Hindawi
Mobile Information Systems
Volume 2022, Article ID 3395019, 9 pages
https://doi.org/10.1155/2022/3395019

Research Article

Computer Data Encryption System Based on Nonlinear Partial Differential Equations

Junpu Yang

Information Center, Liaoning Provincial Party School of CPC, Shenyang 110004, Liaoning, China

Correspondence should be addressed to Junpu Yang; 1764200067@e.gzhu.edu.cn

Received 10 May 2022; Revised 8 July 2022; Accepted 19 July 2022; Published 19 August 2022

Academic Editor: Rutvij Jhaveri

Data encryption is to convert plaintext data into ciphertext through a data encryption algorithm and then transmit the ciphertext. After the recipient receives the ciphertext, the ciphertext is restored to plaintext, which provides protection and technical support for information security. The main purpose of this article is to design a computer data encryption system based on nonlinear partial differential equations. This paper uses the DES encryption algorithm to encrypt data and implements an onion encryption system that encrypts the outer layer of the database and tests and analyzes the encryption efficiency and additional overhead of the database encryption system on a general database to verify the design application prospects of ideas. In addition, the overall scheme of the encryption system, the hardware, and software of the system are designed in detail, the system is debugged, the overall test is tested, and the data encryption and decryption are effective and feasible. The experimental results of this paper show that after the construction of a computer data encryption system based on nonlinear partial differential equations, the overall security of the data is increased by 25%. In addition, after comparison, the security performance of the onion-type data encryption system is higher than that of the MySQL-type data. The performance of the encryption system is 21% lower. It has certain practical value and significance to apply it to the computer data encryption system.

1. Introduction

With the development of computer network technology and the application of network systems, computer networks have penetrated into all areas of people's lives. For example, study life, work life, and social life all need to use computer networks, greatly facilitating the exchange of information between each other, but also laying down hidden dangers for the security of information. Nowadays, losses caused by information leakage occur every day, such as personal account information leakage, the outflow of personal private files, and so on. Benefiting from the vigorous promotion of digital certificates in the banking industry, the author has been inspired to develop a personal encryption system similar to a USB flash drive, which can encrypt all kinds of sensitive data of users at any time and escort the information security of each of us.

With the continuous popularity of cloud services, outsourcing encrypted data will become more common, and protecting the privacy of outsourced data will become more and more important. Encryption technology is the main security and confidentiality measure adopted by e-commerce, and it is the most commonly used security and confidentiality means. It uses technical means to convert important data into garbled codes for encrypted transmission and then uses the same or different means to decrypt after reaching the destination. The privacy protection problem in outsourcing encrypted data calculation has its particularity: in general, users encrypt their own data and upload it to the cloud server, as long as the encryption algorithm is selected appropriately and the key protection is intact, the privacy of the data can be considered to be guaranteed. However, in the process of outsourcing encrypted data calculation, in addition to protecting the user's original data information, some intermediate information generated in the calculation process must also be protected because the attacker may infer the user's original data by analyzing this information. On the premise of

protecting the privacy of user data, processing and analyzing encrypted data on the cloud server so that users can complete the corresponding data analysis tasks is a problem that needs to be solved urgently.

In order to gain an in-depth understanding of data encryption technology, this paper explores the research and discussion of previous scholars. Siddig A proposed a fourth-order image denoising model. Using the fixed point theorem, he determined the existence and uniqueness of entropy solutions. Based on the Fast Explicit Diffusion Scheme (FED), numerical experiments demonstrate the effectiveness of this method in image denoising. The results are compared with three well-known fourth-order models: You and Kaveh models; Lysaker, Lundervold, and Ta models; and the most recent mean curvature (MC) model. The proposed model has advantages in removing noise while retaining image features. However, the performance of this model is not very stable, making the results not very accurate [1]. Ali et al. proposed a multi-mode authentication system that uses encrypted biometric technology for the edge center cloud environment. In the proposed system, a personal portable device is used to encrypt biometrics, thereby optimizing the use of resources and solving another limitation of the cloud environment. However, the design of the encryption system is relatively simple, making data access not very secure [2]. Ye and Huang designed an effective symmetric image encryption algorithm. In order to solve the problem of the low sensitivity of ordinary images measured by the uniform average change intensity and the number of changing pixel rates, he proposed using the premodular operation to preprocess the classic encryption algorithm. Before and after the position exchange, the invariance of the sum of pixels in the pure image, the keystream used for the replacement operation, is designed to depend on the pure image. But for most encryption algorithms, it is difficult to achieve the diffusion of the correlation with the ordinary image operation [3].

The innovations of this article are as follows: (1) many improvements have been made to the DES encryption algorithm. On the basis of maintaining the original functions, the operation steps are reduced and the encryption speed is accelerated. And in terms of code implementation, the use of assembly language with faster execution speed and the programming principle of time first has greatly improved the execution speed of the program. (2) The system uses a USB connection, which enhances the practicability of the system. The hardware part of the whole system is very small, easy to carry, can be used at any time, and is of low cost. The research presented in this paper can provide new ideas for data encryption and can also provide a new direction for the application of nonlinear partial differential equations.

2. Encryption Algorithm Based on Partial Differential Equation

2.1. Nonlinear Partial Differential Equations. Partial differential equations originated in the 18th century [4]. The formation and development of their theories are closely related to the development of physics and other natural sciences and promote each other [5]. Partial differential equations have a wide range of applications in explaining and predicting natural phenomena [6].

Various physical quantities in the objective world often change with the changes of time and space position, so they can be expressed as a function of the time coordinate t and space coordinate $(x_1, x_2, \ldots, x_n)$. And, this kind of physical change law is usually expressed as the relationship between the rate of change of each order of time and space coordinates, that is, the equation of the partial derivative of the function v with respect to t and $(x_1, x_2, \ldots, x_n)$. For example, in a uniform heat transfer object, the temperature v satisfies

$$\frac{\partial v}{\partial t} - a^2\left(\frac{\partial^2 v}{\partial x_1^2} + \frac{\partial^2 v}{\partial x_2^2} + \frac{\partial^2 v}{\partial x_3^2}\right) = 0. \tag{1}$$

Such equations containing unknown functions and their partial derivatives are called partial differential equations (7). Generally, a partial differential equation with v as an unknown function and $(x_1, x_2, \ldots, x_n)$ as a variable can be written in the following form:

$$W\left(x_1, x_2, \ldots, x_n, v, \frac{\partial v}{\partial x_i}, \ldots, \frac{\partial^q v}{\partial x_1^{q_1} \partial x_2^{q_2} \ldots \partial x_n^{q_n}}\right) = 0. \tag{2}$$

Among them, W is a function of its arguments, and the highest order of the partial derivative in the equation is called the order of the equation (8). The above equation can also be written as

$$W[v] = 0, \tag{3}$$

where W is called a partial differential operator [9]. If a partial differential equation is linear with respect to all its unknown functions and the derivatives of the unknown functions, it satisfies

$$W[C_1 v_1 + C_2 v_2] = C_1 W[v_1] + C_2 W[v_2]. \tag{4}$$

It is called a linear partial differential equation. If not, it is called a nonlinear partial differential equation. The study of nonlinear partial differential equations is the center of current differential equation research. Solving nonlinear partial differential equations is much more difficult than solving linear partial differential equations, and most nonlinear partial differential equations can only rely on numerical solutions.

Partial differential equations can be divided into three categories: elliptic equations, parabolic equations, and hyperbolic equations (10). At present, the research on second-order partial differential equations has formed a relatively mature system. Higher-order equations, especially higher-order parabolic partial differential equations, have received extensive attention due to their profound physical background [11, 12].

2.2. Symmetric Encryption Algorithm

2.2.1. DES Algorithm

(1) The DES algorithm is a symmetric cryptosystem in the cryptosystem, also known as the American Data

Encryption Standard. The DES encryption algorithm is a 64 bit encryption, and the key is up to 64 bits [13]. After 8 bits are discarded, the effective key is 56 bits, that is, 8 characters. If you want to decipher, you only need to enumerate 256 times to try all the keys, which is not difficult for current supercomputers [14]. The algorithm implementation process is as follows:

(2) Given a 64 bit plaintext A, convert A to A_0 through a replacement IP, and the following formula can be obtained:

$$\begin{aligned} A_0 &= IP(A) \\ &= T_0 S_0. \end{aligned} \tag{5}$$

Among them, the left 32 bits of A_0 is T_0 and S_0 is the right 32 bits of A_0.

(3) Combine the data with the key and perform 16 rounds of the same calculation, and the calculation is as follows:

$$S_i = T_{i-1} \oplus f(S_{i-1}, k_i). \tag{6}$$

Among them, $\oplus$ represents the exclusive OR between two bit strings, f is a function, each k_i is a replacement of the initial key k, and the length is 48 bits, which constitutes a key scheme [15].

(4) Do the inverse permutation of the initial permutation to $S_{16}T_{16}$ and get the ciphertext as

$$B = IP^{-1}(S_{16}T_{16}). \tag{7}$$

It is particularly important to note that in the last iteration, the left and right sides are not exchanged, but $S_{16}T_{16}$ is used as the input of IP^{-1} to get the ciphertext [16].

The design basis of DES is Shannon's replacement permutation network [17]. This encryption network takes a block of plaintext and a key as input and produces a block of ciphertext by interleaving several "rounds" (or "layers") of substitution and permutation operations. The SP network is based on two basic operations of cryptography. The alternative is called the S-box [18]. It is the only nonlinear part of the DES algorithm [19]. Its strong password determines the entire algorithm. Security strength provides the obfuscation necessary for cryptographic algorithms. The permutation is called a P-box, and its purpose is to provide an avalanche effect, that is, a small change in the plaintext or the key will cause a larger change in the ciphertext [20].

2.2.2. Double DES Algorithm. As the weaknesses of DES are being studied more and more deeply, it is necessary to improve DES. One of the methods is to compound DES to strengthen its antiattack ability. This algorithm combines the advantages of both the DES and RSA algorithms. The principle is that sender uses the DES key to encrypt important data and transmit the message, and the receiver uses the RSA private key to encrypt the encrypted DES after receiving the message key to decrypt it. The simplest way is to perform secondary DES encryption [21, 22]. Given civilization Q and an encryption key L_1L_2, the cipher text is expressed as

$$C = F_{l_2}\left(F_{l_1}(Q)\right). \tag{8}$$

Given a plaintext, there are 2^{64} possible ciphertexts after double DES encryption. The key length used by double DES should be 112 bits, so there is a 2^{112} possibility to choose the key. That is to say, for a given ciphertext, there are 2^{48} possibilities to encrypt it into the same ciphertext [23].

2.2.3. Triple DES Algorithm. This article uses triple DES, which means that the plaintext is encrypted three times with three different keys so that the effective key is 168 bits and there are 24 characters in total. If you try to decipher, you must try 2168 keys, which increases the strength of the password many times and can effectively prevent brute force cracking [24].

Triple DES is a variant of the very popular DES algorithm. 3DES was designed to provide a relatively simple way to avoid similar attacks by increasing the key length of DES, rather than designing an entirely new block cipher algorithm. It is widely used in network security and data transmission. It is simple and easy to use, low in cost, and low in hardware requirements. In this article, the data transmission between the upper computer and the lower computer is a block transmission method, the block size is 64 bits, and the DES encryption algorithm is the same block encryption algorithm, so the 64 bit block length is the basic encryption unit, and the 64 bit encryption key performs a series of calculations and finally outputs a 64 bit ciphertext. In this article, a two-dimensional array key [8] [8] is used to represent a block encryption unit, and a two-dimensional array Date [8] [8] is used to represent a unit of key length. In order to improve the speed and efficiency of data encryption, the function *DES* is written in assembly language, which improves the execution efficiency of the code, saves the operating space of the single-chip microcomputer, and makes encryption of large amounts of data a reality [25].

2.3. Encryption System RSA Algorithm. Symmetric keys have the advantages of fast encryption speed and convenient software and hardware implementation, but they have disadvantages such as complex key management and the inability to perform digital signatures. Although the RSA algorithm can achieve digital signature and key management, the amount of calculation is very large [26]. The decryption speed is very slow. Now the common practice is to combine the two, encrypt the file with AES, and then encrypt the key with RSA to give full play to their respective advantages [27].

RSA security is equal to the mathematical problem of decomposition of large numbers. In order to ensure data security, the choice of prime numbers is usually very large, which causes many problems in the calculation speed. Not only that, but RSA also has the most useful feature of the public key cryptosystem; that is, anyone can use the public

key, which allows the attacker to leave traces when performing selective ciphertext attacks. Therefore, it should be recommended to implement a protective measure for public key security. In response to the above problems, this article improves the RSA algorithm and proposes a new encryption algorithm, that is, more information communication [28].

Through the analysis of the RSA algorithm, it can be seen that if three or more prime factors are used, that is, $N = qwe$ or more, the algorithm is still valid and will not be proved here. Rabin has achieved good results by using qwe as a private key in an encryption algorithm based on the secondary residue [29]. Therefore, the improved algorithm proposed in this paper uses three prime factors and will be used as a private key.

At present, RSA allows to choose the size of the public key. A 512 bit key is considered insecure; a 768 bit key has no fear of being compromised by anything other than the National Security Administration (NSA); and 1012 bits in the RSA algorithm are considered safe, so the number of qwe bits is about 490. The improved algorithm uses three prime numbers. If they are all around 490 bits, the result will reach 1450 bits, which will make the algorithm safer. As the number of digits increases, if the factor is not known, the calculation will become more difficult, and it will become more difficult to crack the algorithm by calculating N. If you want to decompose N, you need to get four 490 bit prime factors. Assuming that one 490 bit prime factor is obtained, you still need to decompose 980 bits n to crack the algorithm [30].

3. Data Encryption Experiment

3.1. Overall Design of the Data Encryption System. The design of a data encryption system mainly involves hardware circuit design, single-chip principle and program design, USB interface technology, DES encryption program design, and host computer software design. In the design concept, modular design is used to separate the entire system into several subsystems, which is conducive to the orderly completion of the design.

The expectation of the data encryption system based on the USB interface is to design a portable device similar to a USB disk to encrypt the data on the computer and use the USB interface to connect the two. In order to improve the security of encryption, the subject chose to separate the encryption device and the operation page. According to this requirement, the data encryption system is divided into two parts: the upper computer and the lower computer, as shown in Figure 1.

In this system, the upper computer is the computer that sends operation commands. The design of the host computer uses VC++ programming to develop an application program, which is used to perform encryption operations, allowing users to send operation commands, send data, receive data, select files, display execution speeds, etc., on the page; the design of the host computer includes two parts: layout design and functional design. The layout design mainly develops the front-end operation page, and the functional design mainly realizes the entire process of communicating with the lower computer through the USB interface, including a series of USB interface operations, data sending, and receiving.

The lower computer mainly executes the corresponding operation according to the command of the upper computer and specifically refers to the hardware encryption device in this system. It contains the USB interface, the microcontroller and its peripheral circuits, and the program code packaged by the microcontroller. The work of the lower computer mainly revolves around the single-chip microcomputer, reads the command of the upper computer through the code in the single-chip microcomputer, and performs corresponding operations.

The data encryption system realizes the separation of two machines. The application program of the upper computer is installed on the computer, and the lower computer is a plug and play encryption device. The user inserts the lower computer into the computer's USB slot, then opens the PC-side application, and sends the preprocessed data, and the lower computer receives the data, processes it according to the instructions of the microcontroller, and finally sends the data back to the upper computer to complete an operation.

According to the function of the host computer, it is divided into layout design and functional design. Layout design is mainly to design a user operation page. On the page, you can enter a 24 bit key, select the storage location of the encrypted and decrypted files and the processed file, and send the encryption, decryption, and reset commands. In the lower part of the page, the progress of data encryption and decryption, the start and end execution time of the program, and the total time spent in program execution are displayed. The function design should call for the software development kit to realize operations such as opening, closing, and refreshing the device. In addition, the handshake process with the lower computer must be designed, including command information sending and receiving and data sending and receiving. This effectively strengthens the combination of system functions.

The design of the lower unit is based on the C8051F340 microcontroller, and the design of the entire hardware circuit is very simple. The peripheral circuit must be designed for the normal operation of the microcontroller, including the provision of a 3.3 V power supply and the design of an external reset circuit. Connect two LED lights to the single-chip microcomputer. One indicates whether the single-chip microcomputer is powered on, and the LED is on when it is normally powered on; the other indicates data transmission. When there is data flow on the USB, the LED flashes. The single-chip microcomputer programming uses C language to write functional functions and realizes the functions required by the system by calling the built-in software development kit, including USB interface operation, "handshake" with the host computer, sending data, receiving data, storing data, and calling encryption algorithm program to process data.

3.2. Data Encryption Algorithm Improvement Experiment. The plaintext data to be encrypted are initially transformed into the unit of basic block length [31, 32]. The 64 bit

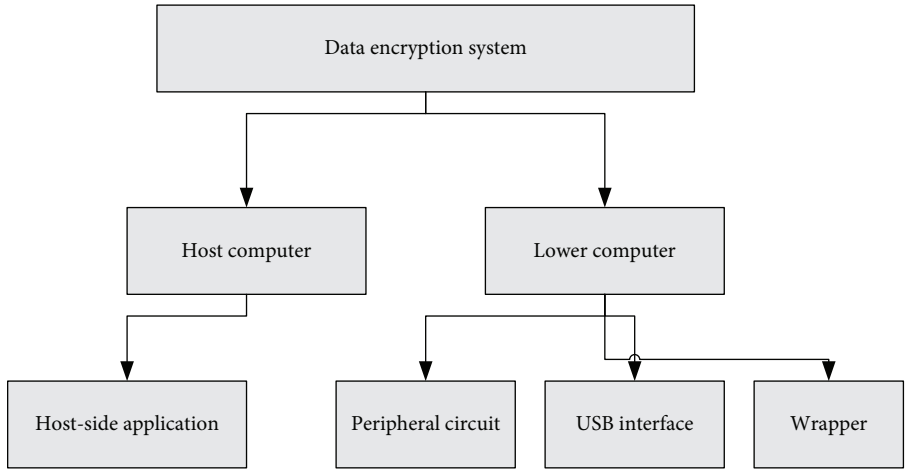

Figure 1: Overall structure of the data encryption system.

plaintext is divided into 8 columns each with 8 bits as a line, and the rows and columns are exchanged. In the program design, the DES_IP() function is defined to realize the data The rows and columns are interchanged, but it does not make the left and right plaintext physical space continuous as in the DES general algorithm, but only makes it logically continuous, and the odd and even rows are stored interleaved. There is no need to change the storage order, which simplifies the code and improves execution efficiency.

First, open up the space R, using two layers of loops, and the first layer of the loop indicates the line and the second layer of loop shifts to the left. When the first column is taken, Data [1][j] is shifted to the left as a whole, and Data [1], [1] becomes the overflow bit, which is stored in the first bit of R0. Then cyclically shift down, Data [2][j] is shifted to the left as a whole, Data [2][1] becomes an overflow bit, R0 is shifted to the left as a whole, and Data [1][1] is shifted to the left by one bit. Data [2][1] replaces Data [1][1] position. By analogy, after Data [1][j] is shifted left eight times, the data of R0 are the data of Data [i][1] from left to right, so that the first column becomes the first row. When the second column is taken, the same operation is performed, and finally, after 64 cycles of left shifting, the row and column exchange of the data is realized.

Then the obtained 64 bit plaintext block is divided into two parts, each with 32 bits, and the left block is the left plaintext, and the right block is the right plaintext. In the array, odd numbers are left plaintext and even numbers are right plaintext.

3.3. Onion Encryption Model Design. The basic technology of the architecture server interface database encryption system is to realize the encryption of various SQL functions in the ciphertext. Literally speaking, this technology encrypts the data layer by layer like an onion, making the data look like an onion. The SQL function corresponding to each layer of the onion is different. The top layer uses the most secure encryption algorithm to ensure the security of all database data. In SQL functions, data are always stored in ciphertext, but the ciphertext encryption algorithm is different.

The design of the security model of the onion encryption structure is mainly based on the classification of SQL functions to design a function that satisfies the SQL. These four models complete the functions of SQL and perform confidential operations on database data.

The four encrypted onions are nested into onion encryption by seven different cryptographic systems. Among the seven cryptographic systems, RND is the encryption system with the strongest encryption performance. It cannot perform homomorphic calculations and maximize data security. In the design of the onion model, search and add onions are purely functional onions, with two layers; equivalent onions and comparison onions are full performance onions, which are designed with four layers, and the outer layer encryption is highly secure. The encryption scheme is used to ensure that no information is leaked. The inner encryption is an encryption scheme with a gradual decrease in security, which can only be accessed when the corresponding inquiry is required.

Since users initiate various queries, which onion type and layer of onion layers need to be accessed for different queries, the data encryption agent in the proxy architecture of the database encryption system is mapped to different encryption layers according to the query. In addition, the database management server needs to dynamically record the status of each onion of each data item in the database. Then, according to the query, the data are decrypted or encrypted for the corresponding onion layer.

4. Computer Data Encryption System Analysis

4.1. Data Encryption Algorithm Analysis. Confusion and diffusion are the bases of Shannon's design of encryption algorithms, and chaotic systems have exactly this property. Since the chaotic system is sensitive to the initial value, even a small disturbance in the initial value will bring about a huge difference, which is just in line with the avalanche effect of the algorithm. Chaotic systems generally use nonlinear equations, which are particularly critical for cryptographic design. Usually, the core of an algorithm is its nonlinear part because the linear part is vulnerable to differential attacks.

For example, the core of DES is its nonlinear S-box, and the reason why the MH backpack algorithm is easy to crack is not only due to its low density but an important reason is that its threshold function adopts a linear structure, which greatly reduces its security. The chaotic system has good characteristics, so it is used in the design of encryption algorithms, and the effect is significant; it solves the problem of image encryption. The specific results are shown in Figure 2.

From the graph, we can see that even if the initial value is very small, it cannot be decrypted correctly, which is caused by the sensitivity of chaos to the initial value. Also, the gray distribution of the ciphertext image is more uniform, which can effectively resist probability density attacks.

Since chaotic encryption belongs to symmetric encryption, in practice, the key, that is, the control parameter, can be transmitted using public key encryption algorithms such as RSA and ECC. At the same time, we can see that when we chaotically encrypt the image, we mainly apply the chaotic sequence to the plaintext image. In order to make the ciphertext image more complex and difficult to identify, we can use some complex transformations, such as wavelet changes. Its main feature is that it can fully highlight the characteristics of some aspects of the problem through transformation, can analyze the localization of time and frequency, gradually refine the signal at multiple scales through scaling and translation operations, and finally achieve time subdivision at high frequencies. At the same time, in the selection of chaotic sequences, different sequences of multiple chaotic systems can also be used for superposition, which is more random and achieves a better encryption effect.

4.2. Performance Analysis of the Data Encryption System. The performance test of TPC-C query mixing was carried out on MySQL and the onion database encryption systems. The test results are given through analysis, which shows the TPC-C query throughput on servers with different core numbers. It can be seen that when the number of cores is 1 to 2, the throughput of MySQL and the onion database encryption system is similar. As the number of cores increases, the performance of the onion database encryption system is worse than that of MySQL. Of course, this is because the onion database encryption system is inevitably caused by operations on ciphertext data, but the overall throughput of the onion database encryption system is only 21%-26% less than that of MySQL. This efficiency can make the onion database encryption system practical, as shown in Figure 3.

In order to understand the resource overhead of the onion database encryption system, different types of SQL queries were tested through throughput in TPC-C, and the test results of the onion database encryption system and MySQL were compared, as shown in Figure 4. It can be seen that compared with MySQL, the onion database encryption system has less throughput on different types, and the highest value is only 3.5×10^4, but the difference is less. Mainly SUM, the efficiency loss on Upd.inc is large.

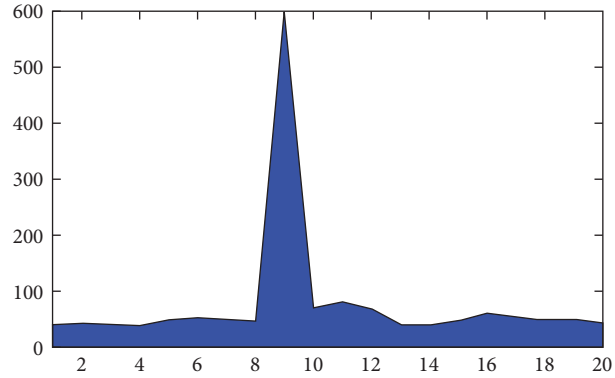

Figure 2: Area map of the ciphertext image.

In order to understand and analyze the time difference between the onion database encryption system processing various standard SQL queries, we have completed the program-level test on different types of SQL processing time of the onion database encryption system and MySQL, as shown in Table 1. As shown by the time expenditure results of the database encryption system and MySQL on different SQL queries, the related test results show that the overall overhead on the server has increased by 19% or 0.03 ms. Onion database encryption system agents add 0.05 ms to each query, of which 23% are used for MySQL agents, 24% are used for data encryption and decryption, and 49% are used for query analysis and processing.

According to the performance test results, the efficiency of the onion database encryption system is slower than that of MySQL. This is because the onion database encryption system performs SQL queries on encrypted data while MySQL performs SQL queries on plaintext data. Encryption and decryption will inevitably lead to a reduction in efficiency. But, this loss will not affect the practicality of the onion database encryption system. Therefore, the onion database encryption system is a practical design idea for an encrypted database system, that can execute complete SQL queries on encrypted data.

4.3. Evaluation and Analysis of the Data Encryption System. This article surveys 400 professional encryption personnel. Through statistics and analysis of data, they can get their evaluation of the computer data encryption systems. Among them, 54% of the professionals are very satisfied with the evaluation of the computer data encryption systems. The computer data encryption system is handy, and 33% of professionals are generally satisfied with the computer data encryption system, and 9% are dissatisfied with the computer data encryption system. Finally, 4% of the professionals are very satisfied with the computer data encryption system. If they are satisfied, it may be that they are used to the previous encryption system, as shown in Figure 5.

A comprehensive analysis can conclude that most professionals are still satisfied with the data encryption system, and their knowledge of information security has also improved to a certain extent during the learning process of

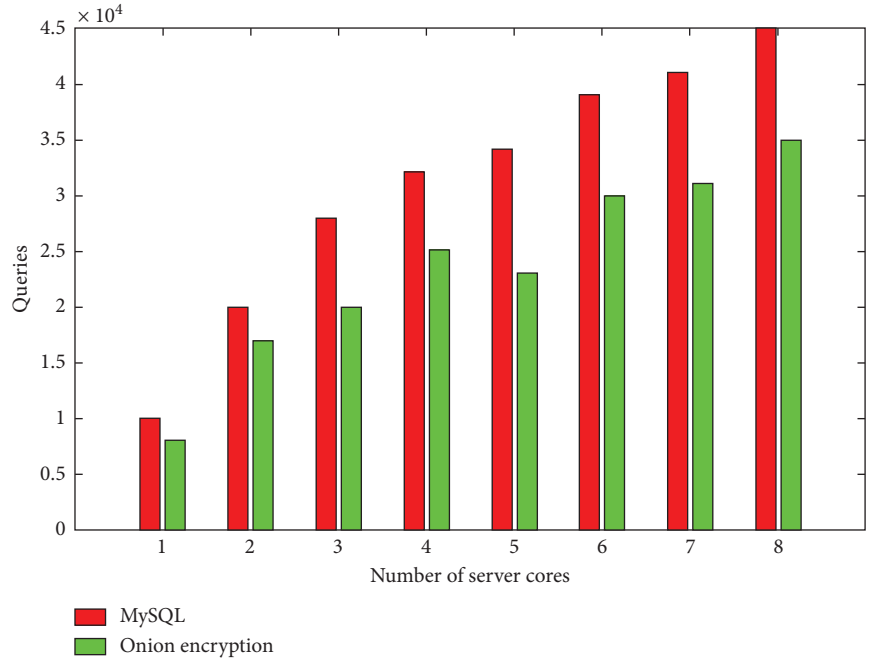

Figure 3: Throughput test results on the server.

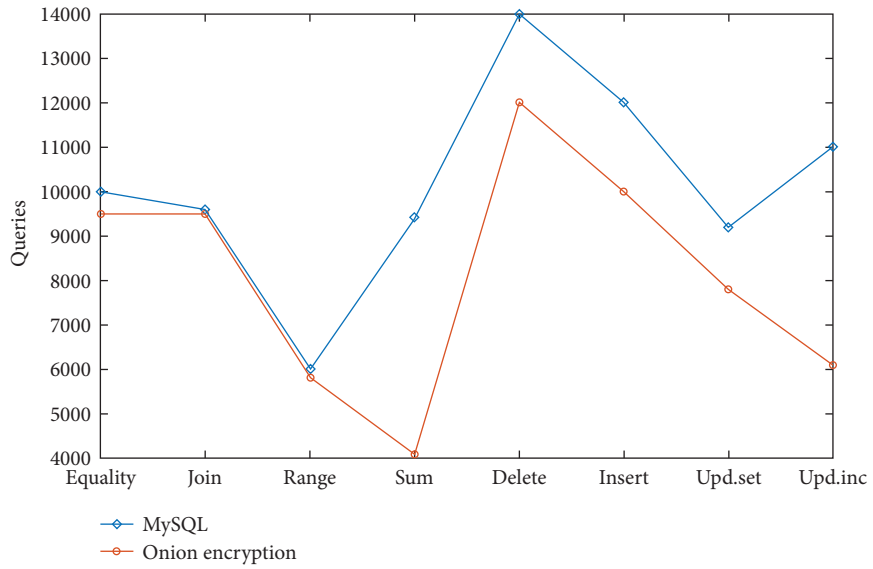

Figure 4: Throughput test results of different types of SQL queries.

Table 1: Comparison of query time of different data encryption systems.

Query	MySQL server (ms)	Onion encryption system server (ms)
DET	0.09	0.77
JOIN	0.11	0.73
OPE	0.20	29.0
HOM	0.12	1.10
Delete	0.09	0.26
Insert	0.10	15.9

encryption algorithms. The encryption algorithm is the core of information security. At the same time, there are many aspects such as key distribution, key management, security protocol, and authentication protocol. If applied to the database, the information security system will be greatly protected. In the communication protocol, there are still only a few types of algorithms. I hope to design more and more encryption algorithms, signature algorithms, hash algorithms, etc., so that multiple algorithms can be cross-combined so that the communication protocol will also be richer and there will be more choices.

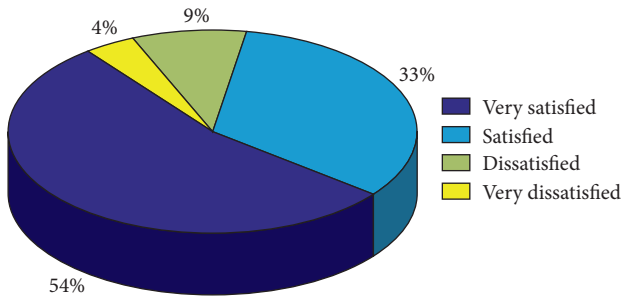

Figure 5: Evaluation of the data encryption system.

5. Conclusions

This paper improves the efficiency of the data encryption algorithm, improves the decryption efficiency and security of the algorithm, and reduces the encryption efficiency a little bit. At the same time, by combining the symmetric encryption algorithm and the public key algorithm, a new encryption system is proposed. The system integrates identity authentication, protection of public keys, digital signatures, and other technologies. It can resist attacks by multiple means and meet the needs of modern communication.

Based on the design idea of ciphertext database processing, this paper designs an encryption model for onion databases, provided that the fully unified encryption cannot meet the practical requirements and the start-up and implementation of the database encryption system have been completed. In this article, by creating a simple test environment, the performance tests of the MySQL database encryption system and the onion basic system are carried out, and the encryption efficiency of the overhead time is compared and analyzed, and the onion database is verified by indicators such as encryption efficiency.

With the in-depth development of scientific research, experts and scholars have found that the description of the specific model of the variable coefficient nonlinear partial differential equation is closer to the reality. Therefore, the research on the fractional order nonlinear partial differential equation can be used for deeper variable coefficient fractional nonlinear partial differentiation in the future. The equation's direction develops. When selecting auxiliary equations, you can not only limit yourself to the auxiliary equations in the text, but also you can exchange them for other auxiliary equations, such as the Bernoulli equation. You can explore their Backlund transformation and nonlinear superposition formula. The research machine of the data encryption system is complex. The experiments in this paper are carried out under the exclusion of many interference factors, and there are still shortcomings in the scale of use. In the future research process, we will continue to improve this point and improve the quality of work.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. Siddig, Z. Guo, Z. Zhou, and B. Wu, "An image denoising model based on a fourth-order nonlinear partial differential equation," *Computers & Mathematics with Applications*, vol. 76, no. 5, pp. 1056–1074, 2018.

[2] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Generation Computer Systems*, vol. 85, pp. 76–87, 2018.

[3] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, no. 16, pp. 45–53, 2017.

[4] L. Zhang, "Hamilton's gradient estimates for a nonlinear partial differential equation under the Yamabe flow," *Journal of Mathematical Analysis and Applications*, vol. 477, no. 2, pp. 1353–1368, 2019.

[5] A. Itkin, "A new nonlinear partial differential equation in finance and a method of its solution[J]," *Journal of Computational Finance*, vol. 21, no. 4, pp. 1–21, 2018.

[6] X. B. Wang and B. Han, "Characteristics of abundant lumps and interaction solutions in the (4+1)-dimensional nonlinear partial differential equation," *International Journal of Nonlinear Sciences and Numerical Stimulation*, vol. 21, no. 3-4, pp. 283–289, 2020.

[7] W. Cui, L. Mi, J. Zhang, and L. Yin, "Invariant tori for a fifth order nonlinear partial differential equation with unbounded perturbation," *Dynamics of Partial Differential Equations*, vol. 15, no. 3, pp. 183–199, 2018.

[8] A. I. Aristov, "Exact solutions of a second-order nonlinear partial differential equation," *Differential Equations*, vol. 54, no. 9, pp. 1137–1146, 2018.

[9] A. Caboussat and R. Glowinski, "An alternating direction method of multipliers for the numerical solution of a fully nonlinear partial differential equation involving the jacobian determinant," *SIAM Journal on Scientific Computing*, vol. 40, no. 1, pp. A52–A80, 2018.

[10] P. J. Kiptum, J. Esekon, and R. O. Esilaba, "Explicit solution of a nonlinear Black-Scholes partial differential equation: tanh method," *Applied Mathematical Sciences*, vol. 13, no. 7, pp. 339–346, 2019.

[11] L. I. Peiyan and G. U. Wei, "Estimation of 1-dimensional nonlinear stochastic differential equations based on higher-order partial differential equation numerical scheme and its application," *Frontiers of Mathematics in China*, vol. 12, no. 6, pp. 1441–1455, 2017.

[12] J. A. Al-Hawasy and M. A. Jawad, "Approximation solution of nonlinear parabolic partial differential equation via mixed Galerkin finite elements method with the Crank-Nicolson scheme," *Iraqi Journal of Science*, vol. 60, no. 2, pp. 353–361, 2019.

[13] B. S. Han and K. H. Kim, "Boundary behavior and interior Hölder regularity of the solution to nonlinear stochastic partial differential equation driven by space-time white noise," *Journal of Differential Equations*, vol. 269, no. 11, pp. 9904–9935, 2020.

[14] S. Fabio, G. C. Juan, S. Esteban, and F. Zhilan, "A partial differential equation model with age-structure and nonlinear recidivism: conditions for a backward bifurcation and a

general numerical implementation," *Computers & Mathematics with Applications*, vol. 78, no. 12, pp. 3916–3930, 2019.

[15] D. Kaya, "The use of Adomian decomposition method for solving a specific nonlinear partial differential equations[J]," *Social ence Electronic Publishing*, vol. 9, no. 3, pp. 343–349, 2018.

[16] J. Li, "Research on the application of data encryption technology in network security transmission[J]," *Revista de la Facultad de Ingenieria*, vol. 32, no. 5, pp. 595–604, 2017.

[17] S. Angizi, Z. He, N. Bagherzadeh, and D. Fan, "Design and evaluation of a spintronic in-memory processing platform for nonvolatile data encryption," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 9, pp. 1788–1801, 2018.

[18] J. J. Ong, G. Ijemaru, L. M. Ang, K. P. Seng, J. H. Kong, and Y. W. Wong, "A low-complexity DWT module and CRS minimal instruction set computer architecture for wireless visual sensor networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 30, no. 2, pp. 73–90, 2019.

[19] B. Vyas and A. Vajpayee, "Local data security through encryption," *International Journal of Computer Trends and Technology*, vol. 47, no. 2, pp. 137–141, 2017.

[20] P. Yang, G. Sun, J. He, P. Zhou, and J. Liu, "A student information management system based on fingerprint identification and data security transmission," *Journal of Electrical and Computer Engineering*, vol. 2017, no. 2, pp. 1–6, 2017.

[21] S. Xu, G. Yang, Y. Mu, and X. Liu, "A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance," *Future Generation Computer Systems*, vol. 97, no. AUG, pp. 284–294, 2019.

[22] J. Kynshi and D. D. V. Jose, "Enhanced content based double encryption algorithm using symmetric key cryptography," *Oriental Journal of Computer Science and Technology*, vol. 10, no. 2, pp. 345–351, 2017.

[23] N. A. Sharma and M. Farik, "A performance test on symmetric encryption algorithms - RC2 Vs rijndael," *International Journal of Scientific & Technology Research*, vol. 6, no. 7, pp. 292–294, 2017.

[24] Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," *Future Generation Computer Systems*, vol. 82, no. MAY, pp. 342–348, 2018.

[25] A. Anukirti and V. Jayaswal, "Modified AES algorithm integrating IBDP (image block displacement procedure) for data encryption," *International Journal of Computer Application*, vol. 179, no. 44, pp. 5–9, 2018.

[26] D. Imran and R. Ranjana, "An analysis of access control mechanism with authentication of anonymous user and deduplication of data in decentralized clouds," *International Journal of Computer Application*, vol. 159, no. 3, pp. 12–18, 2017.

[27] M. S. Fanselow and Z. T. Pennington, "The danger of LeDoux and pine's two-system framework for fear," *American Journal of Psychiatry*, vol. 174, no. 11, pp. 1120-1121, 2017.

[28] F. Y. Wang, C. Li, Y. Guo et al., "Parallel gout: an ACP-based system framework for gout diagnosis and treatment," *Moshi Shibie yu Rengong Zhineng/Pattern Recognition and Artificial Intelligence*, vol. 30, no. 12, pp. 1057–1068, 2017.

[29] N. V. K. Jasti and R. Kodali, "An empirical investigation on lean production system framework in the Indian manufacturing industry," *Benchmarking: An International Journal*, vol. 26, no. 1, pp. 296–316, 2019.

[30] B. K. Mishra and R. Sahoo, "A hybrid knowledge mining approach to develop a system framework for Odia language text processing," *Materials Today Proceedings*, vol. 5, no. 1, pp. 1335–1340, 2018.

[31] S. Aljawarneh, M. B. Yassein, and W. A. Talafha, "A multithreaded programming approach for multimedia big data: encryption system," *Multimedia Tools and Applications*, vol. 77, no. 9, Article ID 10997, 2017.

[32] B. Rodrigues, A. Cardoso, J. Bernardino, N. Simoes, and J. Marques, "Secure remote data collection system using data encryption," *IFAC-PapersOnLine*, vol. 52, no. 27, pp. 400–405, 2019.