International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 4103-4112

https://doi.org/10.70517/ijhsa464526a

Establishment of Risk Analysis Model for Endowment Insurance Data Management Based on Intelligent Optimization RSA Algorithm

Xiaoxu Yin[1,*]
[1]School of Economics, Dalian University Of Finance And Economics, Dalian 116000, Liaoning, China
Corresponding authors: (e-mail: yinxx308@dlufe.edu.cn).

Abstract Nowadays, computer technology and network technology are constantly innovating, and the related information management system is becoming more and more mature. Therefore, it is necessary to combine the relevant national pension insurance policies, and use computer network technology under the management mode of the new system to establish a fair, just and open system. The old-age insurance system is convenient for insured personnel and managers to manage and inquire about old-age insurance information. Through a sound system and standardized management, work efficiency can be improved, so that the old can depend on and support the old. Combining the actual situation of current pension insurance intelligent management and risk management and control, this paper uses the relevant theoretical knowledge of software engineering to conduct a complete analysis and design of the development of the pension insurance information management and risk management and control system for land-expropriated persons. At the same time, taking this module as an example, it focuses on the development, design and implementation of the three-tier architecture model of the client, middleware, server-side business logic layer and data storage layer. Finally, the functional application display and testing of the system are given. According to the experimental verification, its development module has significantly improved the accuracy of risk management and control, and the standard error value has decreased by 3%.

Index Terms RSA optimization, evolutionary algorithm, pension insurance, data management, risk analysis

I. Introduction

The problems existing in social endowment insurance and people's cognition of social insurance, such as the transparency and security of social insurance information and the safety of social insurance funds, have led to many people's prejudice against social endowment insurance [1] and questioning. In view of the above problems, it is necessary to design and develop an online social pension insurance information system to improve people's understanding of social security work, improve social security work ability, and quickly improve the social security system. Social endowment insurance is an endowment insurance system that covers the people and constitutes a part of my country's insurance system. The management of social security information has been transformed from the previous paper-based handwriting method to a computer system management method. There must be a series of problems in this transformation process. In order to ensure the security of social security information and improve people's awareness of social security under the new situation [2].

In a word, as a developing country, my country's insurance system needs to be developed and improved, and gradually mature. When faced with the difficulties in pension payment caused by aging, countries around the world have also reformed the pension system one after another, trying to establish a new institutional framework, hoping to fully guarantee the living standards of the elderly on the basis of the sustainable development of the system. Faced with the same problem, our country has also promulgated corresponding laws and regulations, thus providing a legal basis for the basic pension system. Under the constraints of the law, our country's basic pension system will gradually mature and improve. After a preliminary understanding of the old-age insurance system and management system, it is found that the establishment of the old-age insurance system is necessary. Therefore, the management mode can be changed, the organizational structure of management can be optimized, and the scientific process of endowment insurance management can be developed as soon as possible.

But at the same time, although information technology has provided many conveniences for the management of pension insurance data, many criminals use the Internet to conduct illegal and criminal acts, which also brings certain risks to the management of pension insurance data. For example, every day our users need to upload, transmit, exchange, download, and store information on the network to obtain various resources they need, but criminals will intercept, tamper, destroy, and steal users' information, causing users to suffer mental shock, financial loss, and leakage of personal privacy. If important units such as banks and state agencies are successfully invaded by hackers, the losses will be immeasurable, including the information of state citizens, the ownership of state property, and national security issues.

Compared with symmetric ciphers, the RSA algorithm is relatively secure, but the amount of computation required to obtain encryption keys and decryption keys is very large, resulting in low computational efficiency, so the operation speed cannot be compared with symmetric ciphers [3]. In today's fast-developing and efficient society, it is very necessary to reduce the computing waiting time. While improving the computing speed, the security of the algorithm should also be guaranteed [4]. In addition, the openness of the RSA password is also very open to meet the needs of the network environment. It is relatively easy to understand the algorithm theory, but the power multiplication operation of large integers is very complicated, time-consuming and labor-intensive.

Taking the intelligent optimization of RSA as a breakthrough, exploring the risk analysis model of endowment insurance data management is the current research hotspot. The design of this system will enable us to make full use of modern computer communication technology, improve the management level, further improve the existing management concepts and management methods, and accelerate the modernization, informatization and scientific process of social endowment insurance management.

II. Related Work

Recently, the role of multimedia communication in digital communication is gradually increasing, and the daily storage and transmission of multimedia data has greatly increased. The protection of data security and privacy has brought urgent challenges to experts and scholars in the field of security. In 1949, Shannon first proposed the use of scrambling-diffusion structures in secure communications. In 1998, in order to understand the relationship between discrete chaos and cryptosystem, [5] considered the possible relationship between the two, and based on this, a symmetric image encryption scheme was proposed combined with a two-dimensional Baker map. Subsequently, chaos theory began to be widely known, and algorithms based on chaos theory were gradually increased in the proposed image encryption schemes. [6] uses the Cat map to rearrange the pixel positions of the image and uses the Logistic map to greatly reduce the strong correlation between image pixels. Then, the low-frequency coefficients are scrambled and diffused sequentially by using the pseudo-random sequence generated by the hyperchaotic system. This method is different from the traditional scrambling operation, and is closely combined with discrete wavelet transform in the process of diffusion.

In order to save the time required for the image encryption and decryption process, some works [7] use spatiotemporal chaos, which realizes the change of pixel values while performing scrambling, and effectively generates pseudo-random numbers through some traditional encryption operations, further reducing the time consumed. The security level of conventional permutation-only image encryption algorithms is not high. In order to avoid this shortcoming, [8] proposes a novel bit-level permutation scheme based on chaos. In [15], the input image is decomposed into bit planes, and the different planes are exchanged. Then the chaotic map is used for diffusion, and the scheme of converting four grayscale images into one encrypted image is realized. [16] performs XOR diffusion on the image components respectively, and uses the Chen chaotic system for encryption twice by establishing a bijective function between the sub-block set and the S-box. Among them, the initial value and parameter design of the chaotic system are dynamically changed, which increases the security.

Most image encryption algorithms require iteration and quantization of the key stream during the diffusion operation, which reduces the overall encryption efficiency. [17] uses a dynamic reuse permutation matrix to generate a dynamic diffusion key stream, which does not require additional sequence iteration and quantization process, greatly improving the efficiency.

One approach to chaotic encryption uses one-dimensional Logistic mapping to generate the initial value of a quantum chaotic system, fully integrating plaintext information into the encryption process through three-dimensional Arnold scrambling and diffusion. Another method tunes a sinusoidal map with the output of the logistic map, creating a new chaotic map by extending the phase plane to two dimensions; this chaotic system is then used to design an image encryption scheme with added random values.

To overcome the contour problem in interference encryption, a double image encryption method can be applied. In this technique, two original images are combined, scrambled using a logistic map, and split into two new components. One component is encrypted into ciphertext with double random phase encoding, while the other is decomposed into a phase mask, which is encoded alongside another phase mask to enhance the nonlinearity of the cryptosystem.

Another method involves an image parallel encryption algorithm based on a chaotic window, in which grayscale images are encrypted using logistic mapping, making the approach suitable for practical communication and parallel processing. In addition, a bit-level scrambling method can be used to swap low- and high-order planes, thereby reducing inherent redundancy in the image. Some encryption designs employ a combination of obfuscation and diffusion linear transformation mechanisms of one-dimensional chaotic maps; however, certain weaknesses in such schemes make them vulnerable to chosen-plaintext attacks. A more secure alternative is a chaotic image encryption method with an alternative diffusion structure, incorporating circular S-boxes and keystream buffers, and performing scrambling and diffusion in a bidirectional multi-round transformation network.

The assumption of establishing an endowment insurance data management risk analysis model based on intelligent optimization RSA algorithm is worthy of attention.

III. Introduction to Relevant Models of Intelligent Optimization of RSA Algorithm

As the most secure asymmetric cryptosystem, the classic RSA algorithm was developed. The encryption key of this algorithm is inconsistent with the decryption key. The calculation of the plaintext encrypted by the encryption key is usually relatively simple. On the contrary, the calculation process of decrypting the ciphertext by the decryption key is very complicated, ensuring that the ciphertext will not be easily cracked by an attacker. A function that is easy to operate and more complicated to decrypt and inverse is called a one-way function. It is precisely because the reverse operation of the one-way function is complicated that the algorithm is not easily broken, thus ensuring the security of information. The one-way function process is as follows:

$$a = bq_1 + r_1, \quad 0 < r_1 < b, \tag{1}$$

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \tag{2}$$

$$\dots$$

$$r_{n-2} = r_{n-1} q_n + r, \quad 0 < r_n < r_{n-1}, \tag{3}$$

$$r_{n-1} = r_n q_{n+1} + r_{n-1} = 0. \tag{4}$$

Here, for each division with remainder, the remainder is reduced by at least one, and b is finite, so we do at most b divisions with remainder and always get an equation with a remainder of zero.

III. A. *Optimizing RSA Encryption*

In the cryptosystem, the core of various encryption algorithms is the encryption and decryption process. Similarly, in the RSA algorithm, the public key is used to encrypt the plaintext to ensure the security of the information during the transmission process, and the private key is used to decrypt the ciphertext. Both processes involve modular exponentiation of large integers. Suppose the encryption process is:

$$C \equiv M^e \pmod{n}. \tag{5}$$

During the transmission process, a hacker can intercept the ciphertext, and since the public key is open to all users, the hacker can attempt to brute force the public key to crack the modulus n. To ensure security, it is usually necessary to set the values of e and n such that the number of bits is large, which increases security but also consumes more computing resources. Therefore, how to effectively handle the power multiplication of large integers becomes the key.

The key generation stage, the encryption stage, and the decryption stage all work together in common improvement methods to enhance the overall performance of the algorithm. The combination of improvements in each stage forms the system of the double-enhanced RSA cryptographic algorithm.

III. B. *Digital Signature of RSA Algorithm*

The RSA algorithm is very powerful; it can not only encrypt and decrypt information to ensure security but also authenticate the sender of the information. This measure confirms whether the identity of the sender is legitimate. It is crucial to ensure security by eliminating the threat of attackers from the outset. The method used in the verification process is called a digital signature. In the process of digital signature, if the user is legitimate, they will possess the correct private key; an illegitimate user will have an incorrect private key. The private key is used to sign the plaintext M. Assuming the signed message is H, we have:

$$H \equiv M^e \pmod{n}, \tag{6}$$

After the signature is completed, the receiver authenticates the validity of the message. The authentication process involves restoring the message by using the public key. Let the restored information be H^1, then:

$$H^1 \equiv M^e \pmod{n}. \tag{7}$$

The restored information is then compared with the original message. If the two match, it confirms that the sender possesses the correct private key and the identity is verified.

IV. Methods

The database is responsible for saving business processing data and can also complete some business processing logic. The core platform architecture is shown in Figure 1.

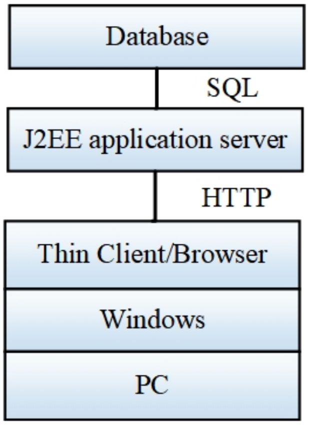

Figure 1: Core platform architecture

The file management of pension insurance participants mainly involves operating and maintaining the basic information of insured units and individuals, including adding, modifying, and deleting information. The business handling personnel enter the basic information of the unit according to the registration form of the insured unit, enter the relevant information of the employee, and establish the personal file of the employee. After creating unit and personal files, modifications can be made when necessary. When the unit provides details of personnel increases or decreases, personnel file management is carried out accordingly. For example, on-the-job employees may be transferred to retired or deceased status, and retired personnel may be transferred to deceased personnel.

In this process, it is necessary to shield database differences, complete the encapsulation of access, and reduce the impact on business logic programs as much as possible when the database is migrated. Standard and commonly used database access tools should be provided to minimize repetitive statement preparation and complete the mapping of the business model to the data model, as shown in Figure 2.

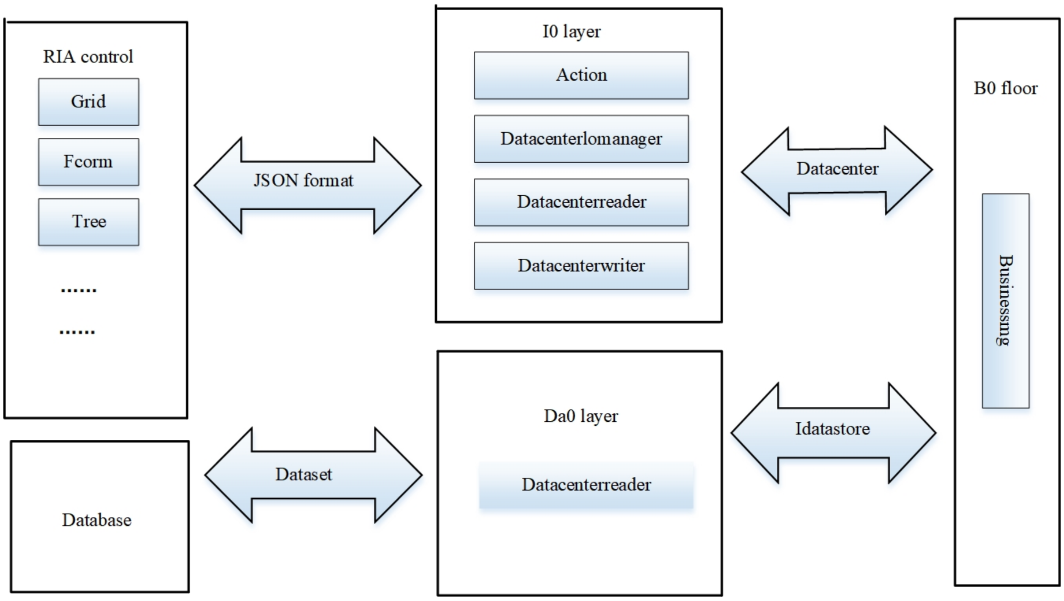

Figure 2: Mapping between business model and data model of pension insurance database

When issuing endowment insurance benefits, it is necessary to first calculate the insurance benefits, and then record the transactions after arrival. For late payment by insurance units, supplementary payment processing procedures are implemented. In the event of death, a one-time funeral payment is made and recorded as a completed transaction. The operator can inquire and modify the relevant information at any time to ensure that pension insurance funds can be transferred and issued in time. The insured unit and its in-service and retired employees can log in to the system through the unit number or ID number to perform related query operations. The overall business process is shown in Figure 3.

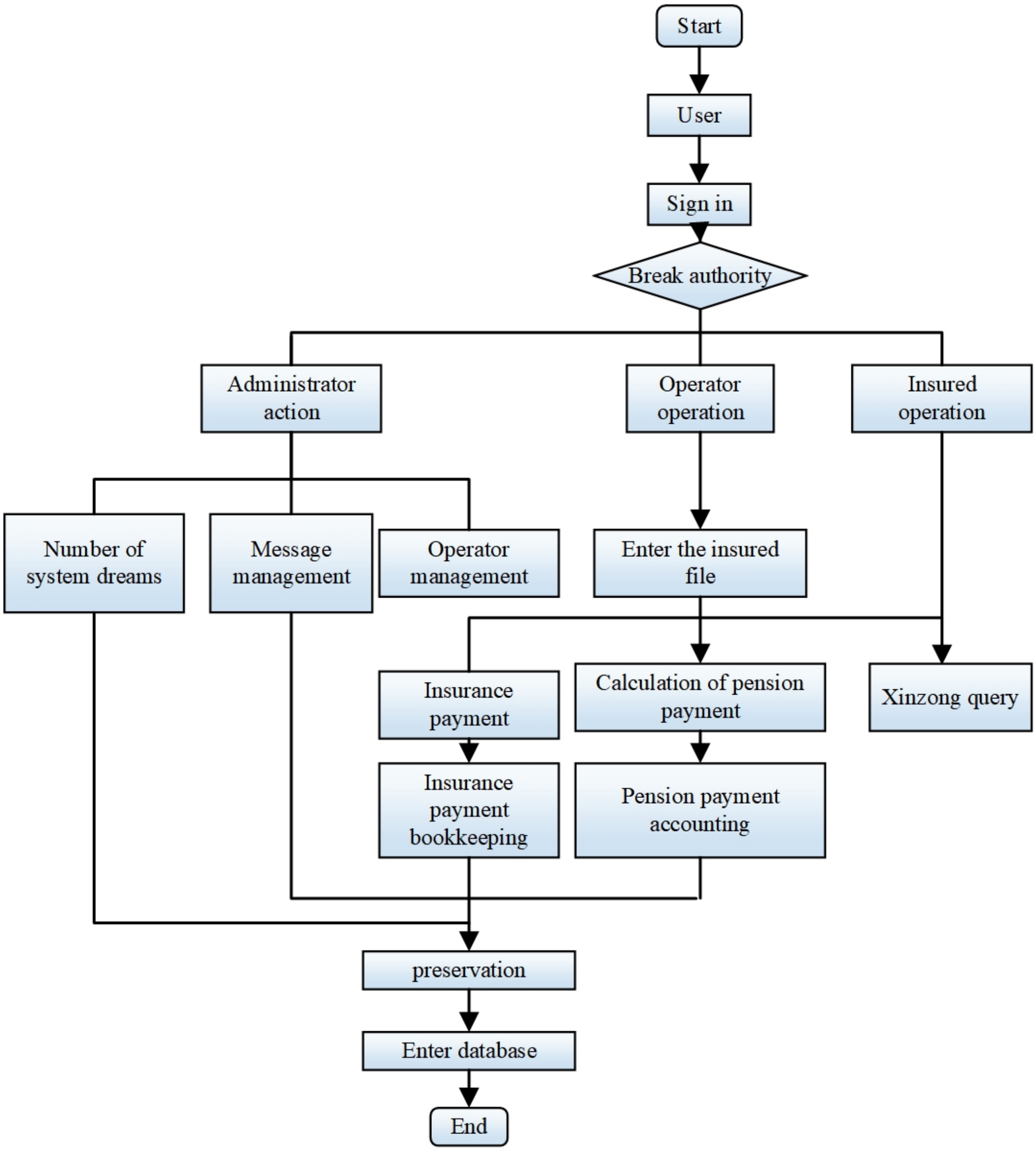

Figure 3: Business flow chart of pension insurance data management and control

IV. A. Data Flow Analysis

A data flow diagram is a tool for expressing information flow and information transformation processes graphically. It records the logical input and output processes of the system and directs the logical input to the required processing. Through the combination of data flow connections, a logical model of the target can be established during demand analysis.

In this case, after the operator logs in to the system with a valid account, they select the corresponding function module according to their account authority to perform business operations, maintaining and processing insurance payment, file management, pension payment, and other related inquiries. The data flow chart of file information management is shown in Figure 4.

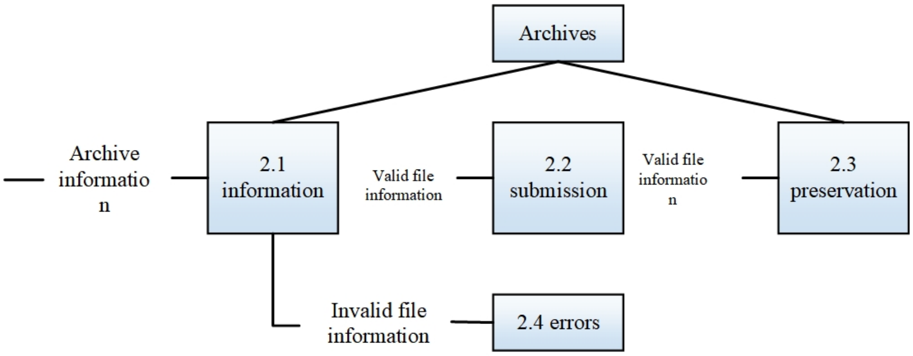

Figure 4: Data flow chart of pension insurance case information management

Once the unit or individual information is entered into the system, insurance payments are made to personnel who meet the relevant regulations of the state and the unit. The data processing flow is shown in Figure 5.

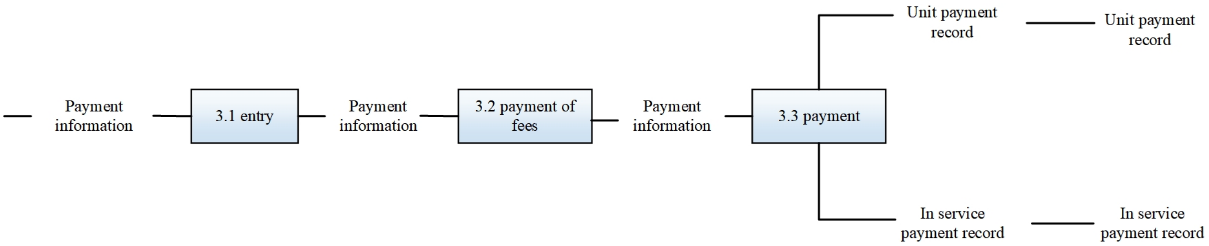

Figure 5: Flowchart of pension insurance data

IV. B. Module Design and Implementation

The operational flow of the module design is shown in Figure 6.

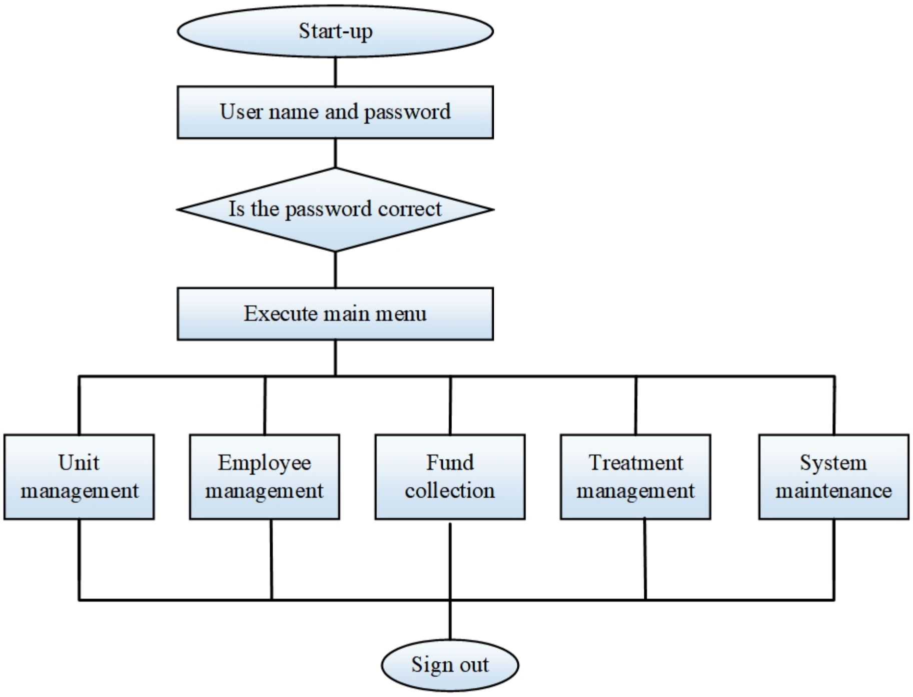

Figure 6: Operation flow

From the overall structure, the system design is divided into several major modules: basic information management, pension treatment management, fund collection management, and system maintenance. The structure of the entire system is shown in Figure 7.

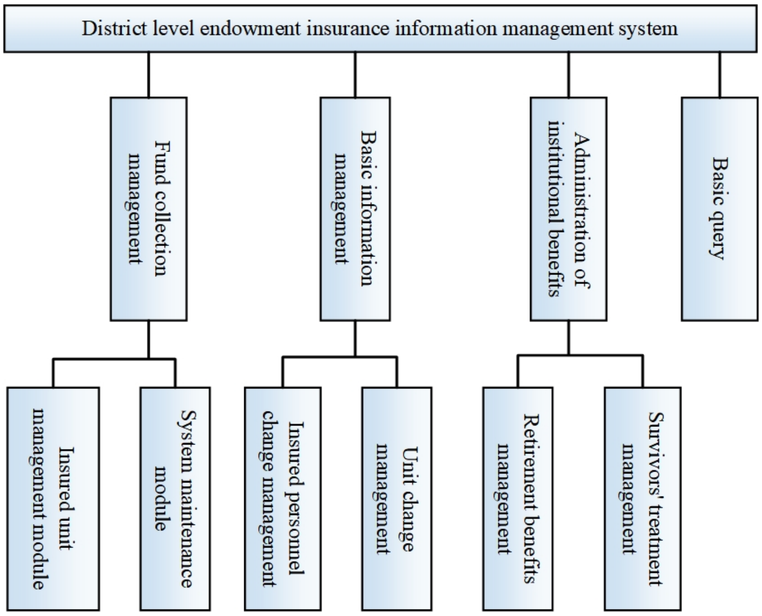
District level endowment insurance information management system
Fund collection management
Basic information management
Administration of institutional benefits
Basic query
Insured unit management module
System maintenance module
Insured personnel change management
Unit change management
Retirement benefits management
Survivors' treatment management

Figure 7: System structure diagram

In the key generation stage of the algorithm, a very important modulus n is generated, which is crucial to the algorithm. An attacker could perform brute force attacks on the modulus to obtain the prime numbers that compose n, and then calculate the Euler function value, public key, and private key. To address this vulnerability, a hidden key G is designed to replace the modulus n in the key generation stage, preventing direct attacks and increasing security.

Additionally, a set of secret keys is generated at this stage. These keys are used in the encryption stage to enhance confidentiality alongside the public key. Even if the attacker cracks both the public and private keys, the secret key is still required to fully decipher the message.

In the encryption phase, the plaintext is encrypted with both the secret key and the public key, producing ciphertext, which is then transmitted to the receiver. In the decryption phase, the receiver uses the secret key and private key to decrypt the message. Since this process involves exponentiation of large prime numbers and significant computation, the modular repeated square algorithm is applied to reduce the computation and improve operational efficiency.

V. Case Study

When adding an endowment insurance file, the system will uniquely identify the unit or employee. After information verification and identity authentication, if there is an error, the system will prompt for repeated entry. When modifying data and transferring files, the operator must first enter the number corresponding to the unit or the ID card information of the employee, and the system will match it in the database. If the file does not exist, a warning box will pop up, prompting the user to check the input data again.

The above operation process requires the system to connect to the database, check the information, and effectively compare the current information with the input data after modification and verification. Parameter information such as system public parameters, social insurance payment ratio parameters, payment area parameters, and payment ratios are maintained. Its logical view is shown in Figure 8.

To test the performance of the proposed algorithm, the work is simulated on MATLAB software using the Windows 10 operating system. The risk time cost is shown in Table 1.

Table 1: Optimized encryption time cost of RSA algorithm.

Image	Key stream generation (s)	Scrambling diffusion (s)	Round time (s)
Boat (256×256)	0.256227	0.241598	0.241729
Male (1024×1024)	0.550869	2.227202	2.227412

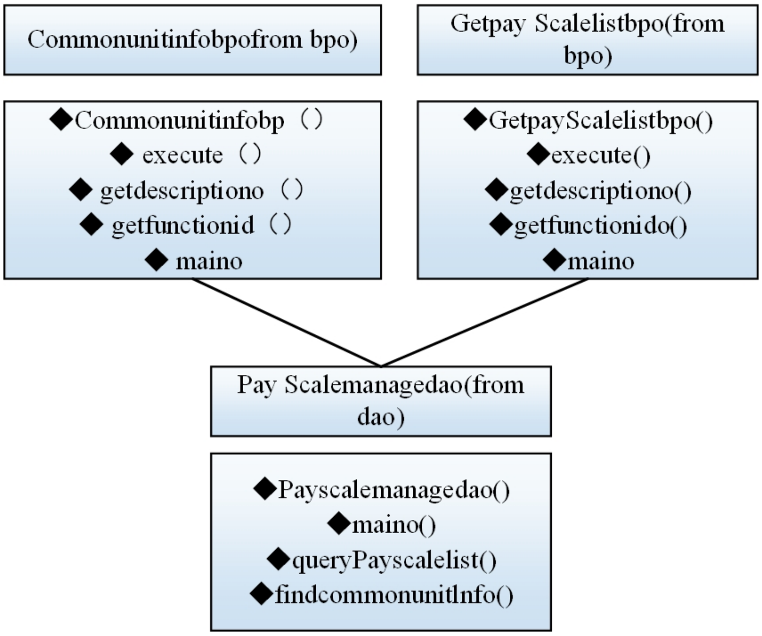

Figure 8: System parameter management logic diagram.

V. A. *Security Enhancement*

To test the changes in the distribution of pixel values before and after encryption of the pension insurance data, a histogram analysis was performed. Figure 9 shows the overall outline of the distribution of pixel values before and after encryption. It can be seen that the gray value is evenly distributed in the encrypted data, indicating that no useful information can be obtained from pixel statistics, and the histogram attack can be resisted.

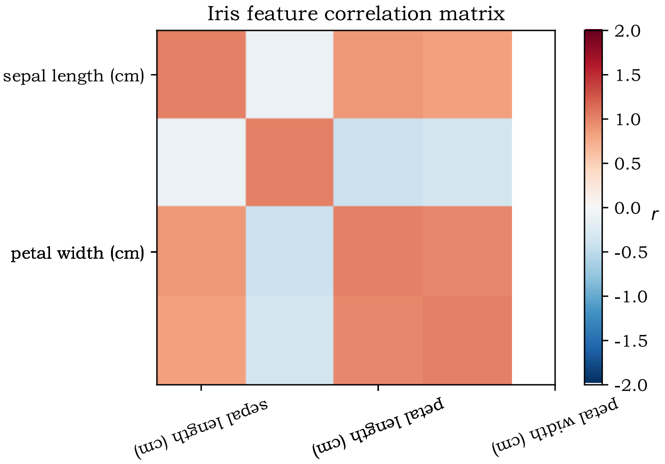

Figure 9: Overall outline of pixel value distribution before and after encryption.

The chi-square test values for plaintext and encrypted images are shown in Table 2. If the chi-square value is smaller than 293.2478, it indicates that the ciphertext images pass the test.

Table 2: Chi-square test values.

Image	Boat	Camera	Male	Peppers
Plaintext image	383969.69	392972.18	709341.68	340999.45
Ciphertext image	239.3282	241.9552	257.8116	267.2065
Result	Adopt	Adopt	Adopt	Adopt

Figure 10 compares the correlation coefficient between encrypted pension insurance data and other algorithms. The proposed algorithm significantly weakens the correlation between adjacent pixels, indicating strong resistance to statistical analysis attacks.

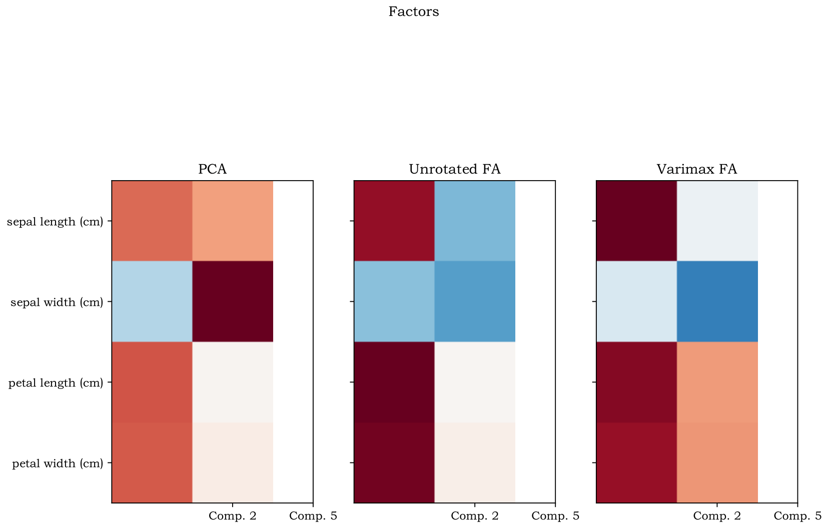

Figure 10: Comparison of the correlation coefficient between encrypted pension insurance data and other algorithms.

V. B. Information Entropy Optimization

The information entropy of the ciphertext is shown in Table 3. The values approach the theoretical value, and the local information entropy is above 7.95.

Table 3: Entropy of ciphertext information.

Entropy	Boat	Camera	Male	Peppers		
				R	G	B
Plaintext image	7.19135	7.10905	7.52375	7.33883	7.49626	7.05832
Ciphertext global entropy	7.99935	7.99934	7.99983	7.99925	7.99925	7.99936
Ciphertext local entropy	7.95558	9.75659	7.95708	7.95708	7.95678	7.95645

Table 4 compares the information entropy of color images from different schemes. The proposed scheme achieves the highest entropy, indicating stronger pixel randomness.

Table 4: Image information entropy comparison.

Algorithm	F	G	B
This scheme	7.9994	7.99995	7.9995
Literature [12]	7.9987	7.9992	7.9985
Literature [15]	7.9972	7.9974	7.9972

When the initial value of the generalized Arnold map changes, the decrypted image is shown in Figure 11. The results show that the proposed algorithm is very sensitive to key changes.

At present, there are two main methods to crack a password system. One is an exhaustive search of keys, which requires guessing all possible cipher combinations. However, the RSA algorithm is calculated at the exponential level in the encryption process, making exhaustive search impractical. Therefore, the only feasible approach is cryptanalysis, which requires factoring large integers. Although it is possible to decipher low-level keys, as the key length increases, the time required for factoring grows exponentially.

VI. Conclusion

This paper introduces an image encryption algorithm based on a generalized Arnold map and the RSA algorithm, where the parameters of the generalized Arnold map are generated using the RSA algorithm. The method employs two generalized Arnold maps to generate the key stream, thereby increasing the key space and enhancing security. The proposed scheme leverages the computational difficulty of large integer factorization to improve the security of image transmission.

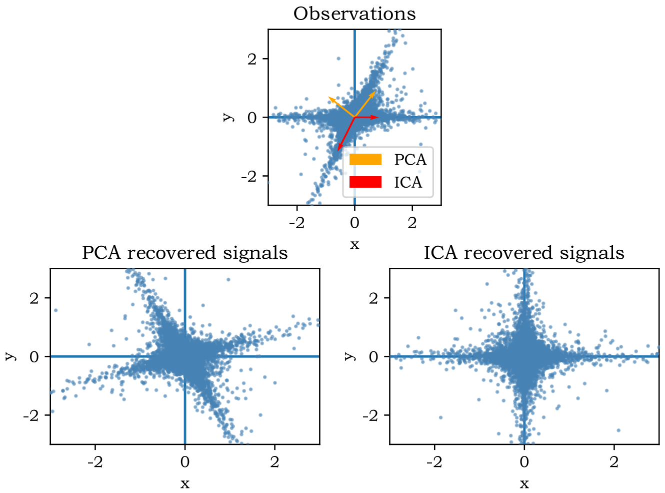

Figure 11: Decrypted image of mapping initial value change.

To verify the effectiveness of the encryption algorithm, analyses of the histogram, correlation coefficient, information entropy, and sensitivity were conducted. The results indicate that the algorithm proposed in this study demonstrates strong resistance to histogram difference attacks.

Data Availability

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

References

[1] Zou, C., Du, S., Liu, X., Liu, L., & Li, Z. (2021). Optimizing the empirical parameters of the data-driven algorithm for SIF retrieval for SIFIS onboard TECIS-1 satellite. *Sensors, 21*(10), 3482.

[2] Nie, C., Wei, H., Shi, J., & Zhang, M. (2021). Optimizing actuated traffic signal control using license plate recognition data: Methods for modeling and algorithm development. *Transportation Research Interdisciplinary Perspectives, 9*, 100319.

[3] Acampora, G., & Vitiello, A. (2021). Implementing evolutionary optimization on actual quantum processors. *Information Sciences, 575*, 542–562.

[4] Luo, J., Gupta, A., Ong, Y. S., & Wang, Z. (2019). Evolutionary optimization of expensive multiobjective problems with co-sub-Pareto front Gaussian process surrogates. *IEEE Transactions on Cybernetics, 49*(5), 1708–1721.

[5] Hu, X. B., Wang, M., Leeson, M. S., Paolo, E., & Liu, H. (2016). Deterministic agent-based path optimization by mimicking the spreading of ripples. *Evolutionary Computation, 24*(2), 319–346.

[6] Islam, M. M., Singh, H. K., Ray, T., & Sinha, A. (2017). An enhanced memetic algorithm for single-objective bilevel optimization problems. *Evolutionary Computation, 25*(4), 607–642.

[7] Jia, Y. H., Chen, W. N., Gu, T., Zhang, H., & Zhang, J. (2018). Distributed cooperative co-evolution with adaptive computing resource allocation for large scale optimization. *IEEE Transactions on Evolutionary Computation, PP*(99), 1–1.

[8] Du, X., Ni, Y., & Ye, P. (2015). A multi-objective evolutionary algorithm for rule-based performance optimization at software architecture level. *Proceedings of the ACM*, 1385–1386.

[9] Han, D., Du, W., Du, W., Jin, Y., & Wu, C. (2019). An adaptive decomposition-based evolutionary algorithm for many-objective optimization. *Information Sciences, 491*, 204–222.

[10] Chen, Y., Zhong, J., Feng, L., & Zhang, J. (2019). An adaptive archive-based evolutionary framework for many-task optimization. *IEEE Transactions on Emerging Topics in Computational Intelligence, PP*(99), 1–16.

[11] Tian, Y., Zhang, X., Wang, C., & Jin, Y. (2020). An evolutionary algorithm for large-scale sparse multiobjective optimization problems. *IEEE Transactions on Evolutionary Computation, 24*(2), 380–393.

[12] Zhang, C., Shan, G., & Roh, B. H. (2024). Communication-efficient federated multi-domain learning for network anomaly detection. *Digital Communications and Networks*.

[13] Zhang, C., Shan, G., Lim, J., & Roh, B. H. (2024). Dynamic reinforcement learning for optimal Go AI training: Adaptive adjustment and optimization. *IEEE Transactions on Consumer Electronics*.

[14] Elkawkagy, M., Elwan, E., Alsumayt, A., Elbeh, H., & Aljameel, S. S. (2024). Elevating big data privacy: Innovative strategies and challenges in data abundance. *IEEE Access, 12*, 20931–20941.

[15] Timilehin, O. (2024). Quantum computing for big data: Pioneering techniques in uncertainty modeling and scalable data engineering.

[16] Jasim, K. F., & Zeki, A. M. (2024). Design of protection software using some cryptosystems for cloud database files. *Cihan University-Erbil Scientific Journal, 8*(1), 70–79.

[17] Tan, Z. S., Chen, C. H., Chen, X. B., & Xin, Y. (2024). A study on privacy protection of cross-chain transactions based on improved notary mechanisms. *IEEE Access*.