Intelligent Metallurgical Data Statistics Software Encryption based on Real-Time Double Encryption Algorithm

Mu Chen¹, Hongfa Li², Fucai Luo³

¹ Global Energy Interconnection Research Institute Co., Ltd., Nanjing, 210003, China
² State Grid Fujian Electric Power Co., Ltd., Information & Telecommunication Branch, Fuzhou, 361004, China
³ State Grid Fujian Electric Power Co., Ltd., Fuzhou, 350000, China

*Corresponding author e-mail: Jybio11@163.com

Abstract. One-way encryption in the traditional encryption system of smart phone makes mobile phone easy to be attacked by the outside world, resulting in poor security performance. In order to solve this problem, a design of security encryption system for smart phone software based on real-time dual encryption is proposed. The method of resource verification integrity is designed, and a group of congruence numbers is added to the software's sensing resources to perform module operations and homomorphic encryption operations to generate encrypted data. In the reversible hiding process of dual encryption for real-time mobile phone information, chaotic sequence is used to realize the global scrambling of mobile phone information location. According to another new set of chaotic sequence, the 0bit and 1bit are scrambled in the information value of mobile phones. Chaos mapping is used to generate chaotic sequences and are associated with the mobile phone information to ensure that the dual encryption of mobile information can resist the selection of message attack. The experimental results show that the maximum confidentiality of the system can reach 96%, which is of practical value.

Keywords: Chaotic sequence, Mobile phone information, Secret key, Confidentiality

1. Introduction
With the rapid development of mobile information and communication technology, smart phone has become an important way to promote the economic progress of China. Once the information is leaked, it will cause an unexpected economic loss to a single user or even to the society. Therefore, in today's developed mobile communication system, the design of information security encryption system is particularly important. Because the traditional encryption system for smart phone has poor effect, it cannot guarantee the security of mobile phone information [1]. In the process of mobile communication, the confidentiality and integrity of information are very important. Information encryption is an important means to ensure transmission security. Therefore, the chaotic sequence is used to design the security encryption system of mobile phone information. The chaotic sequence has a strong dependence on the initial data value, and it will not be easily intruded by hackers.
2. Software Design of Encryption Algorithm for Smart Phone

2.1. Parameter setting
In resource sensing, a group of congruence numbers is added to carry out modular operation and homomorphic encryption operation to generate encrypted data. The existing resources of the mobile phone are fused to directly encrypt the encrypted data of the sub resources, and the fusion results are transmitted to the higher level fusion resources. The real resources in the results are extracted by the superior fusion resource, and the residual theorem is used to verify the resource integrity, to give the parameter setting of the integrity verification to satisfy the constraint conditions, and then determine the size of public key. The specific process is as follows:

Supposing that $t$ represents the current time interval, $s_i$ represents the perceptual resources of each resource $m_{i,t}$, and a group congruence $m'$ is added to the resource perceptual resource $m'$ to perform the modular operation [2].

$$E = \left( \sum_{i=1}^n c_{i,t} \times k_{i,t} \right) \mod m'$$  \hspace{1cm} (1)

Where, $m'$ represents the operation of modular 2, $k_{i,t}$ represents the scope of detection resources, and $c_{i,t}$ represents the length of detection resources. To prevent resource spillovers, all resources are temporarily reserved for 5Byte. Each resource is encrypted by homomorphism of resource $d_i$, according to formula 2.

$$c_{i,t} = E(d_i, K, k_{i,t}, p)$$  \hspace{1cm} (2)

Where, $K$ represents the attribute class of resource, $p$ represents the key information, $\gamma$ represents the bit length in the public key $x_i$, and $\eta$ represents the length of the private key. The fusion resource $A_i$ is directly combined with the encrypted data in formula (2) to carry out the additive fusion operation:

$$d_{f,t} = \frac{A_i (a_{i,t} + a_{2,t}) d_i}{c_{i,t} \rho^\gamma} \mod E$$  \hspace{1cm} (3)

Where, $\lambda$ is the public key, $\rho'$ is the bit length of noise $r_i$ in the additive fusion operation, $\rho^\gamma$ is the secondary noise parameter in the fusion process, and $\varphi$ is the noise signal to noise ratio. When the fusion resource $A_i$ receives two ciphertexts $a_{i,t}$ and $a_{2,t}$, the higher level fusion resource receives the data fusion result $d_{f,t}$, that is, all the modular addition operations. The first 10 bytes of $d_{f,t}$ are the actual fusion result $m_{i,t}$ of encrypted data, and the congruent number fusion result of the latter 5 bytes of $m_{i,t}$ is $m_{1,t}, m_{2,t}, m_{3,t}, m_{f,t}$ is extracted from the fusion resource, and then the residual theorem [3, 4] is used to verify the resource integrity.

$$m_{f,t} = \left( \sum_{i=1}^n m_{i,t} \times Q_i \times q_i \right) \lambda \mod d_{f,t}$$  \hspace{1cm} (4)

By comparing the equality of $m_{i,t}$ and $m_{f,t}$, it can prove the integrity of multi-source information resources. $Q_i$ represents integrity verification of inverse elements, $q_i$ indicates integrity verification coefficients, $N$ indicates prime numbers, and $\lambda$ indicates safety parameters.

The parameters in the above resource integrity verification need to satisfy the following constraints: to avoid noise attack, set $\varphi = 2\lambda$; In order to ensure the correctness of decryption of plaintext information, set $\eta = \varphi + 1 + \log_2(I)$; In order to evaluate the auxiliary homomorphic operation
when calculating the addition of the resource congruence number [5], set \( \gamma = \eta^2 \cdot \log \lambda \); in order to apply the requirements of the Chinese remainder theorem to verify resource integrity, set \( \sigma = \gamma + \lambda \).

According to the above parameters, the size of ciphertext public key is \( \Theta(n^2) \). To avoid noise attacks in the cloud computing environment, the length of the public key \( x_i \) is at least 225 bits. At this stage, the length of ciphertext public key is at least 246 bits. Such a large bit length of public key is not applicable in the actual cryptographic system.

2.2. Design of Dual Encryption Algorithm for Real Time Mobile Phone Information

In the reversible hiding process of dual encryption for real-time mobile phone information, chaotic sequence is used to realize the global scrambling of mobile phone information location. According to another new set of chaotic sequence, the 0bit and 1bit are scrambled in the information value of mobile phones. Chaos mapping is used to generate chaotic sequences and are associated with the mobile phone information to ensure that the dual encryption of mobile information can resist the selection of message attack. The specific process is as follows:

The Kent mapping form is used in the selected chaotic system. The mobile phone’s information matrix \( A_{max} \) is scanned with row priority sequence, and after scanning, the sequence \( P = \{p_1, \ldots, p_{max}\} \) with the length of \( m \times n \) is generated. Then the cumulative sum \( \text{sum} \) of all the pixel values are calculated. The control parameter \( S \) of the chaotic encryption system and the number of estimated iterations \( K \) in the system are calculated by using the formula (5).

\[
\begin{align*}
S &= \text{sum} \times 10^8 \\
K &= 1000 + \text{mod}(\text{sum}, 1000)
\end{align*}
\]

The initial key of chaotic encryption for the mobile phone information is input, to eliminate the adverse effects caused by the transient effect after \( K \) times of predicted iteration. The continuous iteration of formula (5) by \( m' \times n' \) times can generate the chaotic sequence \( L = \{L_1, \ldots, L_{max}\} \) with the length of \( m \times n \). The sequence \( L \) is arranged from the order of large to small, and the ordered sequence \( L' = \{L'_1, \ldots, L'_{max}\} \) after chaotic encryption is obtained, which is used to mark the new sequence \( T = \{t_1, \ldots, t_{max}\} \) of the location of the different elements in the initial sequence \( L \) in \( L' \).

According to the new sequence \( T \), the plaintext sequence \( P \) of mobile phone information is scrambled, and the mobile phone information \( P' = \{p'_1, \ldots, p'_{max}\} \) after scrambling is obtained. The scrambling process is expressed by formula (6):

\[
p'_i = p_i, i = 1, 2, \ldots, m \times n
\]

It is assumed that \( d_i = 0.255 \) is another set of chaotic sequence values generated by the chaotic system, and the sequence generated by the group of sequence values is \( W' \). Then the pixel value of the \( i \) th point in the image \( p' \) of the mobile phone information location after the global scrambling is converted into a binary form, and a set of sequence \( P\text{Bit} = \{P\text{Bit}_1, \ldots, P\text{Bit}_i\} \) can be generated. Sequence \( W \) is sorted from small to large, and ordered sequence \( W' \) is obtained. Array \( WT \) is used to store the location of different elements of \( W' \) in \( W \). The \( WT \) is used to scramble sequence \( P\text{Bit} \) to get the reordering sequence \( P\text{Bit}' = \{P\text{Bit}'_1, \ldots, P\text{Bit}'_i\} \) after the pixel bit value is scrambled. Then \( P\text{Bit}' \) has been converted into binary number, and the middle ciphertext \( C_1' \) in chaotic encrypted is obtained. The next encryption of the ciphertext \( C_1' \) is used, and the final ciphertext \( C_i \) of the \( i \)th point is obtained.

\[
\begin{align*}
D_i &= \text{mod}(d_i \times 2^i, 48, 256) \\
C_i &= \text{mod}(D_i + C'_1, 256) \oplus C_{i-1}
\end{align*}
\]

3
In the process of decrypting the mobile phone information, the iteration value of $D_i$ generated by the chaotic system is used as the basis, and the formula for solving $C'_i$ is given:

$$C'_i = \text{mod}(C_i + C_{i-1} + 256 - D_i, 256) \quad (8)$$

Where, $C_{i-1}$ represents the final ciphertext of the $i$th point, the corresponding binary bits of $C'_i$ are executed reverse the scrambling operation, the information bit sequence of the original mobile phone is obtained, then the sequence is converted into decimal number, and the pixel value after the global scrambling is obtained. It can calculate the control parameters of the chaotic system and the number of iterations, and then uses the initial key $x_0$ to obtain the reverse scrambled sequence of generating the pixel position of the mobile phone information. After the reverse scrambled plaintext sequence is transformed into a two-dimensional matrix, the decrypted information can be recovered.

3. Experimental Results and Analysis

The throughput and chaos mapping are taken as experimental subjects, and the confidentiality of information security encryption system for mobile phone is experimentally verified and analyzed.

3.1. Result and Analysis of the Influence of throughput on Information Confidentiality

When mobile information is not stolen by hackers, the system hardware can receive data information, and the number of information that has been successfully received is called data throughput. By changing the amount of information, whether the throughput has an impact on the degree of information security can be verified. Then the traditional system is compared with the system based on chaotic demand sequence, and the result is shown in Figure 1.

![Figure 1. Comparison results of confidentiality of two systems under different throughput](image)

According to Figure 1 it is known that, when the throughput is 20, the confidentiality of traditional encryption system to mobile phone is 30% lower than that of the system based on chaotic sequence; when the throughput is 100, the traditional system achieves the highest confidentiality, which is 80%; when the throughput is 83, the degree of confidentiality of traditional system to mobile phone information is the lowest, which is 8%; when the throughput is 95, the confidentiality of mobile phone information based on chaotic sequence system is 96%; when the throughput is 81, the confidentiality of mobile phone information based on chaotic sequence system is the lowest, which is 25%. From this we can see that throughput has a great influence on the confidentiality of traditional systems, which is 16% different from the maximum value of confidentiality based on chaotic sequence system, and the minimum value is 17%.
3.2. Result and Analysis of the Influence of Chaos Mapping on Information Confidentiality

The information of mobile phone can be obtained according to the system software, and the information of the mobile phone is processed digitally to ensure the circulatory characteristics of the key’s output sequence. Different mobile information has different keys. In order to overcome the shortcoming and irregular problems existing in traditional systems, a perturbation chaotic mapping method is introduced. In order to make the experimental results more reliable, the traditional system is compared with the system based on chaotic demand sequence.

3.3. Experimental Summary

According to the results and analysis of the influence of throughput on the degree of information secrecy, it is found that the throughput has a great influence on the secrecy of the traditional system, and the difference between the highest value of the secrecy based on the chaotic sequence system is 16%, and the minimum value is 17%.

In view of the results and analysis of the influence of chaotic mapping on the degree of information secrecy, the perturbation chaos mapping method introduced in the mobile information security system can improve the degree of security of the system, which indicates that the security coefficient of the chaotic sequence system is high.

According to the above experimental results, we can draw the conclusion that the design of security encryption system based on chaotic sequence for mobile phone information is reasonable.

4. Conclusions

By using the security encryption system for mobile phone information designed in this paper, the problem of poor encryption in traditional system is improved. By adding encryption devices to the computer interface, the security of text and data can be guaranteed. Experiments show that the system has better encryption performance and can meet the needs of the society. At the same time, the system can be realized through the field programmable gate array, and then a system with real-time security encryption communication for mobile information is constructed, so as to adapt to the pace of the rapid development of modern information technology.

Acknowledgments

This research work is funded by 2019 Industrial Internet Innovation Development Project of Ministry of Industry and Information Technology of P.R. China “Comprehensive Security Defense Platform Project for Industrial/Enterprise Networks”.

References

[1] G. Xu, Y. Zhao, Z. Gong, Design of secure network coding scheme by dual encryption based on chaotic sequences, Journal of Computer Applications. 37 (2017) 3412-3416.
[2] Z. Zhao, M. Bi, R. Chen, et al., IMDD-OFDM encrypted system based on data completed scrambling with chaos sequence, Optical Communication Technology. 41 (2017) 12-16.
[3] X. Li, Y. Shen, X. Kang, Privacy information encryption algorithm based on hyperchaotic bidirectional authentication, Bulletin of Science and Technology. 33 (2017), 152-155.
[4] R. Tang, J. Duan, H. Deng, Image encryption algorithm based on logistic chaotic sequence and DES, Journal of Computer Applications. 37 (2017), 89-92.
[5] L. Yan, H. Li, Dynamic key AES encryption algorithm based on compound chaotic sequence, Computer Science. 44 (2017), 133-138.