Research Article

Lijie Yin* and Nasruddin Hassan

# Multi-level encryption algorithm for user-related information across social networks

https://doi.org/10.1515/phys-2018-0120
Received Oct 03, 2018; accepted Nov 14, 2018

**Abstract:** The traditional RSA information encryption algorithm uses one-dimensional chaotic equations to generate pseudo-random sequences that meet the encryption requirements. This encryption method is too simple and the security performance is poor. A multi-level encryption algorithm for user-related information across social networks is proposed, and a user association model across social networks is constructed to obtain user-related information across social networks. This multi-level chaotic encryption algorithm based on neural network is used to select three different chaotic mapping models based on user-related information, and a multi-level chaotic encryption algorithm is designed. According to the characteristics of error sensitivity of chaotic system, the neural network is used to inversely propagate the error. A chaotic encryption algorithm that implements multi-level encryption of user-related information across social networks is optimized. The experimental results show that the average rate for which the proposed algorithm correctly identified the user-related information across social networks was 97.6%, the highest frequency of average character distribution probability in cipher text was 0.021, and the average time for encryption was 18.45 Mbps. The average time for decryption was 21.90Mbps.

**Keywords:** Across social network, user-related information, multi-level encryption, chaotic mapping model, neural network, inverse propagation

**PACS:** 07.05.Mh, 89.20.Ff, 05.45.Pq

## 1 Introduction

With the rapid development of Internet technology, the Internet has become popular on a large scale. As of the end of December 2015, the number of Internet users in China reached 688 million and the Internet penetration rate was 50.3%. The Internet ushered in the Web 2.0 era. Along with the advent of the Web 2.0 era, a large number of excellent Internet products based on the UGC (User Generated Content) model were born, the fastest growing of which was the Online Social Network application [1]. According to statistics, the number of Chinese netizens using social networking sites, Weibo and various vertical social applications reached 530 million, and the usage rate of QQ space and Weibo was 65.1% and 33.5%, respectively. When studying the behavior of users on different social networking sites, there is a challenge: the inability to efficiently encrypt information associated with users across social networks [2]. A user has individual social accounts on different social networks and the behavior on these social networks may be different. It is impossible to effectively identify whether the accounts are from the same user. Thus the user-related information across social networks cannot be further encrypted and can easily be disclosed, which brings inconvenience and harm to the social network users. The identification and encryption of the user-related information across social networks is the key to solving these problems.

At present, there are few association studies for domestic social networking users. Li Xia *et al.* proposed a user recognition model of subjective vector-driven objective weights based on the similarity weight method [3]. Haw LK *et al.* proposed a two-stage associated entity recognition model and an incremental verification algorithm based on the pattern characteristics and attribute characteristics of the users [4]. This method can be applied to user identification across social networks. Chaos is a seemingly irregular movement; a random process that occurs in deterministic systems. Due to the complex pseudo-randomness exhibited bya chaotic system and its extreme sensitivity to initial values, it can be used for encryption. In recent years, this application of the chaotic principle has

***Corresponding Author: Lijie Yin:** School of Information Engineering, Hebei Geo University, Shijiazhuang, 050031, China; Email: yinxzy@126.com
**Nasruddin Hassan:** School of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia UKM Bangi, Selangor, Malaysia; Email: nas@ukm.edu.my

received more and more attention and many scholars are studying it and applying it to image encryption, voice encryption and many other aspects.

Wang *et al.* used a simple one-dimensional chaotic equation to generate a pseudo-random sequence that satisfies the encryption requirements [5]. This encryption method was too simple and the encryption effect (security performance) was poor. A traditional chaotic synchronization scheme was used to realize the secure communication of digital signals [6]. Parpas group proposed that on the basis of real values [7] the symbol matrix and permutation matrix were generated by discrete mapping. The digital image was encrypted, and the two encryption methods respectively encrypted the communication of the digital signal and the digital image, and the limitation was high. Lai *et al.* proposed a symmetric encryption scheme based on a chaotic iterative system [8], which required inter-node communication for each iteration, and the efficiency was low. Other than those, two synchronous sequence cryptographic algorithms based on composite discrete chaotic systems have been created [9]. Encryption and decryption were the same iterative process of a composite discrete chaotic system. The algorithm has fewer types of operations. It does not support operations of any number, and its homomorphism was poor.

Aiming at the problems in previous studies, a multi-level encryption algorithm for user-related information across social networks is proposed. The user association model across social networks is used to determine whether different social network accounts are from the same user. After obtaining the corresponding information, the third-level chaotic encryption algorithm is used to encrypt social network user-related information. On this basis, the neural network is used to improve the multi-level chaotic encryption algorithm, so that the error is transmitted in reverse, and the security of the chaotic algorithm is improved.

# 2 Multi-level encryption algorithm for user-related information across social networks

The multi-level encryption algorithm for user-related information across social networks obtains the user-related information through the cross-social network user association model and then uses neural network-based multi-level chaotic encryption algorithm based on the association information to realize multi-level encryption of user-related information across social networks.

## 2.1 Construction of the cross-social network user association model

The candidate user set selected according to the seed data set [10] is utilized to restore the social relationship. First the algorithm calculates the similarity between the fields of the corresponding user pairs in the Weibo and QQ and combines the similarities between the fields as the similarity feature vector as follows:

$$\vec{S} = \langle V_0 V_1 V_2 V_3 V_4 V_5 V_6 V_7 V_8 V_9 \rangle \tag{1}$$

In formula (1), $V_0$ represents the similarity of the user nickname, $V_1$ represents the similarity of the user's gender, and the different dimensions represent the similarity between the different attributes.

When confirming the user across social networks, the confirmation of classification is regarded as a two-category problem; that is, the confirmation of the same entity user and the different entity user is a two-category problem.

The logistic regression model is a commonly used classification model [11]. The most commonly used logistic regression is binomial logistic regression. There are only two types of the classification. Therefore, this paper uses the logistic regression model to confirm the association information of social network users. For classification, the results are positive (represented by 1) and negative (represented by 0), and the conditional probability of binomial logistic regression is:

$$P(Y = 1\,|x, w) = \frac{e^{w^T x+b}}{1 + e^{w^T x+b}} = \frac{1}{1 + e^{-(w^T x+b)}} \tag{2}$$

$$P(Y = 0\,|x, w) = \frac{1}{1 + e^{w^T x+b}} \tag{3}$$

In formula (2) and (3), $xR^n$ is an input representing the characteristics of the instance; $Y\{0, 1\}$ is the output with only two types, simply represented as yes or no. $xR^n$ and $PR$ represent parameters, where the weight vector is represented by $w$, the corresponding value representing the weight of the input feature, and $b$ representing the offset. At the time of classification, according to the input example, formula (2) and formula (3), $P(Y = 1x, w)$ and $P(Y = 0x, w)$ can be obtained separately, the two conditional probabilities are compared by logistic regression, and the input instance is divided into the type of relatively large probability values.

The classification model flow is shown in Figure 1.

To use the model for the prediction of classifications, it is necessary to train the model first, obtain the feature weight parameter, and then calculate the input feature

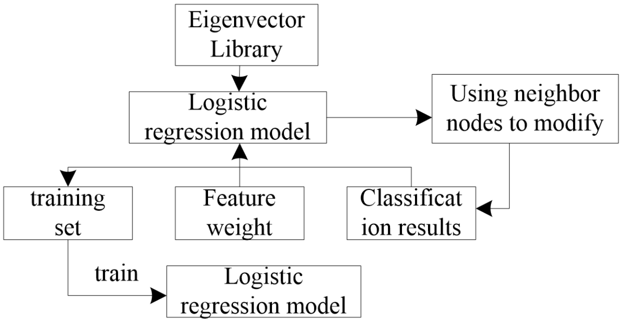
Eigenvector Library
Logistic regression model
Using neighbor nodes to modify
training set
Feature weight
Classificat ion results
train
Logistic regression model

**Figure 1:** Classification model process

vector according to the feature weight, and compare and judge according to the calculated result and the classification threshold. When the result of the logistic regression calculation is greater than the threshold, the result is positive, indicating that the users of the two social network platforms belong to the same entity user; otherwise, the result is negative, indicating that they are not directed to the same entity user.

Through this cross-social network user association model, it is possible to determine whether different social network accounts are from the same entity user, and then obtain user-related information across social networks. On the basis of this, a multi-level chaotic encryption algorithm based on neural networks is used to realize multi-level encryption processing of user-related information across social networks.

## 2.2 Multi-level chaotic encryption algorithm based on neural network

Based on the user association information obtained in the previous section, three different chaotic mapping models are selected to design a multi-level chaotic encryption algorithm. The neural network is used to improve the multi-level chaotic encryption algorithm to achieve multi-level encryption of user-related information across social networks.

### 2.2.1 Chaotic Mapping Model

Chaotic mapping model 1: A hybrid optical bistable model is selected [12] and its iterative equation is:

$$X_{n+1} = A^{*}Sin^{2}\left(X_n - X_b\right) \tag{4}$$

In equation (4), $X_n$ and $X_b$ represent user-related information across social networks at time n and b, and A is used to describe chaotic correlation between information. When $A = 6$ and $X_b = 3$, the model is known to be in a chaotic state. In the proposed multi-level encryption algorithm, the model is used to generate a permutation matrix to replace the input plaintext.

Chaotic mapping model 2: A piecewise linear chaotic mapping model is utilized [13]:

$$X_{n+1} = \begin{cases} X_n/p & X_n \in [0, p] \\ (1 - X_n)/(1 - p) & X_n \in [p, 1] \end{cases} \tag{5}$$

In equation (5), $p$ represents the piecewise linearity of the information. When $0 < p < 1$, the Lyapunov exponent of the model is positive and in a chaotic state. In the proposed multi-level encryption algorithm, the model acts as the first-order chaotic system for generating the key stream, and uses it to determine the number of iterations of the next-order chaotic system (the second-order chaotic system that generates the key stream).

Chaotic mapping model 3: The chaotic mapping model adopts the most widely used logistic mapping model [15]:

$$X_{n+1} = \mu X_n \left(1 - X_n\right) \tag{6}$$

In equation (6), $\mu$ represents the Lyapunov exponent of the information. When the map is $3.5699456 < \mu < 4$, its Lyapunov exponent is positive and in a chaotic state. In the proposed multi-level encryption algorithm, the model is used to generate the final key stream; the second-order chaotic system that generates the key stream mentioned above.

### 2.2.2 Design of multi-level chaotic encryption algorithm

#### Implementation steps of algorithm

The multi-level encryption algorithm for user-related information across social networks proposed in this paper combines the above three chaotic models. The initial values and parameters of each chaotic model (a total of 7) can be used as keys. However, in order to ensure that the designed algorithm is in chaos [15], the parameter $A = 6$ $X_b = 3$ in the hybrid optical bistability model is defined, and the remaining four values of the parameter $\mu = 4$ in the logistic mapping are defined as the initial key of the algorithm and entered by the user. So the initial key is a 4-tuple: $Key = (X, P, Y, Z)$. Among them:

X: initial value of model I, requires $0 < X < A$
P: initial value of model II, requires $0 < P < 1$
Y: initial value of model II, requires $0 < Y < 1$
Z: initial value of model III, requires $0 < Z < 1$

The multi-level chaotic encryption algorithm is described as follows:
First, enter the key $Key\,(X, P, Y, Z)$.
Second, open the file and take out 2 characters (or a Chinese character) for a total of 16 bits, and then feed into the variable $C_1$, $C_2$.
Third, the 16-bit information is expanded to 32 bits by sequentially inserting a binary digit 1, 0 between adjacent two bits.
Fourth, iterate 32 times according to the input key X and the chaotic model 1, and 32 values are obtained. These 32 values are respectively taken to the remainder of 32, and the same remainder is processed to ensure that 32 different results are obtained, which are sequentially stored in the array$P$ in the order of generation.
Fifth, the 32-bit data generated in the third step is replaced according to the array $P$ [16].
Sixth, according to the input key $P$, $Y$ and chaotic model 2, the $Y_{n+1}$ is obtained through iteration. Since the value of $Y_{n+1}$ is in [0, 1], this range is equally divided, and $Y_{n+1}$ is quantized into an integer $K$ accordingly. The algorithm in this paper is quantized into 10 levels, that is, $K$ is an integer between 1 and 10.
Seventh, according to the input key $Z$, the chaotic model 3 is iterated $K$times to generate the encrypted key $Key_1$.
Eighth, the 32-bit information after the fifth is replaced with $Key_1$ to generate the ciphertext $C$.
Ninth, the 32-bit ciphertext $C$ is processed into 4 character outputs. The next 2 characters are read until the end of the file.

The input of this encryption algorithm is 16 bits and the output is 32 bits. The 16-bit plaintext is extended, replaced, and then interacted with the key stream $Key_1$ to generate ciphertext. The original key entered is 4 real numbers; one is used to generate the permutation matrix and the other 3 are generated by the level 2 chaotic system to produce the key stream $Key_1$.

#### Discussion of algorithm

The multi-level chaotic encryption algorithm proposed in this paper is designed in C language [17] and the specific implementation of the algorithm is discussed as follows:
First of all, in the fourth step of the algorithm design, the chaotic model 1 is iterated 32 times to obtain 32 values. In order to obtain better pseudo-randomness [18], the values from the initial iterations should be discarded and the iteration values from the first $k + 1$ to the $k + 32$ times are chosen. The iteration of chaotic model 2 in step 6 should also be the same.
Then, in the fourth step of the algorithm, the 32 numbers obtained are used for the remainder operation. When the result of the remainder of 32 is the same, the linear detection method is adopted; that is, the remainder is incremented by 1. If the number obtained is not the same, it is stored in the array, otherwise it is incremented by 1 (when it is full, it will be 0 again).
At last, the key $Key_1$ obtained in step 7 of the algorithm; because $0 < Key_1 < 1$, $Key_1$ will be XORed with a 32-bit number in the eighth step. The data type of $Key_1$ is float. In order to ensure that the binary code circumference of the long type is as large as possible, it should be transformed: $Key_1 = Key_1 * 1000000000$.

### 2.2.3 Improving multi-level encryption algorithm with neural network

The core of the above multi-level chaotic encryption algorithm lies in the key stream generated by the chaotic mapping model 2 and the model 3. According to Shannon's theory, a one-time pad is a truly safe system [19]. However, due to the limitation of computer precision, it is difficult to achieve a one-time pad using a chaotic system. Gong *et al.* pointed out that communication systems based on low-dimensional chaos are vulnerable to adaptive synchronization control and do not have high confidentiality [20–26]. However, the hyperchaotic system is quite complicated in iterative calculation and implementation details, which makes greatly reduced the efficiency of the algorithm. Therefore, according to the error sensitivity of the chaotic system between the encryptor and the decryptor, the neural network is used to improve the multi-level chaotic encryption algorithm such that the error is reversely transmitted and the security of the chaotic system is improved. Accurate encryption of information associated with users across social networks.

#### Neural network model

In this paper, the BP algorithm in the neural network is used to realize the learning and generation of chaotic sequences. If one selects $n$ inputs: $X_{K+1}, X_{K+2}, \cdots, X_{K+n}$, their corresponding weights are: $V_1, V_2, \cdots, V_n$. Each time $m$ steps are predicted, $m$ values are output: $X_{K+n+1}, X_{K+n+2}, \cdots, X_{K+n+m}$. The predicted value is $X_{k+n+j} = f\left(\sum_i x_i v_i - \theta_i\right)$ $(i = 1, 2, \cdots, n; j = 1, 2, \cdots, m)$. And $X_{K+1}, X_{K+2}, \cdots, X_{K+m}\,(m <= n)$ is replaced with $X_{K+n+1}, X_{K+n+2}, \cdots, X_{K+n+m}$ at the iteration, along with

$X_{k+m+1}, \cdots, X_{k+n}$ as the second input to predict the new $m$ values, and iterate again. This is a neural network with a feedback structure, as shown in Figure 2.

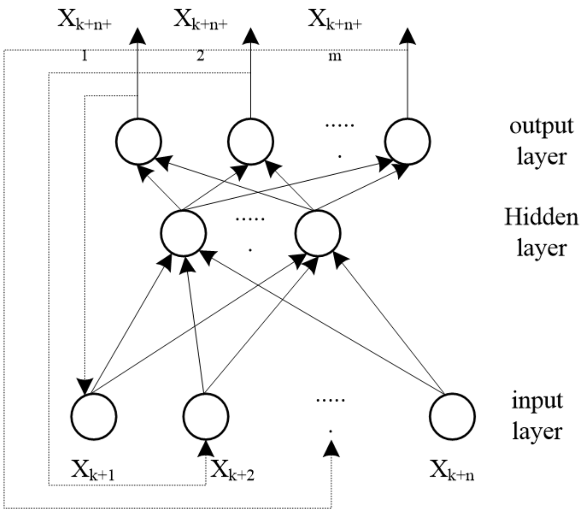

**Figure 2:** Neural network structure diagram

**Improved algorithm of neural network model**

The neural network model of the above structure is applied to the chaotic mapping model 3, Logistic chaotic model, in the algorithm of this paper, which is used to assist the Logistic model to generate the key stream. The original key $Z$ entered generates $Z_1, Z_2, \cdots, Z_n$ after $n$ iterations. Using these $n$ values as the first input, $Z_{n+1}, \cdots, Z_{n+m}$ is generated by the hidden layer calculation, and they are looped back to the input layer. The second time, $Z_{m+1}, \cdots, Z_n$, $Z_{n+1}, \cdots, Z_{n+m}$is used as input to generate a new round of $m$ outputs. In this cycle, the neural network is used to cycle $K$ rounds ($K$ is the result of the chaotic mapping model 2).

In the neural network of the algorithm, there are$n$ inputs of each neuron: $X_{k+1}, X_{k+2}, X_{k+n}$, whose weights are $1, 2, \cdots, n$, respectively. That is, each time the neural network pushes forward, the corresponding weight of the input $X_i$ is decremented by 1 until it is 0. In the specific implementation of the algorithm, the ratio of the number of neurons in the input layer, the hidden layer, and the output layer is 5:1:2.

At this time, the complete structure of the multi-level chaotic encryption algorithm based on neural network is shown in Figure 3.

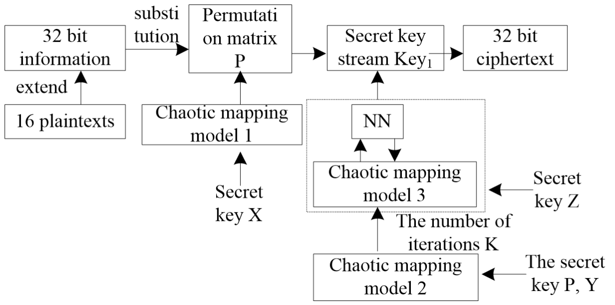

**Figure 3:** A complete multi-level chaotic encryption algorithm based on a neural network

# 3 Results

## 3.1 Accuracy of user information recognition across social networks

In order to evaluate the multi-level encryption algorithm of social network user association information proposed in this paper, the information of 1000 different social network users is randomly divided into 10 groups. Each group is different, and the algorithm is used for determination of the related information. According to the information to identify the exact number of people, and obtain the identification accuracy of the related information of different groups, the results are shown in Table 1.

**Table 1:** Information distribution accuracy rate of cross social network users

| Group number | Number of groups / groups | Identifying the exact number of people / people | Accuracy rate /% |
|---|---|---|---|
| 1 | 107 | 104 | 97.2 |
| 2 | 96 | 94 | 97.9 |
| 3 | 98 | 97 | 99.0 |
| 4 | 122 | 118 | 96.7 |
| 5 | 89 | 86 | 96.6 |
| 6 | 106 | 103 | 97.1 |
| 7 | 92 | 89 | 96.7 |
| 8 | 96 | 95 | 99.0 |
| 9 | 110 | 108 | 98.2 |
| 10 | 84 | 83 | 98.8 |
| Average accuracy | | | 97.6 |

Analysis of Table 1 shows that the lowest accuracy of information related to 1000 cross-social network users using the algorithm is 96.6%, the highest is 99.0%, and the average accuracy is 97.6%.

## 3.2 Validity of the proposed algorithm

The algorithm is used to test the above plaintext 1, and the probability statistics are obtained, as shown in Figure 4 and Figure 5. The plaintext 2 is tested, and the probability statistics before and after the encryption are obtained as shown in Figure 6 and Figure 7. In the figures, the abscissa indicates the code value of the ACSII code, and the ordinate indicates the frequency at which the corresponding code value appears.

Figure 4 and Figure 5 shows that the highest frequency in plaintext 1 is 0.118, after encryption, the probability distribution of characters in the ciphertext is averaged, the highest frequency is only 0.021. Therefore, it can be considered that plaintext 1 is randomly spread into the entire ciphertext, and no plaintext information is retained in the ciphertext. In Figure 6 and Figure 7, the four characters that appear consecutively are encrypted, the frequency is spread, and the highest appearance frequency of ciphertext characters is only 0.024. The experimental results show that the proposed algorithm can effectively prevent the frequency attack method based on probability statistics.

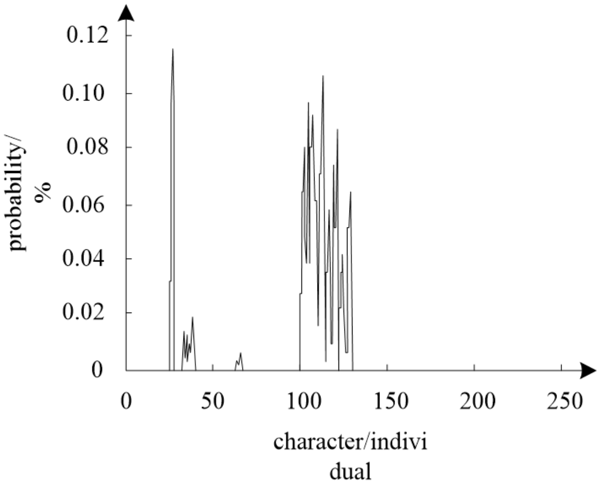

**Figure 4:** Statistical probability of 1 characters in plaintext (up to 0.118)

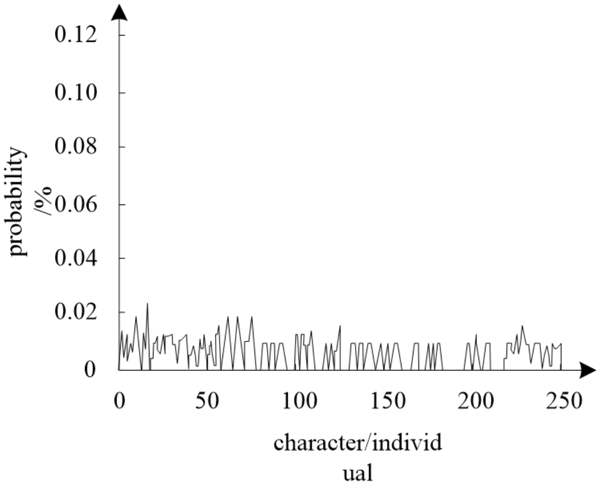

**Figure 5:** Plaintext 1 statistical probability of ciphertext characters (up to 0.021)

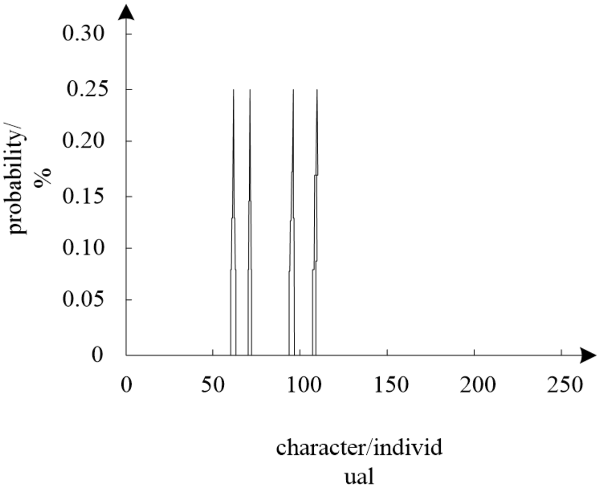

**Figure 6:** Statistical probability of 2 characters in plaintext (maximum 0.25)

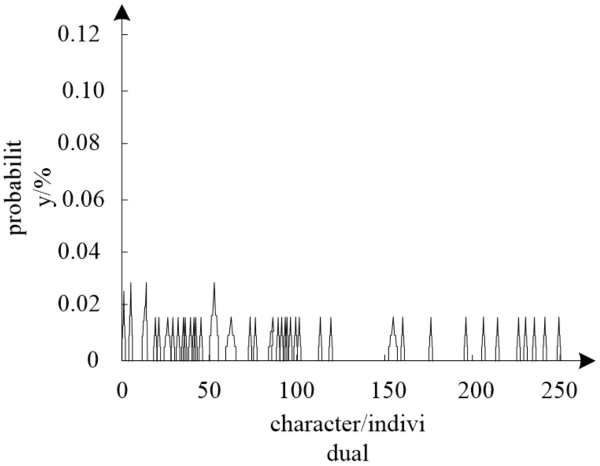

**Figure 7:** Statistical probability of ciphertext characters in plaintext 2 (up to 0.024)

**Table 2:** Comparison and analysis of security characteristics

| Safety characteristics | SMM encryption algorithm | MCS encryption algorithm | LCS encryption algorithm | RSA encryption algorithm based on PKC | Skipjack encryption algorithm | Algorithm in this paper |
|---|---|---|---|---|---|---|
| Extensibility | focus | Dispersed | Dispersed | blend | blend | blend |
| encryption algorithm | Symmetric | Symmetric | Symmetric | RSA | IBE | Symmetric, IBE |
| Self destruction of data | no | yes | yes | yes | yes | Yes |
| Existing equipment and facilities | yes | yes | yes | no | yes | Yes |
| Secret key management | complex | complex | complex | complex | High efficiency | High efficiency |
| Fine-grained access control | yes | no | no | no | yes | Yes |
| Multilevel security | no | no | no | no | no | Yes |

**Table 3:** Encrypted / decrypted file processing speed test

| Experiment times | RSAalgorithm | | SMMalgorithm | | Algorithm in this paper | |
|---|---|---|---|---|---|---|
| | encryption /Mbps | Decrypt /Mbps | encryption /Mbps | Decrypt /Mbps | encryption /Mbps | Decrypt /Mbps |
| 1 | 27.23 | 27.23 | 23.32 | 21.44 | 18.79 | 23.25 |
| 2 | 25.56 | 25.34 | 24.33 | 24.23 | 20.55 | 21.29 |
| 3 | 27.56 | 27.56 | 25.34 | 24.23 | 18.36 | 21.31 |
| 4 | 26.87 | 20.87 | 24.33 | 24.77 | 17.56 | 22.77 |
| 5 | 24.29 | 25.44 | 24.23 | 23.58 | 17.93 | 21.27 |
| 6 | 27.31 | 24.39 | 25.15 | 22.69 | 19.22 | 22.04 |
| 7 | 26.54 | 26.22 | 22.59 | 22.34 | 19.64 | 20.82 |
| 8 | 26.89 | 25.65 | 23.68 | 24.06 | 17.51 | 22.07 |
| 9 | 24.96 | 27.01 | 22.71 | 23.81 | 16.87 | 21.69 |
| 10 | 25.77 | 22.58 | 24.06 | 22.94 | 18.02 | 22.53 |
| Average value | 26.30 | 25.23 | 23.97 | 23.41 | 18.45 | 21.90 |

## 3.3 Comparative analysis of security features of different algorithms

The experiment analyzes the security features of the algorithm from the following seven aspects, and compares and analyzes with the existing algorithms. The analysis results are summarized in Table 2.

It can be concluded that both the proposed algorithm and the Skipjack encryption algorithm use KGC to support the IBE encryption/decryption symmetric key, and the DHT distributed storage mixed ciphertext component is a completely decentralized way with good scalability. The key management of the proposed algorithm is simple and efficient. This algorithm implements multi-level security while further improving the efficiency of key management.

## 3.4 File processing speed and efficiency analysis

In order to verify the specific function of the algorithm, a simulation experiment is carried out. Different network information data is utilized to decrypt and encrypt the operation. The experimental data is shown in Table 3.

When the algorithm performs a large amount of information processing, the average speed of encryption is 18.45 Mbps. Compared with the average speed of the other two algorithms, 26.30 Mbps and 23.97 Mbps, the algorithm has a higher processing speed.

Figure 8 shows the comparison of the encryption efficiency of different algorithms.

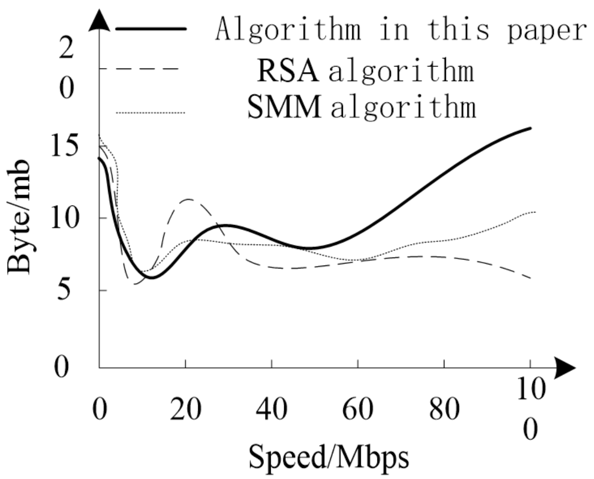

**Figure 8:** Comparison of encryption efficiency

Analysis of the above figure shows that with increasing data processing, the encryption efficiency of this algorithm is significantly higher than the other two algorithms.

### 3.5 Homomorphism analysis of different algorithms

It is difficult for existing encryption algorithms to achieve full homomorphism, and there may be cases where the scheme is not applicable, such as the type of operation or the number of operations. Plaintext is selected randomly and different algorithms are employed to encrypt and perform operations. If the result satisfies the homomorphism of operation in the plaintext space, one can continue to select plaintext encryption and calculate until the result does not satisfy the homomorphism of operation in the plaintext space or the operation result exceeds the plaintext space. By selecting different operations, the application of each scheme to these operations can be obtained, as shown in Table 4.

The analysis of the results in Table 4 shows that the algorithm in this paper has more types of operations. Further, it not only supports any number of addition and multiplication and mixture of addition and multiplication operations, but also supports multiple subtraction operations and division operations. The algorithm can still support an average of 72.23 addition, subtraction, multiplication and mixing operations.

## 4 Discussion

### 4.1 Accuracy analysis of user information identification across social networks

By analysis of Table 1, one can obtain the accuracy of the association information identification of the social network users by the multi-level encryption algorithm of user-related information proposed in this paper. The data in Table 1 indicates that the lowest accuracy for the proposed algorithm to identify the cross-social network user association information is 96.6%, the highest accuracy is 99.0%, and the average accuracy is 97.6%. The accuracy of more than half of the group is higher than the average value, which indicates that the algorithm has strong ability to identify related information of social network users. Users with similar features in the data set are highly likely to be identified, which is mainly because the method for acquiring user association information is based on the social network user association model. Firstly, the model is trained to obtain feature weight parameters, and then it calculates the input feature vector according to the feature weight and compares the calculated result with the classification threshold to determine whether different social network accounts are from the same entity user. It then obtains cross-social network user association information. It can be seen that the proposed method for obtaining user association information is rigorous and logical and improves the accuracy of user information recognition across social networks.

### 4.2 Analysis of validity of the algorithm

Encryption experiments are performed on the two sets of plaintext using the Matlab tool. The plaintext of the experiment is as follows: Cryptology it’s the scrence of over writing (cry ptog raphy), of its authorized decryption (cry ptanaly Sis), and of the rules which are in tum intended to make that unauthorized decryption difficult (encryption security). The plaintext 2 of the experiment is: aaaaaaaaAAAAAAAAuuuuuuuuLLLLLLLL. As shown in Figures 4 and 5, the highest frequency in plaintext 1 is 0.118. After encryption, the probability of character distribution in ciphertext is averaged, and the highest frequency is only 0.021. In Figure 6 and Figure 7, the four characters that appear consecutively are encrypted, the frequency is spread, and the highest frequency of ciphertext characters is only 0.024. A comprehensive analysis of these results can lead to the algorithm proposed in this paper, so as to

**Table 4:** Comparison of different algorithms for different operations

| Experiment | Algorithm in this paper | | | | | RSA algorithm | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| times/second | addition /second | subtraction /second | multiplication /second | division /second | Multiple operations /second | addition /second | subtraction /second | multiplication /second | division /second | Multiple operations /second |
| 10 | 10 | 10 | 10 | 9 | 10 | 8 | 9 | 9 | 7 | 10 |
| 20 | 20 | 20 | 20 | 18 | 20 | 18 | 18 | 19 | 16 | 20 |
| 30 | 30 | 29 | 30 | 28 | 30 | 27 | 28 | 27 | 26 | 29 |
| 40 | 40 | 39 | 40 | 36 | 40 | 35 | 38 | 37 | 35 | 37 |
| 50 | 50 | 47 | 50 | 46 | 50 | 45 | 45 | 46 | 45 | 47 |
| 60 | 60 | 57 | 60 | 53 | 60 | 55 | 55 | 56 | 54 | 55 |
| 70 | 70 | 67 | 70 | 63 | 70 | 63 | 63 | 66 | 64 | 62 |
| 80 | 80 | 75 | 80 | 73 | 80 | 71 | 70 | 75 | 72 | 70 |
| 90 | 90 | 84 | 90 | 80 | 90 | 80 | 77 | 83 | 82 | 77 |
| 100 | 100 | 94 | 100 | 88 | 100 | 88 | 85 | 91 | 89 | 86 |
| Experiment | SMM algorithm | | | | | Skipjack encryption algorithm | | | | |
| times/second | addition /second | subtraction /second | multiplication /second | division /second | Multiple operations /second | addition /second | subtraction /second | multiplication /second | division /second | Multiple operations /second |
| 10 | 9 | 10 | 10 | 8 | 8 | 10 | 7 | 9 | 9 | 10 |
| 20 | 19 | 19 | 20 | 18 | 17 | 17 | 15 | 18 | 15 | 20 |
| 30 | 28 | 29 | 27 | 27 | 26 | 26 | 25 | 28 | 23 | 27 |
| 40 | 36 | 39 | 35 | 36 | 35 | 36 | 32 | 37 | 31 | 36 |
| 50 | 45 | 47 | 44 | 46 | 45 | 46 | 40 | 47 | 40 | 46 |
| 60 | 53 | 56 | 52 | 56 | 54 | 55 | 48 | 55 | 50 | 54 |
| 70 | 63 | 66 | 61 | 62 | 64 | 65 | 57 | 64 | 57 | 62 |
| 80 | 72 | 75 | 67 | 72 | 72 | 73 | 65 | 71 | 63 | 70 |
| 90 | 80 | 82 | 75 | 79 | 80 | 81 | 72 | 80 | 73 | 77 |
| 100 | 88 | 91 | 83 | 87 | 90 | 89 | 80 | 87 | 81 | 84 |

effectively prevent the frequency attack method based on probability statistics.

## 4.3 File processing speed and efficiency analysis

The file processing speed and efficiency results of the algorithm described in Table 3 are analyzed. We can conclude that the average speed of encryption with this algorithm is 18.45Mbps when processing a large amount of information. Therefore, this type of encryption method not only has certain security performance, but also can quickly process various network information.

When the proposed algorithm is compared with the RSA algorithm and the SMM algorithm, we can clearly see that the higher the efficiency, the higher the utilization value of the algorithm. The specific comparison results are shown in Figure 8. From Figure 8, we can clearly conclude that although the operating speeds of the three algorithms are in a slow state in the early stage of system operation, the number of data processing increases with the passage of time. The advantage of the proposed algorithm is obvious. Although there has been a tendency to speed up in the early period for the RSA algorithm, it becomes very slow in the later stage. The proposed algorithm adopts a multi-level chaotic encryption algorithm to encrypt the user-related information, and the neural network is used to inversely propagate the error based on the error-sensitive characteristics of the chaotic system. This improves the multi-level chaotic encryption algorithm and improves the efficiency of multi-level encryption of user-associated information.

## 4.4 Homomorphism analysis of different algorithms

The homomorphism of different encryption algorithms in Table 4 is analyzed. Compared with other algorithms, the proposed algorithm has more types of operations, not only supporting any number of addition, multiplication, and mixture operations, but also supporting multiple subtraction operations and division operations when the number can be divided without any reminder, so that it can satisfy the needs of practical applications. Although the algorithm does not support subtractions of random times, in the test the proposed algorithm can still support an average of 72.23 times of addition, subtraction and multiplication. Therefore, for applications with a small amount of subtraction, the algorithm proposed in this paper can also be applied.

Based on the results of all experiments, the proposed algorithm solves the problem that the existing encryption algorithm does not support multiple multiplication and addition and mixture operations. In addition, compared with the existing homomorphic encryption algorithm, the overall efficiency of the algorithm is higher, and the key and ciphertext length are smaller, so it is more suitable for practical applications.

# 5 Conclusion

Traditional encryption algorithms such as SMM encryption algorithm, RSA encryption algorithm and Skipjack encryption algorithm have the disadvantages of slow speed, high limitation and poor homomorphism. In order to solve the shortcomings in the above algorithms, this paper proposes a multi-level chaotic encryption algorithm, which uses three different chaotic models to transform and spread the plaintext. Based on this, a neural network model is introduced, and the BP algorithm of the neural network model is used to make the error transmit reversely, further confusing the plaintext. Through experiments, the average accuracy of using the proposed algorithm to identify the user-related information across social networks is 97.6%. The highest frequency obtained by averaging the probability distribution of characters in the ciphertext is only 0.021. After encrypting the four consecutive characters, the highest appearance frequency of ciphertext characters is only 0. 024; the average time for encryption using this algorithm is 18.45 Mbps, and the average decryption time is 21.90 Mbps. The experimental results show that the key management of the proposed algorithm is simple and efficient, the encryption speed is fast, and the homomorphism is good. At the same time, the algorithm is a symmetric encryption algorithm. When decrypting, the inverse operation of the encryption and the addition according to the initial key can realize correct decryption and restore the original information.

**Acknowledgement:** Soft science research project of Hebei science and Technology Department (No. 17456001D); the key project of Hebei Federation of Social Sciences (No. 201701501; No. 201802020211).

# References

[1] Liu Q., Zeng J., Yang G., MrDIRECT: A Multilevel Robust Direct Algorithm for Global Optimization Problems, J. Global Optim., 2015, 62(2), 205-227.

[2] Woldemariam A.T., Kassa S.M., Systematic Evolutionary Algorithm for General Multilevel Stackelberg Problems with Bounded Decision Variables (SEAMSP), Annals Oper. Res., 2015, 229(1), 771-790.

[3] Li X., Wang L., Wang J., Multi-Focus Image Fusion Algorithm Based On Multilevel Morphological Component Analysis and Support Vector Machine, IET Image Proces., 2017, 11(10), 919-926.

[4] Haw L.K., Dahidah M.S.A., Almurib H.A.F., A New Reactive Current Reference Algorithm for the STATCOM System Based on Cascaded Multilevel Inverters, IEEE Trans. Power Electr., 2015, 30(7), 3577-3588.

[5] Wang X., Zhang H.L., A Novel Image Encryption Algorithm Based on Genetic Recombination and Hyper-Chaotic Systems. Nonlinear Dynamics, 2016, 83(1-2), 333-346.

[6] Vaisman R., Roughan M., Kroese D.P. The Multilevel Splitting Algorithm for Graph Colouring With Application to the Potts Model, Phil. Mag., 2017, 97(19), 1646-1673.

[7] Parpas P. A. Multilevel Proximal Gradient Algorithm for a Class of Composite Optimization Problems, Siam J. Sci. Comp., 2016, 39(5), S681-S701.

[8] Lai C.G. ShortCommunication: A Note on Optimal Hybrid V-Cycle Multilevel Algorithms for Mixed Finite Element Systems with Penalty Term, Num. Lin. Algebr. Appl., 2015, 4(6), 491-498.

[9] Dekka A., Wu B., Zargari N.R. Dynamic Voltage Balancing Algorithm for Modular Multilevel Converter: A Unique Solution, IEEE Trans. Pow. Electr., 2015, 31(2), 952-963.

[10] Wu Y., Yan C.G., Liu L., An Adaptive Multilevel Indexing Method for Disaster Service Discovery, IEEE Trans. Comp., 2015, 64(9), 2447-2459.

[11] Wenig S., Rojas F., Schönleber K. Simulation Framework for DC Grid Control and ACDC Interaction Studies Based on Modular Multilevel Converters, IEEE Trans. Pow. Deliv., 2016, 31(2), 780-788.

[12] Hu J.S., Lin J.N., Chen H.C. A Discontinuous Space Vector PWM Algorithm in abc Reference Frame for Multilevel Three-Phase Cascaded H-Bridge Voltage Source Inverters. IEEE Trans. Industr. Electr., 2017, 64(11), 8406-8414.

[13] Dekka A., Wu B., Zargari N.R., A Novel Modulation Scheme and Voltage Balancing Algorithm for Modular Multilevel Converter, IEEE Trans. Industr. Appl., 2016, 52(1), 432-443.

[14] Wang M., Xu C., Wang Q., Research of a New Reliability Analysis Method Based on Multilevel Flow Model and Its Application on the Gas Turbine Compressor, J. Chem, Eng. Jap., 2015, 48(8), 656-661.

[15] Zampini S., Tu X., Multilevel Balancing Domain Decomposition by Constraints Deluxe Algorithms with Adaptive Coarse Spaces for Flow in Porous Media., Siam J. Sci. Comp., 2017, 39(4), A1389-A1415.

[16] Kaur S., Bharadwaj P., Mankotia S., Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES, Autom. Instr., 2017, 9(9), 22-29.

[17] Li D.S., Chen Z.G. A New Method to Prevent Trojan-in Node Based on Inner Secure Tunnel, J. China Acad. Electr. Inform. Techn., 2015, 10(4), 379-382.

[18] Alnesarawi A.N., Al-Tamimi M.S.H. An Improve Image Encryption Algorithm Based on Multi-level of Chaotic Maps and Lagrange Interpolation, J. Power Supply, 2018, 59(1A), 179-188.

[19] Hua T., Chen J., Pei D., Quantum Image Encryption Algorithm Based on Image Correlation Decomposition, Int. J. Theor. Phys., 2015, 54(2), 526-537.

[20] Gong L.H., He X.T., Cheng S., Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations, Int. J. Theor. Phys., 2016, 55(7), 3234-32.

[21] Fu H., Liu X., Research on the Phenomenon of Chinese Residents' Spiritual Contagion for the Reuse of Recycled Water Based On Sc-Iat., Water, 2017, 9(84611).

[22] Rosa M., Núñez M.L.G., Multiplier Method and Exact Solutions for a Density Dependent Reaction-Diffusion Equation, Appl. Math. Nonlin. Sci., 2016, 1(2), 311-320.

[23] Martinez-Lara M.J., Paez Melo M.I., Design of Experiments Applied in the Optimization of the Extraction Method Quechers for the Determination of Organoclorated and Organophosphoric Pesticides in Soils, Rev. Int. Contamin. Ambient., 2017, 33(4), 559-573.

[24] Thorenz A., Wietschel L., Stindt D., Tuma A. Assessment of Agroforestry Residue Potentials for the Bioeconomy in the European Union, J. Clean. Prod., 2018, 176, 348-359.

[25] Sardar M.S., Zafar S., Zahid Z., Computing Topological Indices of the Line Graphs of Banana Tree Graph and Firecracker Graph, Appl. Math. Nonlin. Sci., 2017, 2(1), 83-92.

[26] Gao W., Zhu L., Guo Y.,Wang K., Ontology Learning Algorithm for Similarity Measuring and Ontology Mapping Using Linear Programming, J. Intel. Fuzzy Sys., 2017, 33(5), 3153-3163.