RESEARCH ARTICLE OPEN ACCESS

The Encryption Algorithm Based on Principal Component Analysis of Times Series

Xiao Bin-bin[1], Jiang Xiao-qi[2]
1(College of information and technology, Jinan University, GuangDong)
2(College of information and technology,Hengyang Normal University,HuNan)

--************************----------------------------------

Abstract:

As to the poor computing power of the wearable devices, the encryption algorithm based on principal component analysis was proposed.First, the algorithm was divided into groups, and each group of data was encoding to extract its main components, then acquired the trend of time series and according to the sequence of the comprehensive index to generate the encryption key. By using the key to carry out the shift operation, a simple cipher text was generated. In the receiver, the same decryption mechanism can be used to get the decryption. The examples showed that the proposed encryption algorithm, compared with the traditional DES algorithm, was simple and easy, It can be convenient and simple application in wearable devices.

Key words—**wearable device; key; DES algorithm; time series; principal component analysis.**

--************************----------------------------------

I. INTRODUCTION

Time series (time-series) is arranged in chronological order with the time variation of the numerical set [1],which widely exists in the real life, such as daily stock price, according to the season ranking quarterly rainfall, the products of the company's monthly sales.Time series prediction is very important in many real applications[2] and the common methods of analysis are: manual, moving average method, weighted moving average value method ,the least square method [3]and the principal component analysis method proposed in literature 3.For the encryption algorithm, the encryption algorithm is the typical DES, RSA, MD5 etc.. The DES algorithm developed by American IBM company, is by far the most typical symmetric encryption algorithm.It is widely used in many fields, plays a great role in promoting the development of the theory of cryptography. It contains 64 bit plaintext, 64 bit secret key , and actually involved in calculation of only 56 bits of data, which has 8 bits for parity, the plaintext and secret key were a series of replacement operations, and ultimately the encrypted data. But since it was proposed, facing security threat from various aspects, such as the brute force attack, chosen plaintext attacks [4]. At the conclusion of the study shows that the DES algorithm has the following characteristics: (1) DES encryption speed is quite fast, can be applied to large amounts of data encryption. (2) DES algorithm for dense steel length is only 56, relatively short, so the safety of the confidential algorithm of DES is low, the secrecy of the key is the key. (3) the realization of the algorithm rely mainly on S-box substitution function, S-box in DES algorithm is nonlinear, so far has not yet announced the origin of S-box, once the S-box security can not be guaranteed, the algorithm will face severe test [5]. And RAS algorithm initially by the United States Massachusetts science and scientists proposed in 1977, mainly based on randomly generated large prime principle to generate a key currently available for digital signature and encryption, is so far the most perfect cryptography [6] [7].The actual application of the RSA algorithm is mainly used for massive data encryption [8]. While the literature 9 presents an implementation of parallel AES algorithm based on GPU, greatly improved the efficiency of the AES algorithm. The literature10 presents an encryption algorithm based on attribute, pointed out that a constant length of ciphertext and has no center authorized key strategy agency said rich access strategy. For wearable device because of its own CPU equipment capacity calculation. The calculation ability is low, all of the above algorithms are difficult to carry out simple transplantation on wearable devices. Therefore, this paper developed an encryption algorithm based on principal component analysis, principle of the [11][12] algorithm reference attribute encryption, principal component analysis as a feature attribute data sequence itself. Firstly, the original plaintext is quantized, then extract the principal components based on principal component feature extraction of digital encryption key is generated. Then, the original plaintext according to key shift operation, to complete the encryption process. In the receiver, the same according to the algorithm, extract the key and reverse shift operation, can get to the original plaintext. Compared with DES and RSA algorithm: (1) the algorithm is simple, without a large amount of calculation, only simple digital feature extraction and shift operation, can be easily used for wearable devices. (2) according to the principal component analysis to extract the digital characteristics of the algorithm, the key is the only reliable, to ensure strict mathematics. This paper makes a detailed analysis of the algorithm and its application.

II. The time series feature extraction algorithm based on principal component analysis

Step1 For the time series, the principal component extraction follows. Let n is the unit of time (such as year, month, date, etc.), m denotes the index entries, Xij the I (I = 1, 2,... N), in the j index performance score and by Xij constitute a scoring matrix.

$$X = \begin{bmatrix} x11 & x12 & \dots & x1m \\ x21 & x22 & \dots & \dots \\ \dots & \dots & \dots & \dots \\ xn1 & xn2 & \dots & xnm \end{bmatrix}$$

$$R = \begin{bmatrix} r11 & r12 & \dots & r1m \\ r21 & r22 & \dots & \dots \\ \dots & \dots & \dots & \dots \\ rn1 & rn2 & \dots & rnm \end{bmatrix}$$

$$r_{ij} = \frac{1}{n} \sum_{k=1}^{n} xki \quad xkj(i, j = 1, \dots, m)$$

Step2 R matrix eigenvalue lambda K (k=1, 2, M...) units feature vector corresponding to ak= (AK1, ak2, AKM,...) as the unit characteristics corresponding to the vector lambda K. Let YK = AK1 * X1 + ak2 * x2 +... + AKM * xk. for a given amount of information assurance indicators M% (usually 5%).

$$\frac{1}{m}\sum_{i=1}^{j=1}\lambda k < M \le \frac{1}{\mathrm{m}}\sum_{i=1}^{s}\lambda k(1<s<m)$$

Step3 According to the principal component yk calculate the time of the yk index, with the contribution rate of all main components for weight coefficient qk build a comprehensive evaluation index, generate new data arranged by time sequence.

$$f = \sum_{i=1}^{k} yk * qk$$

III. The data encryption algorithm and its implementation based on principal component analysis

Make use of a sequence of principal component analysis can be derived time series of re queuing order, according to the sort order can be the time sequence is sorted change, thus time series get new ranking results, time series is also in accordance with the order of ranking of shift operation, so as to complete the sequence final shift results, the results that encryption time series, derived sequence synthesis index is encryption key. The encryption algorithm realization process as shown in Fig 1.

Step1 The data encoding to generate encryption sequence.Then the sequences were grouped to generate the sequence of matrix X and matrix R.

Step 2 Extraction and analysis of main components of the matrix, analysis algorithm and generate the ranking results according to the principal component 2 section proposed, comprehensive ranking results F, generates the sort key.

Step 3According to the ranking results of F, sequence shift operation, generating encrypted cipher text. Transfer and sent to the receiver

For example,Set to transfer the data to 64 data encoding. The group divided into eight groups, each group of eight bits of data, the matrix X.as shown in Fig2

$$X = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Fig2 Matrix X

Calculation of matrix R and generate the final ranking F, the vector representation of X matrix. X1=[1 010101 1] X2=[1111101 0] X8=[1 011010 1]........, calculate the f index. F=[5428731 6]. Shift operation, namely X1 into X5, X2 into X4, until X8 replaced X6. The shift matrix of X matrix X new.as shown Fig3

Second shift operation, according to the f index will draw new matrix X of each row vector, the first move to replace the five, second place for fourth place, third place for the second, fourth place for the eighth, fifth place for the seven, sixth for the third, seventh for the first, eighth replaced sixth. The final encryption matrix X as follows. As shown in Fig4.

$$X = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Fig 3 Matrix X New

$$X = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Fig 4 Matrix X

IV. CONCLUSION

The encryption process based on principal component analysis makes full use of the principle of principal component analysis of time series, the established time series explicitly, that is, to achieve the encrypted data transfer process, also effective for time series were trend analysis. And for the data to be transferred to the character, or the guy and can be quantitative data and the quantitative data are divided by the ASCII or GB2312 code, specific packet length and the number of bits can be set according to the needs of secure encryption, time series using principal component analysis trend analysis of the crygraphic key and transmitting, compared the algorithm with the existing encryption algorithm, namely effective were encrypted data, while avoiding the calculation complex existing encryption algorithm of the key generation process. Thus greatly reduce the ability of the hardware requirements of computing devices or digital computing logic calculation, can be effectively used in the emerging wearable devices.

V. REFERENCE

[1] Xiu chun-bo.The time series prediction method of [J]. Application Research of computers, 2010 (4): 1265-1269.

[2] LIM T P.PUTHUSSERYPADY S.Chaotic time series prediction and additive white Gaussian noise[J].Physics Letters A.2007.365(4):309-314.

[3] Peng jing-bin.A prediction method of Natural Science Journal of Xiangtan University [J]. time series trend based on principal component analysis, 2010,32 (2): 123-125.

[4] 现代密码学(第二版)[M].北京:清华人学出版社.2007.1-3.

[5] Yang-bo.Modern cryptography (Second Edition) [M]. Beijing: Tsinghua University Press,.2007.1-3.

[6] Chen qiao-chuan.An encryption algorithm of [D]..2015. of Yunnan University and RSA based on hybrid DES

[7] Ning -jie.A new combined fast RSA algorithm [J]. Journal of Shenyang University of Technology, 2001,27 (2): 224-227.

[8] Li-qiang.A fast algorithm of RSA [J]. micro computer system improvement, 20012270-72.

[9] Yang-bo.Modern cryptography (Second Edition) [M]. Beijing: Tsinghua University press, 2007:1-2.

[10] [Zhang-peng.GPU parallel AES encryption algorithm based on the realization of [D]. Jilin University, 2011

[11] LI qin-yi.The encryption algorithm of [D]. based on the attribute of Xi'an Electronic and Science University, 2013

[12]]Su jin-shu.Attribute based encryption mechanism [J]. Journal of software.2011,22 (6): 1299-1235.

[13] X. Liang, Z. Cao, H. Lin, D. Xing. Provably Secure and Effcient Bounded Ciphertext Policy Attribute-Based Encryption.ACM Conferenceon

[14] Computerand Communication Security(ASI-ACCS 2009),New York:ACM,2007:343-352

AUTHOR:Xiao Binbin (1990-), male, master, Major in Information Security and Cryptography