Research and analysis on sensitive data encryption method in accounting information processing system

Heng Li

Department of Accounting,
Henan Finance University,
Zhengzhou 451464, China
Email: lh12hk@163.com

Abstract: In order to protect the confidentiality and integrity of sensitive data in accounting information processing system, it was necessary to study the sensitive data encryption method. The current encryption method was mainly used different technology to make encryption for the sensitivity of sensitive data, which caused a problem of poor security. In order to improve the security of encryption, a hybrid encryption method for sensitive data of accounting information processing system was proposed. Firstly, the sensitive data was preprocessed. Then, based on the elliptic curve encryption mechanism, the additive and multiplicative homomorphic encryption methods of sensitive data were constructed respectively. Experimental results showed that the cryptographic running time obtained by our proposed method was relatively small and the increase in decryption computation overhead was smaller than the traditional method which was good to improve encryption security.

Keywords: accounting information processing system; sensitive data; encryption methods; homomorphic encryption; elliptic curve encryption mechanism.

Reference to this paper should be made as follows: Li, H. (2020) 'Research and analysis on sensitive data encryption method in accounting information processing system', *Int. J. Internet Manufacturing and Services*, Vol. 7, Nos. 1/2, pp.146–161.

Biographical notes: Heng Li holds a Master's degree. She is a Lecturer and Senior Accountant. Her research directions are financial accounting, financial management, and internal control. She published papers such as 'Thinking on the teaching of comprehensive simulation practical training course of accounting in higher vocational colleges-taking henan finance and taxation college as an example', published in *Journal of Henan College of Finance & Taxation*, 'An analysis of university financial management from the perspective of internal control', published in *Enterprise Reform and Management*, and 'Exploration of the new mode of management accounting in collectivised enterprises, published in *The Chinese Certified Public Accountant*.

1 Introduction

With the rapid development of internet technology, communication technology, digital multimedia technology and information processing technology, the information volume of accounting information processing system has gradually increased in the prosperous

economic society. The use of computer processing accounting information has become increasingly popular; meanwhile, financial information analysis of accounting information processing system also has been widely used in the network environment (Abdulgader et al., 2015; Zhan and Zhang, 2017; Zhu et al., 2018; Liu et al., 2013a). At present, the use of computer processing accounting information included two ways. Detailedly, the first one was in the stand-alone system to process the accounting information and the second was in the computer network environment to process the accounting information (Hua et al., 2015; Seyedzadeh et al., 2015; Liu et al., 2013b). However, in the stand-alone system to process the accounting information was prone to counterfeit accounting information vouchers, and accounting information was easy to modify and so on (Yao et al., 2015; Wang and Zhang, 2016). In the computer network environment to deal with the accounting information, the administrator unified to give the various accounting positions of different permissions, so that making mutual supervision. Besides, it made up the defects for the computerisation of single computer system, making that the confidentiality of system's internal data was stronger of computerised accounting information processing. However, there were still some risks (Gong et al., 2016). The computerisation of accounting information processing system made the traditional paper document information, to be replaced gradually by electronic documents. Paperless office became the mainstream development trend of low-carbon, environmental protection. Compared with the earlier accounting information processing, it was easy for paper office to improve the efficiency of accounting information processing, store and make unified management (Yuan and Li, 2015; Yang and Liu, 2014). However, the accounting information processing system still contained many sensitive data and it was easy to be maliciously copied, transmitted, and modified by criminals, resulting in a serious disclosure of accounting information, and even causing irreparable economy and reputation loss (Lu et al., 2016).

In recent years, it was very common that state organs, large and medium-sized enterprises and even individual business confidential information and sensitive data were illegally stealing. The events of sensitive data malicious tampering in accounting information processing system also occurred from time to time. The disclosure of these sensitive data not only caused the volatility of financial markets, but also seriously affected the security of the entire economy, as well as the authority of the national statistical department. Therefore, it was imperative to encrypt the sensitive data in the accounting information processing system (Liang, 2016). According to the practical application and safety technology needs, there have been put forward a number of encryption methods from the beginning of the era of human civilisation. These encryption methods have played a role in maximum extent in a certain period of time. However, with the continuous improvement of computer computing power and the development of distributed computing, the original encryption method has been seriously threatened, and was decoded in different degrees (Pan, 2015). The sensitive data in the accounting information processing system was still potentially risky of being compromised. In order to prevent the leakage of sensitive data in the accounting information processing system, it was necessary to study the sensitive data encryption method (Tong et al., 2015; Jia et al., 2014).

In recent years, the old encryption technology was constantly being cracked, while the new password technology was constantly being put forward. Li et al. (2016) proposed a sensitive data encryption method of the accounting information processing system based on fuzzy search. Firstly, the fuzzy set construction method based on the Elgamal

proxy encryption mechanism and the wildcard technology was used to make multiple encryption of the sensitive data files in the accounting information processing system, and the keywords in the accounting information processing system were made the fuzzy words set construction and stored to the cloud server; then, according to the authorised user's search request, the keywords in the accounting information processing system in the cloud server were made the fuzzy search, and returned the relevant encrypted file. Finally, authorise users used their own private key to decrypt encrypted files and achieve the sensitive data encryption in the accounting information processing system. The method occupied a large storage space, and the confidentiality was poor. In the sensitive data encryption method of accounting information processing system proposed by Yang et al. (2015). The polynomial ring was firstly used to redefine the addition and multiplication of the sensitive data vector in the information processing system, and construct the polynomial coefficient vector ring of the sensitive data. Then, the rational lattice was used to divide the residual class on the polynomial coefficient vector of sensitive data, and create the quotient rings and their representation set of sensitive data. Finally, the sensitive data integer was explicitly mapped to the representative element, and the other elements of the residual class were divided by the representative element on the polynomial coefficient vector of sensitive data, and the representative element was replaced to realise the sensitive data encryption in the accounting information processing system. This method had the problem of low efficiency and poor security. Another sensitive data encryption method in accounting information processing system was proposed by Wu et al. (2016). Firstly, according to the sensitivity of the sensitive data in the accounting information processing system, the method divided the sensitive data into different sensitive data blocks, and stored the divided data blocks in different folders in the accounting information processing system respectively. Then, according to the security level of sensitive data, the sketch parameter encryption technology of the encryption matrix was used to encrypt the sensitive data to reach the purpose of hiding and encrypting the sensitive data.

In order to enhance the security of sensitive data in accounting information processing system, protect these sensitive data and improve the existing problems in the above mentioned methods, a hybrid encryption method for sensitive data in accounting information processing system was proposed. Experimental results showed that the proposed method enhanced the safety performance of sensitive data with small calculation. Besides, the running time of encryption and decryption was shorter. Therefore, combining multiple encryption methods to ensure the security of sensitive data will be the mainstream of future encryption technology development.

2 Research and analysis on sensitive data encryption method in accounting information processing system

2.1 Preprocessing of sensitive data in accounting information processing system

Firstly, a series of preprocessing, such as cleaning, normalisation and clustering analysis, are made for the sensitive data in the accounting information processing system, so as to summarise the clustering rules of sensitive data, and provide accurate data base for the subsequent sensitive data encryption. The specific operation is as follows.

Assuming that the matrix $D = |X_1, \cdots, X_n|$ represents the sensitive data to be clustered in the accounting information processing system, n represents the number of sensitive data in the accounting information processing system; the characteristics of each sensitive data is represented by m indicators, and its expression is defined by equation (1).

$$\begin{cases} X_i = (x_{i1}, \cdots, x_{im}) \\ i = 1, 2, \cdots, n \end{cases} \tag{1}$$

Then the original sensitive data matrix in the accounting information processing system can be expressed as equation (2).

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix} \tag{2}$$

According to equation (2), it is normalised to make all the attributes of the sensitive data in the accounting information processing system into the same interval to weaken the influence of other redundant data on the whole clustering process. Linear transformation method is usually used to convert the sensitive dataset in the accounting information processing system into a range of values for the inconformity sensitive data. The result of the transformation is taken as a new sensitive dataset, and then the clustering analysis is carried out to provide the basis for the subsequent data encryption.

Assuming that the value v of the attribute A of the sensitive data in the accounting information processing system can be obtained after conversion.

$$v' = \frac{v - \min A}{\max A - \min A} \times (new\_\max A - new\_\min A) \tag{3}$$

In equation (3), max A and min A represent the maximum and minimum values in the sensitive data matrix of the accounting information processing system respectively; *new*_max A and *new*_min A represent the new maximum and the new minimum in the sensitive data matrix of the accounting information processing system, respectively.

When the maximum and minimum values in the sensitive data matrix of the accounting information processing system cannot be determined or there are isolated points, the z-score method is used to normalise them. The value v of the attribute A of the sensitive data in the accounting information processing system can be obtained after the conversion.

$$v' = \frac{v - \overline{A}}{\sigma_A} \tag{4}$$

In equation (4), $\overline{A}$ represents the mean value of the sensitive data attribute A in the accounting information processing system; σ_A represents the standard variance of the sensitive data attribute A in the accounting information processing system.

The dissimilarity matrix of sensitive data in accounting information processing system refers to the dissimilarity between any two of n sensitive data objects. The expression is an $n \times n$-dimensional matrix, which is expressed as equation (5).

$$\begin{bmatrix} 0 & & & \\ d(2,1) & 0 & & \\ \cdots & \cdots & 0 & \\ d(n,1) & d(n,2) & \cdots & 0 \end{bmatrix} \tag{5}$$

In equation (5), $d(i, j)$ is the dissimilarity quantification index between the sensitive data object i and the sensitive data object j in the accounting information processing system. Generally, it is the non-negative number. When the sensitive data object i and the sensitive data object j in the accounting information processing system are more similar or closer to each other, the closer the value of the dissimilarity quantisation index is to 0; the more the difference between the sensitive data object i and the sensitive data object j in the accounting information processing system, the bigger the value of the dissimilarity quantisation index. The sensitive data object i, j and k in the accounting information processing system are usually satisfied the following mathematical properties.

$$d(i, j) \geq 0 \tag{6}$$

$$d(i, j) = 0 \tag{7}$$

$$d(i, j) = d(i, j) \tag{8}$$

$$d(i, j) + d(j, k) \geq d(i, k) \tag{9}$$

Equation (6) represents a value in the accounting information processing system, where the distance between sensitive data objects is non-negative; equation (7) represents the distance between the sensitive data objects themselves in the accounting information processing system is zero; equation (8) represents the distance between the sensitive data objects in the accounting information processing system is symmetrical; equation (9) represents that the distance between the sensitive data objects to meet the nature of 'the sum of both sides is not less than third sides' in the accounting information processing system.

In the accounting information processing system, the degree of dissimilarity between sensitive data objects is usually calculated based on the distance between sensitive data objects. Assuming that $i = (x_{i1}, x_{i2}, \cdots, x_{in})$ and $j = (x_{j1}, x_{j2}, \cdots, x_{jn})$ represent two n-dimensional sensitive data objects in the accounting information processing system, the most commonly used distance measurement method is as follows.

1 In the accounting information processing system, the Euclidean distance between the sensitive data objects can be calculated by equation (10).

$$d_1(i, j) = \left[\sum_{k-1}^{n} \left(x_{ik} - x_{jk} \right)^2 \right]^{1/2} \tag{10}$$

2 In the accounting information processing system, the Manhattan distance between the sensitive data objects can be calculated by equation (11).

$$d_2(i, j) = \sum_{k-1}^{n} \left| x_{ik} - x_{jk} \right| \tag{11}$$

3 In the accounting information processing system, the Minkowski distance between the sensitive data objects can be calculated by equation (12).

$$d_3(i, j) = \left[\sum_{k-1}^{n} \left(x_{ik} - x_{jk} \right)^q \right]^{1/q} \tag{12}$$

In equation (12), q denotes a positive integer of the sensitive data in the accounting information processing system; when $q = 1$, q denotes the Manhattan distance calculation formula between the sensitive data objects in the accounting information processing system; when $q = 2$, q denotes the Euclidean distance formula between the sensitive data objects in the accounting information processing system. It can be seen that equation (10) and equation (11) are the special circumstances of the Minkowski distance between the sensitive data objects in the accounting information processing system.

If the variable q is to be given a weight to represent the importance of the sensitive data in the accounting information processing system, the calculation formula of the Minkowski distance between the sensitive data objects with weights in the accounting information processing system can be transformed into equation (13).

$$d(i, j) = \left[\sum_{k-1}^{n} w_k \left(x_{ik} - x_{jk} \right)^q \right]^{1/q} \tag{13}$$

Similarly, the weighted formula also applies to the Manhattan distance and Euclidean distance between the sensitive data objects in the accounting information processing system.

According to the above calculation results, K-means clustering method is used to classify the sensitive data in the accounting information processing system. Firstly, k' sensitive data objects are arbitrarily selected from n sensitive data objects in the accounting information processing system as the initial clustering centre; the rest of the other sensitive data objects are assigned to the most similar clustering respectively according to their similarity of these clustering centres, that is, the distance between the sensitive data objects in the system and them; then the new clustering centre of the sensitive data in the accounting information processing system are calculated, that is, all average of the sensitive data objects is calculated; repeat this process until all the sensitive data in the accounting information processing system is completed.

The preprocessing steps of sensitive data in the accounting information processing system are described as follows.

1 Sensitive data cleaning

In the accounting information processing system, a large number of sensitive data in the collection process will produce dirty data, abbreviation word abuse, sensitive data input errors, records duplication, spelling errors, measurement unit confusion, outdated coding, etc. which is easy to lead to incomplete data, including noise and inconsistency. Thus, it needs to carry out sensitive data cleaning. The purpose of cleaning is achieved by filling the vacancies in the accounting information processing system, smoothing noise sensitive data, identifying and removing the isolated points of sensitive data, and solving the problem of sensitive data inconsistency.

2 The standardisation processing of sensitive data

If the attribute of the sensitive data is clustered, it needs to be normalised. Which can prevent that the sensitive data attribute of which has the larger order occupies too much weight to the smaller one. The original sensitive data in the accounting information processing system can be standardised to ensure that all the attributes of the sensitive data getting the same weight. If the attribute of the sensitive data is not a numeric attribute, it does not need to be normalised. Calculating the dissimilarity matrix of sensitive data to calculate the distance between the sensitive data objects and them can make them standardisation.

3 Using K-means to cluster sensitive data

According to the results of cleaning and normalisation, the sensitive data in the accounting information processing system are clustered and the distance between the sensitive data matrix objects is calculated according to equations (10)–(12).

4 Clustering rules of sensitive data

Assuming that U is a database in the accounting information processing system; R is all the clustering rules that can be mined from U; R_H is the data clustering rules which need to be hidden according to some security measures, then it is said that R_H is the clustering rules of sensitive data in the accounting information processing system; in addition, there are the following other clustering rules R_H', it meets $R_H \cup R_H' = R$, then called R_H' as the insensitive clustering rules of data.

These restricted data clustering rules R_H are extracted from the accounting information processing system database U, and these objects which are related to the restricted data rule R_H are called sensitive data.

Supposing that Y is the set of sensitive data in the accounting information processing system database U, Y_T is the object related to the sensitive data clustering rule R_H in the accounting information processing system, then Y_T is the sensitive data satisfying $Y_T \subset Y$.

2.2 Elliptic curve encryption mechanism of sensitive data in accounting information processing system

According to the preprocessing result of sensitive data and the clustering rules of sensitive data in the accounting information processing system in Section 2.1, two different encryption methods are calculated by using the advantages of elliptic curve encryption mechanism. The details of the process are as follows.

The calculation expression of the common elliptic curve equation on the finite field $GF(q')$ of the sensitive data in the accounting information processing system is defined as equation (14).

$$E : y^2 = x^3 + ax + b \tag{14}$$

In equation (14) a, b, x, $y \in GF(q')$, q' is a large prime number of sensitive data in the accounting information processing system, and $4a^3 + 27b^2 \neq 0 \pmod{p}$. The elliptic curve addition criterion for sensitive data can be defined as assuming that $p(x_1, y_1)$, $Q(x_2, y_2)$ is any two points on the common elliptic curve sensitive data equation E, the straight line

pass through p and Q is intersected to E at point $R'(x_3, y_3)$, symmetry point of R' point for the x-axis is $p + Q$, then equation (15) is obtained.

$$p + Q = x_3 + y_3 \tag{15}$$

According to equation (15), the scalar multiplication of the sensitive data on the elliptic curve is a number of additions of the same point on the elliptic curve. A point P on the elliptic curve is set. For a point $\kappa \in GF(q')$ on the finite field, then the calculation expression of scalar multiplication κP of the sensitive data on the elliptic curve is defined as equation (16).

$$\kappa P = P + P + \cdots P \tag{16}$$

There are many methods for calculating scalar multiplication κP of sensitive data on elliptic curves, the simplest of which is the binary expansion method. Assuming that m' is the length of binary expansion of κ, then the calculated expressions for κ and κP are defined as equations (17)–(18).

$$\kappa = \sum_{i=m'-1}^{0} \kappa_i^* 2^i \tag{17}$$

$$\kappa P = \left(\sum_{i=m'-1}^{0} \kappa_i^* 2^i \right) P = 2\left[\cdots 2\left[2\left(2\kappa_{m'-1} P + \kappa_{m'-2} P \right) + \kappa_{m'-3} P \right] \cdots + \cdots + \kappa_1 P \right] + \kappa_0 P \tag{18}$$

In equations (17)–(18), $\kappa_i \in \{0, 1\}$, and $\kappa_{m'-1} \neq 0$. According to the above formula, using the binary expansion method to calculate the scalar multiplication κP of the sensitive data on ellipse curve needs a total of $m - 1$ times double point operation and $m/2$ doubling operation.

The encryption of sensitive data on the elliptic curve usually requires that the plaintext be encoded on the elliptic curve points. It needs to decrypt the points on the elliptic curve into plaintext when we decrypt sensitive data. For the elliptic curve E on the finite data domain $GF(q')$ of the sensitive data in accounting information processing system, supposing $q' = p^{n'}$, $n' = 2n'$, the plaintext in the accounting information processing system is an integer u, and $0 \le u \le p^{n'}$, the plaintext in the accounting information processing system is expressed as an integer u.

$$u = u_0 + u_1 p + \cdots + u_{n'-1} p^{n'-1} \tag{19}$$

Assuming that $b_0, \cdots, b_{n'-1}$ represents the vector space base of a finite field $GF(p^{n'})$ on the finite data domain $GF(p')$ of sensitive data in the information processing system, and its definition is described as equation (20).

$$x(u) = u_0 b_0 + u_1 b_1 + \cdots + u_{n'-1} b_{n'-1} \tag{20}$$

The vector space base $x(u)$ of the sensitive data in the accounting information processing system is substituted into the equation (14), $y(u)$ is obtained and $y(u) \in GF(q')$, then the point $P_u(x(u), y(u))$ is any point on the elliptic curve E, so that the plaintext u in the accounting information processing system is encoded into a point P_u on the elliptic curve. The following are two encryption methods.

2.2.1 Encryption method 1

A random number l ($l < \upsilon$, υ is the order of sensitive data base point G in the accounting information processing system) is selected as the private key of sensitive data encryption in accounting information processing system, then the public key calculation formula of sensitive data encryption in accounting information processing system is defined as equation (21).

$$K = \upsilon G \tag{21}$$

As the public key of sensitive data encryption in the accounting information processing system, the plaintext u is encoded to a point P_u on the elliptic curve E and a random number γ is selected to calculate C_1 and C_2.

$$C_1 = \gamma G \tag{22}$$

$$C_2 = \gamma K + P_u \tag{23}$$

where (C_1, C_2) represents the ciphertext obtained after the sensitive data is encrypted in the accounting information processing system. In decryption, the private key K of sensitive data encryption is used to decrypt the ciphertext (C_1, C_2), the calculation expression is defined as equation (24).

$$C = \upsilon C_1 \tag{24}$$

According to equation (22) and equation (25) can be obtained.

$$uG_1 = u(\gamma G) = \gamma K \tag{25}$$

Further calculations are available in equation (26).

$$C_2 - C = \gamma K + P_u - \gamma K = P_u \tag{26}$$

According to equation (26), the plaintext u of the sensitive data in the accounting information processing system can be obtained by decoding P_u.

2.2.2 Encryption method 2

C_1 is calculated using equation (22),

$$C_2 = \gamma K \tag{27}$$

$$C_3 = uC_2 \tag{28}$$

In the above formula, (C_1, C_3) represents the ciphertext obtained after the sensitive data is encrypted in the accounting information processing system; the secret key K is used when decrypting the ciphertext (C_1, C_3) obtained after the sensitive data is encrypted in the accounting information processing system. The expression is defined by equations (29)–(30).

$$\upsilon C_1 = \upsilon(\gamma G) = \gamma K = C_2 \tag{29}$$

$$C_3 C_2^{-1} = u \tag{30}$$

According to the calculation of equations (29)–(30), the plaintext message u after the sensitive data is decrypted in the accounting information processing system is obtained.

2.3 Homomorphic encryption method of sensitive data in accounting information processing systems

Based on the elliptic curve encryption mechanism, the additive and multiplicative homomorphic encryption methods of sensitive data in the accounting information processing system are constructed respectively. The detailed description steps are as follows.

Assuming that $(G', *)$ and $(G', \circ)$ represent two algebraic systems of sensitive data in the accounting information processing system; f: $G' \to H$ is a mapping of sensitive data in the accounting information processing system; if $\forall a', b' \in G$, then equation (31) is obtained.

$$f(a' * b') = f(a')^{\circ} f(b') \tag{31}$$

In equation (31), f represents a homomorphic mapping from G' to H.

Assuming that $E'(K', x')$ represent the use of the encryption method E' and the key K' to encrypt the sensitive data x' in the accounting information processing system. F represents an operation that if there is an effective method G' for the encryption method E' and the operation F, equation (32) is obtained.

$$E'\left(K', F\left(x_1', \cdots, x_0'\right)\right) = G'\left(K', F\left(E'\left(x_1'\right), \cdots, E'\left(x_n'\right)\right)\right) \tag{32}$$

The encryption method E' is said to have homology for the operation F.

Assuming that the encryption function of the sensitive data in the accounting information processing system is expressed as E_K'; the decryption function of the sensitive data in the accounting information processing system is expressed as D_K'; the plaintext data in the accounting information processing system is expressed as (u_1, u_2, ··, u_n), then the sensitive data of the formulas for addition homomorphic encryption and multiplication homomorphic encryption in the accounting information processing system are defined as equations (33)–(34).

$$\sum_{i=1}^{n} u_i = u_1 + u_2 + \cdots + u_n = D_K'\left(E_K'\left(u_1\right) + E_K'\left(u_2\right) + \cdots + E_K'\left(u_n\right)\right) \tag{33}$$

$$\prod_{i=1}^{n} u_i = u_1 \cdot u_2 \cdots u_n = D_K'\left(E_K'\left(u_1\right) \cdot E_K'\left(u_2\right) \cdots E_K'\left(u_n\right)\right) \tag{34}$$

1 Additive homomorphic encryption method for sensitive data in accounting information processing system

The plaintext data u_i in the accounting information processing system is embedded in a point P_{u_i} on the elliptic curve E, and the decrypted private key x_i' is used to calculate C_{2_i} according to the above equations (22)–(26) to obtain the i^{th} sensitive data in the accounting information processing system The sensitive data (C_{1_i}, C_{2_i}) in the accounting information processing system is encrypted by the

addition calculation to obtain the $\left(\sum_{i=1}^{n} C_{1_i}, \sum_{i=1}^{n} C_{2_i}\right)$, which is described as equations (35)–(36).

$$\sum_{i=1}^{n} C_{1_i} = C_{1_1} + C_{1_2} + \cdots + C_{1_n} \tag{35}$$

$$\sum_{i=1}^{n} C_{2_i} = C_{2_1} + C_{2_2} + \cdots + C_{2_n} \tag{36}$$

According to the calculation results of equations (29)–(30), the private key K of the sensitive data in the accounting information processing system is used according to equation (29). Therefore, equation (37) is obtained.

$$\sum_{i=1}^{n} C_{1_i} - K\sum_{i=1}^{n} C_{2_i} = \sum_{i=1}^{n} P_{u_i} + Q\sum_{i=1}^{n} x_1' - KP\sum_{i=1}^{n} x' = \sum_{i=1}^{n} P_{u_i} \tag{37}$$

The sensitive data $\sum_{i=1}^{n} P_{u_i}$ in the accounting information processing system of the above equation (37) is decoded to obtain plaintext data.

$$\sum_{i=1}^{n} P_{u_i} = u_1 + u_2 + \cdots + u_n \tag{38}$$

2 Multiplication homomorphic encryption of sensitive data in accounting information processing system

The plaintext data u_i after decrypting the sensitive data in the accounting information processing system is calculated to obtain C_{2_i}, C_{3_i} and C_{4_i} according to equations (36)–(38), respectively.

$$C_{2_i} = x_i' P \tag{39}$$

$$C_{3_i} = P_{u_i} C_{4_i} \tag{40}$$

$$C_{4_i} = x_i' Q \tag{41}$$

According to the above calculation, the encrypted ciphertext data (C_{2_i}, C_{3_i}) of the sensitive data in the accounting information processing system is obtained, and the ciphertext data $\left(\prod_{i=1}^{n} C_{2_i}, \prod_{i=1}^{n} C_{3_i}\right)$ is obtained by multiplying all the encrypted sensitive data $(C_{2_i}, C_{3_i}) \cdots (C_{2_n}, C_{3_n})$ in the accounting information processing system, which is described as equations (42)–(43).

$$\prod_{i=1}^{n} C_{2_i} = C_{2_1} \cdot C_{2_2} \cdots C_{2_n} \tag{42}$$

$$\prod_{i=1}^{n} C_{3_i} = C_{3_1} \cdot C_{3_2} \cdots C_{3_n} \tag{43}$$

According to equation (26), the secret key K is used to obtain equation (44).

$$K^n \cdot C_{2_1} \cdot C_{2_2} \cdots C_{2_n} = K^n \prod_{i=1}^{n} C_{2_i} \tag{44}$$

It is easy to prove equation (45).

$$\begin{aligned} K^n \prod_{i=1}^{n} C_{2_i} &= K^n \cdot C_{2_1} \cdot C_{2_2} \cdots C_{2_n} = K^n P^n x_1' \cdot x_2' \cdots x_n' \\ &= Q^n \prod_{i=1}^{n} x_i = C_{4_1} \cdot C_{4_2} \cdots C_{4_n} = \prod_{i=1}^{n} C_{4_i} \end{aligned} \tag{45}$$

According to equation (27), it is available for equation (46).

$$\begin{aligned} \prod_{i=1}^{n} C_{3_i} \cdot \prod_{i=1}^{n} C_{4_i}^{-1} &= P_{u_1} C_{4_1} \cdot P_{u_2} C_{4_2} \cdots P_{u_n} C_{4_n} \cdot C_{4_1}^{-1} \cdot C_{4_2}^{-1} \cdots C_{4_n}^{-1} \\ &= P_{u_1} \cdot P_{u_2} \cdots P_{u_n} = \prod_{i=1}^{n} P_{u_i} \end{aligned} \tag{46}$$

The sensitive data $\prod_{i=1}^{n} P_{u_i}$ in equation (46) is decoded to obtain plaintext data.

$$\sum_{i=1}^{n} u_i = u_1 \cdot u_2 \cdots u_n \tag{47}$$

By using the homomorphic encryption method described above, when the user encrypts the sensitive data in the accounting information processing system, the ciphertext in the accounting information processing system can be added and deleted to avoid the copied and tampered danger of the sensitive data in the accounting information processing system in the transmission process, so that the security of sensitive data encryption in the accounting information processing system has been greatly improved.

3 Experimental results and analysis

The experimental environment is Intel (R) Core (TM) i7, clock speed of CPU is 3.6 GHz, memory is 8 GB, operating system is Windows8, and development language is C++. The dataset used in the experiment is based on the accounting information processing system of an accounting firm, and 3,200 sensitive data are randomly selected, including 1,600 encrypted ciphertext data and 1,600 decrypted plaintext data. And different encryption methods are made experimental analysis.

The security performance of the sensitive data encryption method in the accounting information processing system is usually reflected by the anti-attack strength of the

method. In addition, the measure of the validity of the sensitive data encryption method in the accounting information processing system is also the calculation, the storage space and the bandwidth requirement. Using the method proposed by Li et al. (2016), Yang et al. (2015), Wu et al. (2016) and the proposed method, the above indicators are compared and analysed, the results are as Table 1.

Table 1 Comparison of the encryption performance of different methods

Method	*Safety*	*The amount of calculation*	*Occupied storage space*	*Bandwidth requirements*
Method proposed by Li et al. (2016)	General	More	More	More
Method proposed by Yang et al. (2015)	Preferably	General	General	Less
Method proposed by Wu et al. (2016)	Poor	More	More	More
The proposed method	Preferably	Preferably	Less	Less

According to the analysis of Table 1, we can see that the anti-attack performance of the proposed method has the absolute superiority and the encryption security performance is better. The anti-attack strength of the method proposed by Li et al. (2016) is poor, and the security performance is generally the same. Both the amount of computation and the storage space occupied by using the method proposed by Li et al. (2016) are larger, and the required network bandwidth is also larger; the security performance of the method proposed by Yang et al. (2015) is better, the required network bandwidth is smaller, but the calculation and storage space are large; the anti-attack performance of the method proposed by Wu et al. (2016) is poor, the required network bandwidth, the amount of computation and the storage space are larger; the encryption method mentioned in this paper only needs to take up a small storage space and network bandwidth requirements, and has a good advantage.

The encryption time and decryption time are two important indexes to measure the validity of the sensitive data encryption method in accounting information processing system.

The encryption time is the time required for the sensitive data to become ciphertext data in the accounting information processing system. The encryption time (s) of the encryption method proposed by Li et al. (2016) and Yang et al. (2015) and this paper are compared, and the comparison result is shown in Figure 1.

It can be seen from Figure 1 that with the increasing number of sensitive data in the accounting information processing system, the encryption time of all encryption methods is correspondingly increased. However, in the same situation, the encryption operation time of the proposed encryption method is relatively less, and the increase of encryption time is relatively stable. The encryption time of the method proposed by Li et al. (2016) and Yang et al. (2015) increases greatly and the change is more intense. Through the comparative analysis, the proposed encryption method adopts less computational cost and gets a better encryption effect to meet the real-time and online requirements of sensitive data encryption in accounting information processing system with good practicality.

Decryption time is the time required for decrypting the sensitive data in the accounting information processing system into ciphertext data. In order to further prove the effectiveness of the proposed method, the decryption time of the method proposed by

Li et al. (2016) and Wu et al. (2016) are compared with the proposed method. Experimental results are shown in Figure 2.

Figure 1 Comparison of encryption time of different methods (see online version for colours)

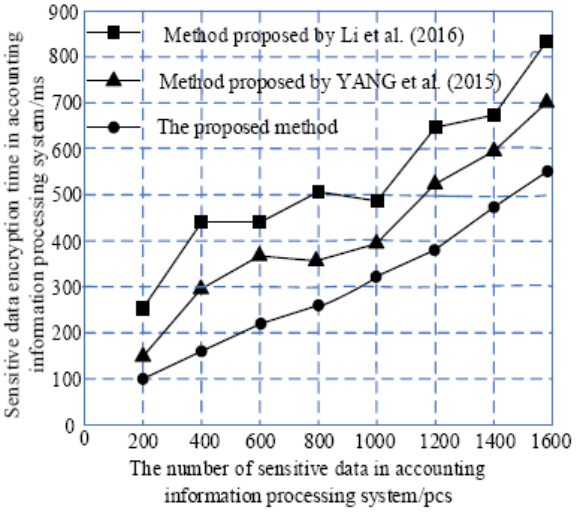
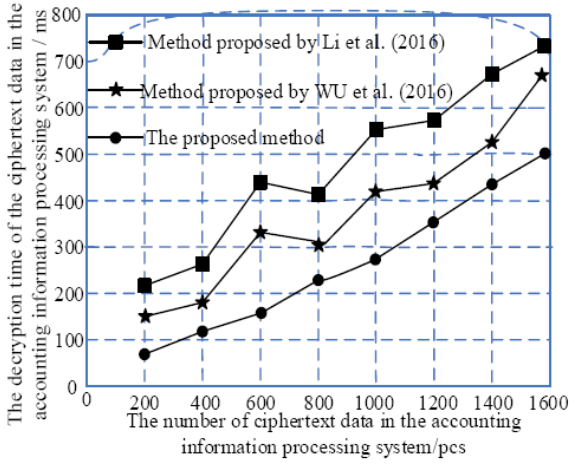


Figure 2 Comparison of decryption time of different methods (see online version for colours)



According to Figure 2, it can be seen that when the number of ciphertext data in the accounting information processing system is small, the proposed method does not take too many advantages, but with the increase of the number of ciphertext data in the accounting information processing system, the superiority of the proposed method is gradually appeared. Under the same conditions, the computational cost increase of the proposed method is smaller than that of the method proposed by Li et al. (2016) and Wu et al. (2016). Experimental results show that the proposed method is effective and is superior to the other methods.

4 Conclusions

When the current encryption method was used to encrypt the sensitive data in the accounting information processing system, the security was poor and it was easy to cause the problem of sensitive data leakage. To this end, a hybrid encryption method for sensitive data in the accounting information processing system was proposed. Experimental results showed that encryption effect obtained by our proposed method was ideal. Detailedly, compared with traditional methods, encryption and decryption run time obtained by our proposed method were the shortest. It was proved that this method not only had good encryption effect, but also consumes the memory occupied and bandwidth requirements were less, which can prevent the sensitive data leakage in the accounting information processing system, and had wide application prospect. Therefore, it had a wide range of application prospects. In the future, we intend to further shorten the time for encrypting sensitive data and increase the efficiency of sensitive data encryption operations to a greater extent.

Acknowledgements

This work is supported by the programs of Henan soft science research project (Nos: 172400410618) and university financial service company internal control problem, countermeasure research results of the project of Henan soft science research project (Nos: 182400410630).

References

Abdulgader, A., Ismail, M. and Zainal, N. (2015) 'Improve the performance of MPEG video encryption algorithm using modified RC4 algorithm based on chaotic map', *Breast Cancer Research*, Vol. 75, No. 1, pp.159–167.

Gong, L.H., He, X.T. and Cheng, S. (2016) 'Quantum image encryption algorithm based on quantum image XOR operations', *International Journal of Theoretical Physics*, Vol. 55, No. 7, pp.3234–3250.

Hua, T., Chen, J. and Pei, D. (2015) 'Quantum image encryption algorithm based on image correlation decomposition', *International Journal of Theoretical Physics*, Vol. 54, No. 2, pp.526–537.

Jia, B., Liu, S. and Yang, Y. (2014) 'Fractal cross-layer service with integration and interaction in internet of things', *International Journal of Distributed Sensor Networks*, Vol. 10, No. 3, p.760248.

Li, T., Wang, Y. and Huang, R. (2016) 'Research on the encryption algorithm supporting multiuser fuzzy retrieval in the cloud computing', *Journal of Chinese Computer Systems*, Vol. 37, No. 10, pp.2244–2248.

Liang, Z. (2016) 'A kind of enterprise core information leakproof data encryption method improvement', *Science Technology and Engineering*, Vol. 16, No. 27, pp.204–208.

Liu, S., Fu, W. and Deng, H. (2013a) 'Distributional fractal creating algorithm in parallel environment', *International Journal of Distributed Sensor Networks*, Vol. 9, No. 9, p.281707.

Liu, S., Fu, W. and Zhao, W. (2013b) 'A novel fusion method by static and moving facial capture', *Mathematical Problems in Engineering*, No. 5, pp.497–504.

Lu, Y., Wang, S. and Chen, L. (2016) 'Research of mixed encryption algorithm based on cloud storage', *Computer Measurement & Control*, Vol. 24, No. 3, pp.129–132.

Pan, Q. (2015) 'A double thread complementary information encryption algorithm based on random amplitude modulation', *Bulletin of Science and Technology*, Vol. 31, No. 12, pp.144–146.

Seyedzadeh, S.M., Norouzi, B. and Mosavi, M.R. (2015) 'A novel color image encryption algorithm based on spatial permutation and quantum chaotic map', *Nonlinear Dynamics*, Vol. 81, Nos. 1–2, pp.511–529.

Tong, X.J., Wang, Z. and Zhang, M. (2015) 'An image encryption algorithm based on the perturbed high-dimensional chaotic map', *Nonlinear Dynamics*, Vol. 80, No. 3, pp.1493–1508.

Wang, X. and Zhang, H.L. (2016) 'A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems', *Nonlinear Dynamics*, Vol. 83, Nos. 1–2, pp.333–346.

Wu, Y., He, F. and Zhang, D. (2016) 'Partial deformation encryption method for CAD model in collaborative design', *Journal of Computer-Aided Design & Computer Graphics*, Vol. 28, No. 10, pp.1767–1778.

Yang, G. and Liu, S. (2014) 'Distributed cooperative algorithm for k-M set with negative integer k by fractal symmetrical property', *International Journal of Distributed Sensor Networks*, Vol. 10, No. 5, p.398583.

Yang, P., Gui, X., Yao, J., Lin, J., Tian, F. and Zhang, X. (2015) 'Research on algorithms of data encryption scheme that supports homomorphic arithmetical operations', *Journal on Communications*, Vol. 36, No. 1, pp.167–178.

Yao, W., Zhang, X. and Zheng, Z. (2015) 'A colour image encryption algorithm using 4-pixel Feistel structure and multiple chaotic systems', *Nonlinear Dynamics*, Vol. 81, Nos. 1–2, pp.1–18.

Yuan, H. and Li, J. (2015) 'Simulation on encryption algorithm for communication under public key cryptosystems', *Computer Simulation*, Vol. 32, No. 3, pp.331–334.

Zhan, F. and Zhang, S. (2017) 'Research on hybrid encryption DAES algorithm based on cloud computing', *Electronic Design Engineering*, Vol. 25, No. 3, pp.185–189.

Zhu, L., Tang, X. and Shen, M. (2018) 'Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks', *IEEE Journal on Selected Areas in Communications*, Vol. 36, No. 3, pp.628–643.