parity bits, the numbers of the non-parity bits of the original 64-bit key are 1-7, 9-15, 17-23, 25-31, 33-39, 41-47, 49-55, and 57-63. After the first permutation selection, it is divided into two parts, left and right, each with 28 bits, denoted as L0 and R0

(2) Cyclically shift L0 and R0 by one bit to the left to generate key strings L1 and R1, respectively

(3) L1 and R1 generate the subkey k1 used in the first round of iterative operation after the second permutation selection

(4) Cyclically shift L1 and R1 to the left by one bit to generate key strings L2 and R2, respectively

(5) After the second permutation selection, L2 and R2 generate the subkey k2 used in the second round of iterative operation

Continuing the above steps, the sub-keys k3 to k16 can be obtained.

2.2.4. 16 Rounds of Iterative Operations. The calculation steps of each round of the ES encryption algorithm are

(1) The 64-bit data input of the grouped plaintext after the initial replacement is divided into two groups: Li (32-bit) and Ri (32-bit), where i represents the number of rounds of the iterative operation, that is, $1 \leq f \leq 16$ and $i \in N$

(2) Change the right group of data obtained in the previous round of operation to the left group of data in the next round of calculation, that is, $L_i + 1 = R_i$

(3) At the same time, the 32-bit right group of data used in this round of operation is extended to 48 bits

(4) The 48-bit data obtained from the extended transformation of the i-th operation is added to modulo 2 of the 48-bit subkey ki of this round, and finally, the 48-bit data is still obtained

(5) Group the 48-bit data obtained in the previous step into a total of 8 groups, each of which is 6 in length. These 8 sets of data are replaced by S-boxes. The first and sixth bits of each group of 6-bit data input determine the number of rows in the S-box conversion table, and the second, third, fourth, and fifth bits determine the number of columns in the S-box conversion table. After processing, each group of 6-bit data becomes 4 bits

(6) The 8 sets of 4 bits processed by the S box are combined into 32 bits and then added to the left set of data Li in the i-th operation by modulo 2 to obtain the right set of data used in the next round of budget

In the above iterative operation, the subkey is combined with the data, and L_i and R_i are calculated according to the following rules:

$$L_i = R_{i-1}, \tag{27}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \tag{28}$$

where $1 \leq f \leq 16$, $i \in N$. Here, $\oplus$ represents the XOR operation of two sets of data. The operational block diagram of f is shown in Figure 4.

As shown in Figure 4, f is a function, and K1, K2, K3, ⋯, K16 are all subfunctions generated by the key k, each having a length of 48 bits. Because L_i is 32-bit, so we need to change the result of the numerator to 32-bit, which is the encryption function f.

2.3. Chaotic System Feature Analysis. Under the deterministic algorithm, the uncertain motion in a limited space is called chaotic motion. Chaos is an irregular movement that appears in a certain system. Chaos is a relatively common phenomenon that exists in nonlinear systems. Chaos movement has the characteristics of ergodicity and randomness and can be based on it within a certain range. It traverses all states without repeating its own laws. In general, chaotic systems should have the following main characteristics:

(1) Initial condition sensitivity: chaos is extremely sensitive to the initial conditions. As long as the initial

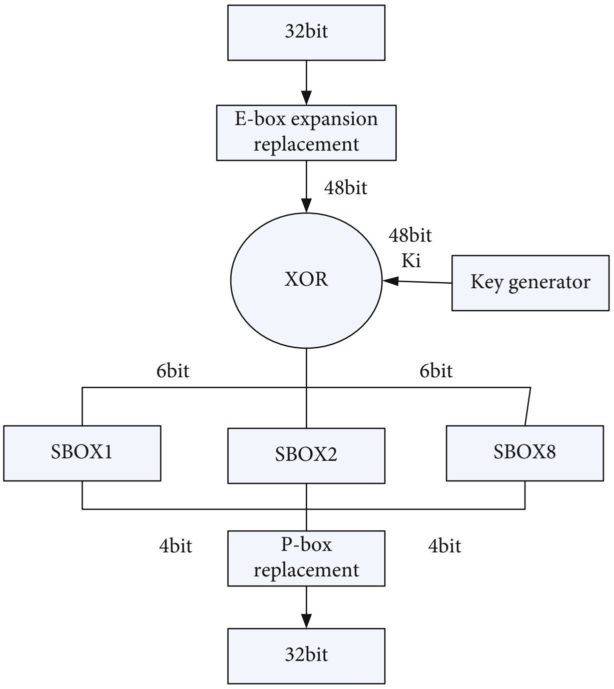

Figure 4: The operational block diagram of the encryption function.

conditions are slightly different or slightly disturbed, after a long period of movement, the final state of the system will be greatly deviated. It is also from this characteristic that the long-term evolution of chaotic systems is considered unpredictable.

(2) Intrinsic randomness: the so-called chaotic system is actually a deterministic system. However, during the evolution process, there is randomness inside, which shows a random-like behavior. The autocorrelation function of the chaotic system is similar to the shock function, and it is similar to the random signal correlation function.

(3) Scale invariance: there is a nonperiodic order in the chaotic system. During the evolution of the bifurcation and entering the chaos, it conforms to the Feigenbaum constant. This constant is a universal adaptive numerical feature that enters chaos as a period doubling bifurcation.

(4) Fractal: there are strange attracting factors in chaotic systems, which have a typing structure. Fractal dimension is a quantitative description of the geometric complexity of the strange attraction factor, and it is also a measure of the complexity of a chaotic system.

The generation of chaos comes from a deterministic algorithm. As long as the equation parameters and the initial values given in the algorithm are determined, chaos can occur. Because the security of the DES encryption algorithm does not depend on the algorithm itself, but on the protection of the key, whether the chaotic encryption algorithm is effective must consider the following points.

Table 1: Different platform performance.

Precalculation time	Platform 1	Platform 2	Platform 3
Average online analysis time	71.2 h	19.83 h	3.21 h
Average successful analysis time	9.274 s	4.773 s	3 s
Average failure analysis time	17.279 s	5.743 s	3.472
Success rate	41.27%	49.28%	48%

Table 2: Number of indications.

Version	Digital mode	Alphanumeric mode	6-bit byte mode	Chinese character pattern
1-10	11	10	9	9
11-29	13	12	17	11
30-40	17	14	21	15

(1) Discrete dynamics: unlike in the natural world, a computer system is a system with limited precision, so if a chaotic system is implemented in the form of a discrete system on a computer, the discrete dynamics of the system will be different from that of a continuous system. Discrete system, that is, discrete time system, is a system that transforms discrete time input signals into discrete time output signals. For control systems, a control system where one or more signals are a series of pulses or numbers is a discrete system. Sampling and quantization are two very important signal processing procedures in discrete systems.

(2) Encryption speed: due to the complexity of chaotic motion, if the speed of chaotic encryption algorithm is too slow, real-time encryption of information cannot be achieved, which has a great impact on the performance of the encryption system. Considering that the fixed-point structure is much faster than the floating-point structure, the fixed-point structure is generally used to maximize the encryption speed of the chaotic system. However, if the chaotic system used by the encryption algorithm is more complicated, then, it is likely that floating point numbers must be used, in which case the encryption efficiency will be greatly reduced. Therefore, when designing a chaotic encryption algorithm, a simple chaotic system is selected or adopted to make the amount of chaos calculation as simple as possible but at the same time meet the requirements of chaotic motion.

(3) Security requirements: the rapid development and in-depth research of chaos theory have led to many chaos analysis techniques being proposed one after another. If the cryptographer and the crypto attacker obtain the relevant information of the chaotic

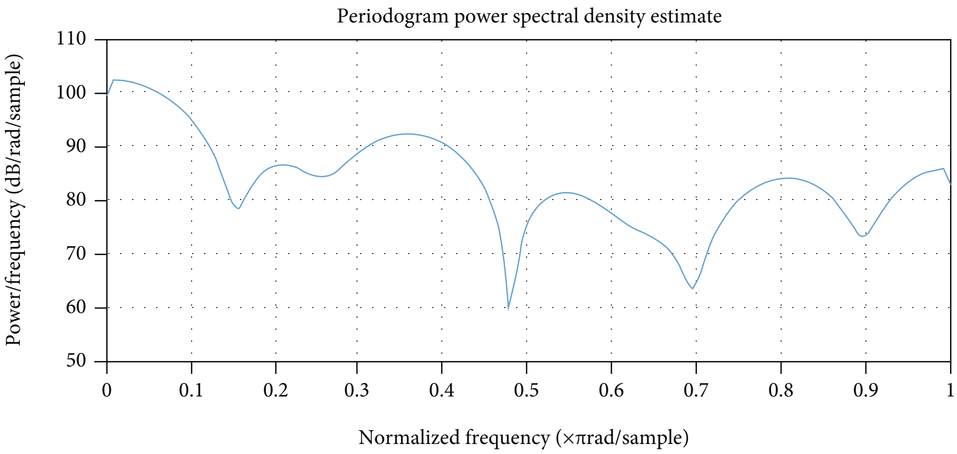

Figure 5: The DES encryption system simulate waveforms of DES.

system, they can analyze the determined structure of the chaotic system, reduce the complexity of the corresponding key generation, and then successfully decrypt the encryption system. Therefore, it is very important to avoid the exposure of chaotic system structure when designing. Of course, if the structure of the chaotic system can be changed according to the actual use situation, the security of the chaotic encryption system can be greatly improved.

(4) Implementation method: the implementation method of the encryption algorithm includes software implementation and hardware implementation. Therefore, an excellent chaotic encryption algorithm should be able to be easily implemented by software and hardware at the same time. Chaotic encryption algorithm has simple structure, refined algorithm, and simple hardware implementation, so it is easy to implement.

For the generation of cryptographic algorithms, the use of chaotic systems has good practicability, and its security is higher than that of traditional encryption algorithms. However, there are many types of chaotic systems and their complexity are also different. The logistic map originated from the insect mouth model, and the Henon map is a two-dimensional chaotic map that has been widely used. Therefore, the logistic chaotic system in chaotic systems is selected as the research object in this paper.

3. Experiments

3.1. Experimental Environment. FPGA technologies provided by FPGA vendors are mainly divided into Flash and SRAM. Although both can be programmed in the system and have higher performance, the system gate density can reach more than 1 M. However, FPGAs based on the SRAM architecture have several serious disadvantages: data cannot be saved when power is lost; the configuration chip is expensive; the power consumption is large; the startup current is large. Therefore, the A3P1000 device of ProASIC3/E series selected by Actel is used in this article. The development language is Verilog, and the development tool is Libero Integrated Design Environment (IDE). The development platform uses the ProASIC3 StartKit development platform. Compare the performance of different platforms, as shown in Table 1.

Table 3: The DES encryption system simulate report.

Chip series	ProASIC3/E	Select device	A3P 1000
Package	478 FBGA	Core Cells	1298/25182 (5%)
I/O Cells	193	Errors	0
Max F	340 MHz	Min T	2.94 ns

3.2. Experimental Settings. Logistic chaotic systems belong to the category of discrete dynamical systems, which can relatively comprehensively study their chaotic and statistical probability characteristics. One-dimensional logistic chaotic model is defined as follows:

$$x_{i+1} = \mu \times x_i \times (1 - x_i), \tag{29}$$

among them, $\mu \in [0, 4], x_n \in (0, 1), n = 1, 2, \cdots$

The chaotic process of logistic mapping was simulated on Matlab R2014b. The software "Synplify Pro" was used to synthesize the DES algorithm system. The ModelSimACTEL6.5d tool was used to conduct Behavior & PoSt Translate Simulate on the Verilog code of the DES encryption system. The 484FBGAPackage of A3P1000 is mainly divided into function verification simulation and performance comparison simulation. And implement the DES chaos algorithm on Matlab R2014b, and use the initial DES algorithm and the improved DES algorithm to encrypt the text document, by simulating the DES algorithm on Matlab R2014b and then mapping logistic. The text files used in the examples in this article are set to "accounting data.txt" uniformly. Count the number of indication digits of character technology, as shown in Table 2.

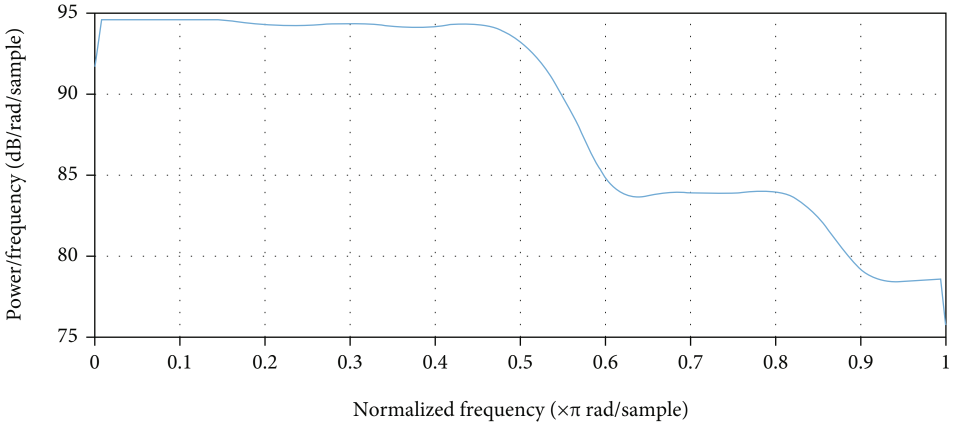

Figure 6: Postcomprehensive simulation waveforms.

4. Discussion

4.1. Functional Simulation Analysis. Mentor's ModelSim is the best HDL language simulation software in the industry. It can provide a friendly simulation environment and is the industry's only single-core simulator that supports VHDL and Verilog hybrid simulation. By writing a TestBench, this article uses ModelSim to simulate the design of each module in the DES algorithm system described in this chapter, then integrates each module, and finally performs functional simulation of the top-level module "des.v" to verify the design. The logic function of the DES algorithm system is correct; that is, the encryption/decryption function of the DES algorithm is correctly implemented. The DES encryption system simulation DES waveform is shown in Figure 5.

As shown in Figure 5, it can be known that the DES waveform of the DES encryption system gradually approaches a certain stable small fluctuation with increasing frequency, indicating that the DES algorithm system has completed the design requirements and the logic function is correct.

4.2. Performance Analysis. The software "SynplifyPro" is called to synthesize the DES algorithm system. After the synthesis is completed, the Log information is shown in Table 3.

The waveform diagram of the simulation after synthesis is shown in Figure 6.

Known from Figure 6 because in the functional simulation, various descriptions are only described from the logical implementation, so many programs are assumed to have zero delay. However, in the actual circuit, both the line delay and the logic operation delay exist, so after synthesizing the design, it is found that it is different from the simulation waveform before synthesis.

Comparing Figures 5 and 6, the selected time points are the time points when the DES algorithm system generates the ciphertext after encrypting the same plaintext of the first group and the second group with the same key, and the difference is 30863.847 ns. After synthesis, the simulation waveform has a large delay, which is caused by the delay of the logic device. But within a reasonable range, at the same time, the generated ciphertext has not changed, so the design achieves the purpose of prediction.

4.3. Initial Value Sensitivity Analysis. In this paper, the sensitivity of logistic chaotic system to initial values is analyzed. The difference between the two is only 10. The initial values a and b of the order of magnitude are substituted into Equation (4), and multiple iterations are performed. In the first 20 iterations, the obtained iteration results are still relatively close; after 70 iterations, the iteration results are obviously independent and different from each other. After 100 iterations, the iteration results have been significantly different. The results of the iteration are shown in Figure 7.

It can be seen from Figure 7 that even if the initial values have extremely slight differences, after multiple iterations, the iteration values will change greatly, and the iteration values are randomly distributed on the plane. Therefore, the initial value sensitivity of the logistic system can be used as the key. If the decipherer does not know the exact key and uses the exhaustive method, the difference method, and other methods to decipher the DES encryption system, the generated key sequence will be difficult to guess and unable to perform the deciphering work, which will greatly increase the difficulty of deciphering. At the same time, the security of the encryption system is greatly improved.

4.4. Simulation Analysis of Improved DES Algorithm. The encryption and decryption results of the initial DES algorithm and the packet experiment are shown in Tables 4–6.

The block encrypted data is shown in Table 4.

Keep the plaintext and encryption key in the improved DES algorithm encryption experiment; see Table 7 after changing the decryption key.

The block-encrypted data is shown in Table 8.

The experimental results are compared and analyzed, as shown in Figure 8.

It can be known from Figure 8 that the initial DES algorithm encrypts the ciphertext and the plaintext without similar characters. After entering the correct key, the decryption yields the correct plaintext; after entering the correct key, the decryption yields a string of garbled characters. Prove that

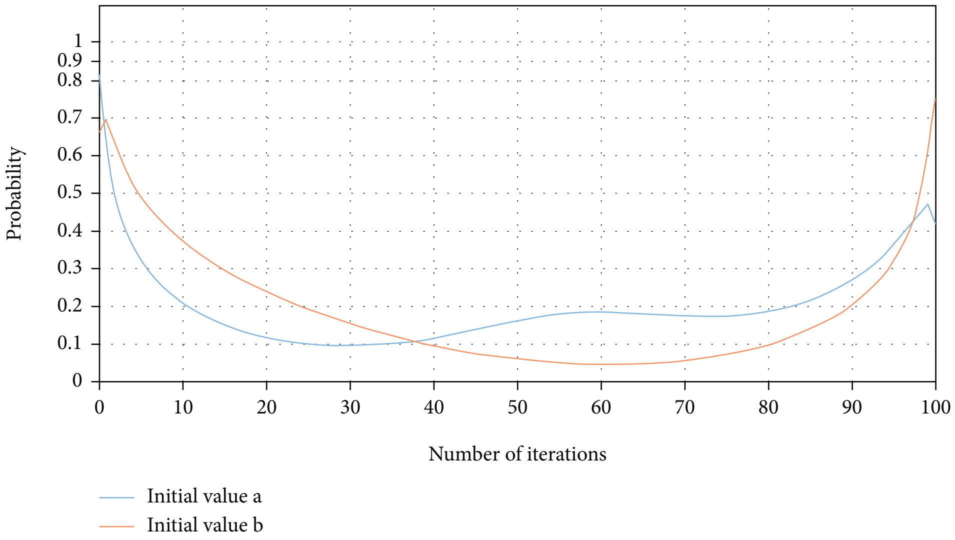

Figure 7: Iteration results.

Table 4: The example of DES.

Data block	Data
Plaintext	Accounting Data!
Encryption key	*1186828*
Ciphertext	)n?fUm???t?<????
Decryption key	$x_0 = 0.4$, $\mu = 4.1$, $n_a = 400$
Decryption result	Accounting Data!

Table 5: Example 1 of DES.

Data block	Data
Plaintext	Accounting Data!
Encryption key	*1186828*
Ciphertext	)n?fUm???t?<????
Decryption key	Accounting Data!
Decryption result	Accounting Data!

Table 6: Group data 1 of chaotic DES.

Grouped plaintext data blocks	Block key
Accounting Da	0110101011001010101101010101 0101001101011010010010101001
ta!	0101010111110110001010100110 1010010110100101101010100001

the improved DES algorithm's encryption and decryption functions are correct.

The experimental simulation proves that the "one-text, one-secret" cryptosystem is indecipherable. From the comparison of "Initial DES Algorithm Encryption Example" and "Improved DES Algorithm Encryption Example 1," it can be seen that although it is block encryption, there is only one "1186828" in the initial DES algorithm encryption process, but each group of plain text in the improved DES algorithm is corresponding to a set of corresponding keys, and comparing the two sets of grouping keys in Table 3 shows that they are independent of each other. From the comparison of "Improved DES Algorithm Encryption Example 1" and "Improved DES Algorithm Encryption Example 2," it can be seen that although x_0 has been changed by 10-11, the original ciphertext cannot be recovered, and the four sets of encryption generated by encryption and decryption before and after are compared. Keys, encryption/decryption of each two groups, with a total of 128 bits and 68 bits, are different, showing that the sensitivity to the initial key is very high.

The initial keys n_0, μ, and x_0 of the DES key algorithm based on the logistic chaotic discrete model are theoretically infinite compared to the keys of the initial DES algorithm and can form a sufficiently large key space, strong resistance.

Table 7: Example-2 of chaotic DES.

Data block	Data
Plaintext	Accounting Data!
Encryption key	$x_0 = 0.4$, $\mu = 4.1$, $n_a = 400$
Ciphertext	)n?fUm???t?<????
Decryption key	$x_0 = 0.4 + 10^{-11}$, $\mu = 4.1$, $n_a = 400$
Decryption result	a? Sd???m&?:???T???Mê???

Table 8: Group data 2 of chaotic DES.

Grouped plaintext data blocks	Block key
Accounting Da	0110101011001010101101010101 0101010101010101101101101001
ta!	0101010111010101010110100110 1010010110100101101010100001

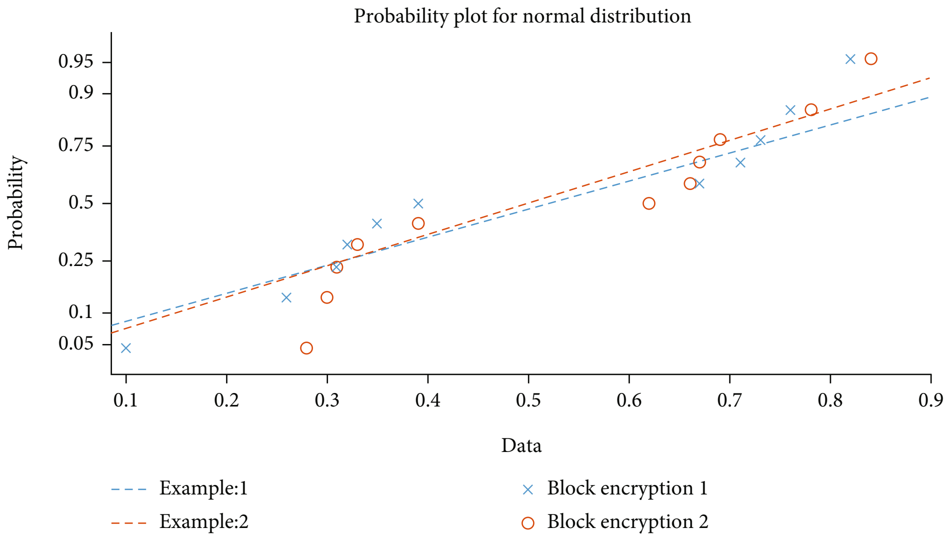

FIGURE 8: Comparison of two groups of experiments.

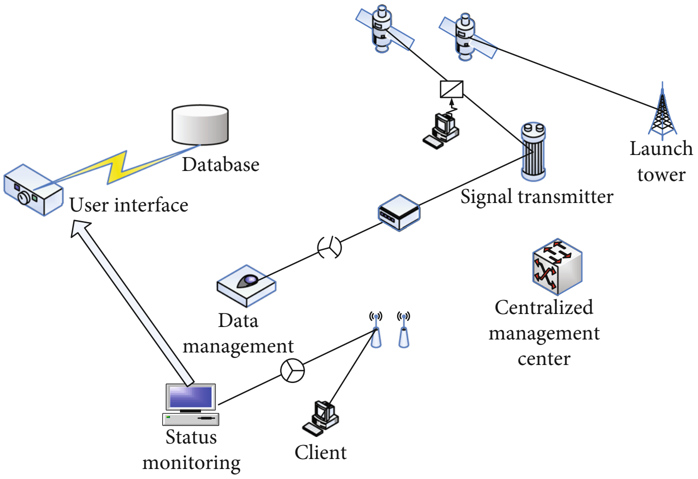

FIGURE 9: Wireless sensor network system.

The chaotic discrete model has initial value sensitivity and iterative nonrepetition, and the resulting key space is independent and random. In practical applications, you can perform random key input based on the performance of software and hardware, which is flexible.

4.5. Application Analysis of the Combination of Wireless Sensor Network and DES Algorithm. With the development of cloud technology, users can store data on remote servers to enjoy high-quality services, without burdening the maintenance of local data, and can also use the powerful computing power of cloud computing to serve themselves, which brings convenience and benefits to people. The structure of the wireless sensor network system is shown in Figure 9.

Data sampling and compression are carried out at the same time. Because the sampled signal is sparse, the signal can be encoded at a rate much lower than the nyquist sampling rate. In this way, each measurement value will contain some information of all collected samples, so it can be used blindly. Under the idea of inversion in source separation, the signal can be completely reconstructed or reconstructed with errors with a certain probability. The relevant data of the simulation parameters are shown in Table 9.

TABLE 9: Simulation parameters.

Parameter	Numerical value
Targeting area	200 ∗ 200 m
Total number of nodes	200
Communication radius (mm)	15.20, 25
Number of beacon nodes	5, 8, 12, 16, 20, 25, 30
Simulation times (s)	20
Number of particle swarms	100
The maximum number of iterations	20

The round key addition operation in the decryption process is completely consistent with the encryption process. The round

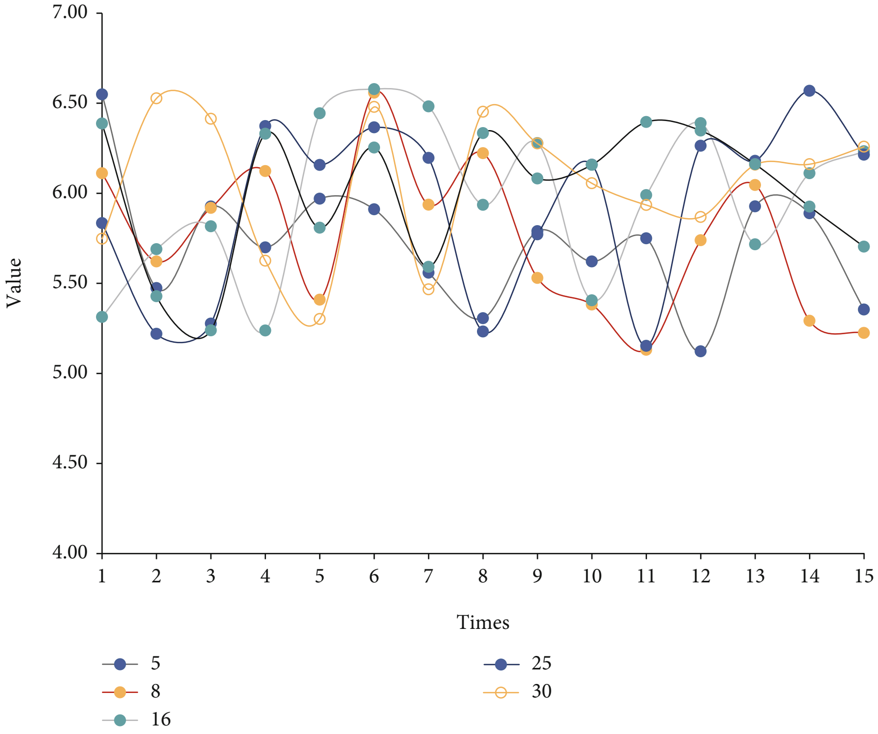

Figure 10: Test results of different numbers of nodes.

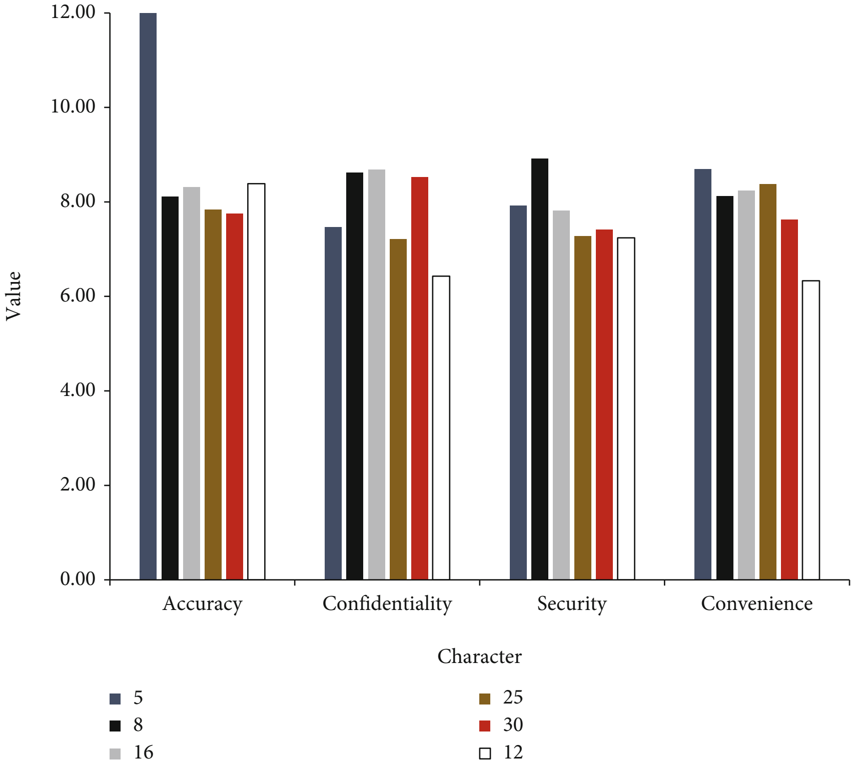

Figure 11: Characteristics of wireless sensor network technology.

key addition operation in the encryption and decryption process mainly changes the state matrix elements through the exclusive OR operation between bytes. Combine different numbers of nodes for simulation test, as shown in Figure 10.

The test results show that they are maintained between 5 and 6.6; even if the data aggregation node is physically or virtually damaged, the data aggregation node owner or attacker cannot access the data, which eliminates people's complete dependence on the data aggregation node. Analyze the characteristics of wireless sensor network technology, as shown in Figure 11.

The abscissa represents the four features in wireless sensor technology, and the ordinate represents the value of the corresponding feature. Using the attribute-based outsourcing encryption method, the heavy calculation is outsourced to a third-party server, which reduces the computational overhead of sensor nodes. Use the data aggregation node to aggregate the data collected by all sensors, reducing the consumption of data aggregation nodes and third-party servers.

5. Conclusions

Aiming at the problems of accounting data security, this paper conducts basic and focused research on cryptography and chaos. There is a deep understanding of DES (Data Encryption Standard), the most widely used block symmetric encryption algorithm in cryptography, and the LogiStic chaotic discrete model with prominent chaos characteristics in chaotic systems, and design of FPGA-based DES encryption system and realization.

This paper analyzes the characteristics of the DES encryption algorithm, such as the security performance of the algorithm, which meets most information encryption requirements, and can ensure the confidentiality of the information. The algorithm is public. The security mainly depends on the storage of the key, but there are some keys that are too short. Disadvantages include long application practice time, with extremely broad application basis. Combined with the logistic chaotic discrete model, the chaotic characteristics are relatively obvious, with high initial value sensitivity, good chaotic motion characteristics, and simple model characteristics. A design of DES algorithm based on logistic discrete chaotic model is proposed. And experimental simulations show that certain effects have been achieved in avoiding the shortcomings of the DES algorithm in the encryption/decryption process and improving the security of the DES algorithm.

The research in this paper still has some shortcomings. Although the chaotic system studied in this paper has good chaotic characteristics, the system structure is relatively simple, and the resistance to some differential attacks has not been fully considered. Although the application of the UART communication interface module can simplify the function verification work, but when the transmitted information is too large, the system performance is significantly reduced, and the encryption speed cannot be guaranteed under a large workload; the design of the DES algorithm based on the logistic discrete model can only guarantee the improvement of the DES algorithm. The security is improved, but the actual impact on the performance of the DES cipher system has not been considered, and there is still room for improvement.

Data Availability

This article does not cover data research. No data were used to support this study.

Conflicts of Interest

The author declares that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Social Science Foundation of China (14BTQ049), Shandong Natural Science Foundation (ZR2020MG003), and Special Project for Internet Development of Social Science Planning Special Program of Shandong Province (17CHLJ23).

References

[1] M. Doumpos, D. Niklis, C. Zopounidis, and K. Andriosopoulos, “Combining accounting data and a structural model for predicting credit ratings: empirical evidence from European listed firms,” *Journal of Banking & Finance*, vol. 50, pp. 599–607, 2015.

[2] V. Giannopoulos and E. Aggelopoulos, “Predicting SME loan delinquencies during recession using accounting data and SME characteristics: the case of Greece,” *Intelligent Systems in Accounting Finance & Management*, vol. 26, no. 2, pp. 71–82, 2019.

[3] W. Elsayed, M. Elhoseny, S. Sabbeh, and A. Riad, “Self-maintenance model for wireless sensor networks,” *Computers & Electrical Engineering*, vol. 70, pp. 799–812, 2018.

[4] S. N. Mohanty, E. L. Lydia, M. Elhoseny, M. M. Gethami Al Otaibi, and K. Shankar, “Deep learning with LSTM based distributed data mining model for energy efficient wireless sensor networks,” *Physical Communication*, vol. 40, p. 101097, 2020.

[5] M. Werner, “Financial process mining - accounting data structure dependent control flow inference,” *International Journal of Accounting Information Systems*, vol. 25, pp. 57–80, 2017.

[6] B. Cornell, W. R. Landsman, and S. R. Stubben, “Accounting information, investor sentiment, and market pricing,” *Journal of Law, Finance, and Accounting*, vol. 2, no. 2, pp. 325–345, 2017.

[7] L. Mbelwa, “Factors influencing the use of accounting information in Tanzanian Local Government Authorities (LGAS): an institutional theory approach,” *Agribusiness*, vol. 27, no. 4, pp. 478–492, 2015.

[8] C. Gullberg, “What makes accounting information timely?,” *Qualitative Research in Accounting & Management*, vol. 13, no. 2, pp. 189–215, 2016.

[9] D. L. Crumbley, K. T. Smith, and M. Smith, “Extending the case study: assigning an educational novel and student role-playing in the accounting information systems course,” *International Journal of Teaching & Case Studies*, vol. 5, no. 1, pp. 1–11, 2014.

[10] J. N. Taiwo and A. A. M. Edwin, “Effect of ICT on accounting information system and organizational performance,” *Social Science Electronic Publishing*, vol. 8, no. 6, 2018.

[11] C. M. C. Lee, “Estimating the cost of capital implied by market prices and accounting data by Peter Easton,” *Journal of Infection*, vol. 46, no. 3, pp. 513–522, 2015.

[12] D. Su, “Accounting information and stock performance,” *World Scientific Book Chapters*, pp. 307–334, 2015.

[13] R. Noordin, Y. Zainuddin, Fuad, R. Mail, and N. K. Sariman, “Performance outcomes of strategic management accounting information usage in Malaysia: insights from electrical and

electronics companies," *Procedia Economics and Finance*, vol. 31, pp. 13–25, 2015.

[14] B. Quosigk and D. A. Forgione, "Do donors respond to discretionary accounting information consolidation?," *Journal of Public Budgeting*, vol. 30, no. 1, pp. 35–58, 2018.

[15] L. Stabingis and J. D. Staliuniene, "Optimisation of measures for accounting information reliability assurance," *Nephrology, dialysis, transplantation : official publication of the European Dialysis and Transplant Association - European Renal Association*, vol. 3, no. 3, pp. 345–353, 2015.

[16] R. S. Camodeca, A. Almici, and B. A. Renzi, "The value relevance of accounting information in the Italian and UK stock markets," *Social Science Electronic Publishing*, vol. 12, no. 4, pp. 512–519, 2017.

[17] A. Jain and V. Kapoor, "Policy for secure communication using hybrid encryption algorithm," *International Journal of Computer Applications*, vol. 125, no. 10, pp. 16–20, 2015.

[18] X. Fei, K. Li, W. Yang, and K. Li, "Velocity-aware parallel encryption algorithm with low energy consumption for streams," *IEEE Transactions on Big Data*, vol. 7, no. 4, pp. 619–631, 2017.

[19] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multilayer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimedia Tools and Applications*, vol. 78, pp. 3457–3470, 2019.

[20] K. Ahmed and I. El-Henawy, "Increasing robustness of data encryption standard by integrating DNA cryptography," *International Journal of Computers and Applications*, vol. 39, no. 2, pp. 91–105, 2017.

[21] H. Abunahla, D. Shehada, C. Y. Yeun, B. Mohammad, and M. A. Jaoude, "Novel secret key generation techniques using memristor devices," *AIP Advances*, vol. 6, no. 2, article 025107, 2016.

[22] S. W. Formal, "Formal specification and verification of fully asynchronous implementations of the data encryption standard," *Electronic proceedings in theoretical computer science*, vol. 196, pp. 61–147, 2015.

[23] L. D. Meyer and S. Vaudenay, "DES S-box generator," *Cryptologia*, vol. 41, no. 2, pp. 1–19, 2017.

[24] T. Wenqing, G. U. Xingyuan, and L. I. Jing, "Power consumption analysis method based on data encryption standard mask," *Computer Engineering*, vol. 41, no. 5, pp. 133–138, 2015.

[25] Z. Zhang, L. Wu, A. Wang, Z. Mu, and X. Zhang, "A novel bit scalable leakage model based on genetic algorithm," *Security & Communication Networks*, vol. 8, no. 18, pp. 3896–3905, 2015.

[26] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 38, no. 5, pp. 968–979, 2020.

[27] N. Lalithamani and M. Sabrigiriraj, "Dual encryption algorithm to improve security in hand vein and palm vein-based biometric recognition," *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, pp. 545–551, 2015.

[28] N. P. Smart, "Physical side-channel attacks on cryptographic systems," *Software Focus*, vol. 1, no. 2, pp. 6–13, 2000.

[29] Y. Zhang, X. Xiao, L. X. Yang, Y. Xiang, and S. Zhong, "Secure and efficient outsourcing of PCA-based face recognition," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1683–1695, 2020.