Application of Encryption System Realized by Voiceprint Information on Remote Education Platform

Jingyun Li
Full Beijing NO.35 middle school, No.8 Zhaodengyu Road, Xicheng District Beijing China
angela@cas-harbour.org

Keywords: Voiceprint recognition, RSA, AES.

Abstract. In the remote education system, teachers and students need to transfer data such as text, voice message, pictures and videos via internet. Thus, information security is very important in such systems, and only by using encryption technology to protect information can intellectual property and personal privacy information protected.This paper proposes a system authentication process using voiceprint information, and encrypts and decrypts files based on the RSA algorithm Methods. The experiment proves that the system can protect the user's private information effectively, thereby improving the system security.

1. Introduction

In remote education systems, teachers and students need to transfer data such as text, voice messages, pictures and videos via internet. Thus, information security is very important for such systems, and only by using encryption technology to protect information can intellectual property and personal privacy information be protected.

The use of fingerprints, irises, faces, voiceprints and other personal biometric information to achieve encryption technology is very beneficial to protect personal privacy. First of all, an encryption system based on personal biometric information can provide security. This is because every person has completely different fingerprints and other biometric information which can hardly be repeated. If an attacker cannot access the private information of others, it will be very difficult to attack such an encryption system. Secondly, this encryption technique also brings convenience. Users can use the biometric information reading device to obtain specific personal biometric data when needed, and complete the encryption and decryption processes without having to memorize a lot of complicated passwords composed of characters and numbers. In contrast, the conventional authorization authentication technology uses passwords, tokens and PINs that require users to memorize and save complex password information. At the same time, it is very inconvenient to use and maintain passwords frequently.

Nowadays, voiceprint recognition technology has been applied to many fields such as finance, securities, criminal investigation, and other civil safety certification systems in a worldwide range. Especially in the aspect of safety certification, the sound does not involve privacy issues, and the related equipment is inexpensive. Besides, using voiceprint for identification is a natural and economical method, and the degree of user acceptance is relatively high. For example, the passwords of banks and securities systems can be replaced by sounds, that is, voiceprint technology can be used to convert sounds into keys, so that people do not need to remember complicated passwords, nor do they need to carry keys (U shield), smart cards, etc.

This paper proposed a technique for generating public/private keys based on the RSA algorithm using users' voiceprint feature data, to protect the data and information transmitted in the remote education system. Hackers or external users cannot obtain users' voiceprint features, so the key generation process is unpredictable, and such an encryption system is difficult to crack. The system proposed in this paper can use the user-generated voiceprint features to generate public and private keys online during the registration phase, while the private key is not stored on any device, thus reducing the risk of the private key being stolen. The system implements a secure environment to prevent unauthorized users from accessing the system. At the same time, the system uses AES

encryption algorithm to encrypt and protect the voiceprint feature data provided by the user during the registration phase, thereby realizing the confidentiality of the biological information. Since the private key is generated online, there is no risk of loss and theft. When using the system, users collect the voiceprint feature data by using a sound pickup device provided by various types of terminals such as smart terminals and PCs, which generates a private key online after authentication, decrypts the received data file, and realizes it in the remote education system to secure data transfer.

2. Related work

A lot of work has been done in developing biometric-based key generation. In the literature [3], Feng Hao et al. proposed a key generation method based on iris features and anti-leak tokens. This method can generate 140-bit biometric keys which is sufficient to generate a 128-bit AES key. In [4], Chen, B. et al. proposed a technique for generating deterministic bitstream sequences from a repeatable one-way transformation through an entropy-based feature extraction method, coupled with Reed-Solomon error correction coding. This technique uses 3D face data to generate a long key sequence for 128-bit AES. In [2], Vincenzo Conti S.V. et al. proposed a method for embedding biometric information into the private key/public key generation process of the RSA algorithm. The private key generation relies on the features of physical or behavioral biology and can be generated on demand. In [5], Gang Zheng et al. proposed a fuzzy mapping method based on grid mapping for generating keys from biological data. The simulation results showed that the authentication accuracy of this method was equivalent to the classification result of the k-adjacent algorithm. In [6], Beng. A et al. proposed a biometric key generation method based on a randomized biometric aid. In [1], Soong, F. et al. proposed a text-independent speaker model based on a vector quantization method to implement speech recognition technology, which can extract voiceprint feature data from users' speech simply and effectively.

3. System implementation

The system generated a key based on the voiceprint data. During the registration phase, the user read the text information for 10 seconds to 20 seconds according to the system prompt in a low-noise environment. Then the system read the audio data, extracted the short-term acoustic spectrum features from the speaker, and used the vector-based quantized speech recognition technology to process the data and generate an original feature vector which was added to the codebook. In the authentication phase, the user also provided audio information by reading aloud to complete the authorization authentication process through feature extraction, and completed the generation of the RSA algorithm public/private key pair. The system used the RSA algorithm to implement an asymmetric encryption method, which was realized by executing the user-based speech feature vector encryption algorithm to generates a pair of prime numbers, and performed the process of mapping feature vectors to prime numbers using the ad-hoc function. The system first sampled a partial bit stream from the feature vector and spliced the obtained multiple pieces of data to generate a final bit sequence. This sequence constituted the index value of the first prime number stored in the lookup table. The system then performed sampling on the rest of the feature vector in turn, and calculated subsequent index values to find subsequent prime numbers. The lookup table was constructed offline and contained high-dimensional prime numbers.

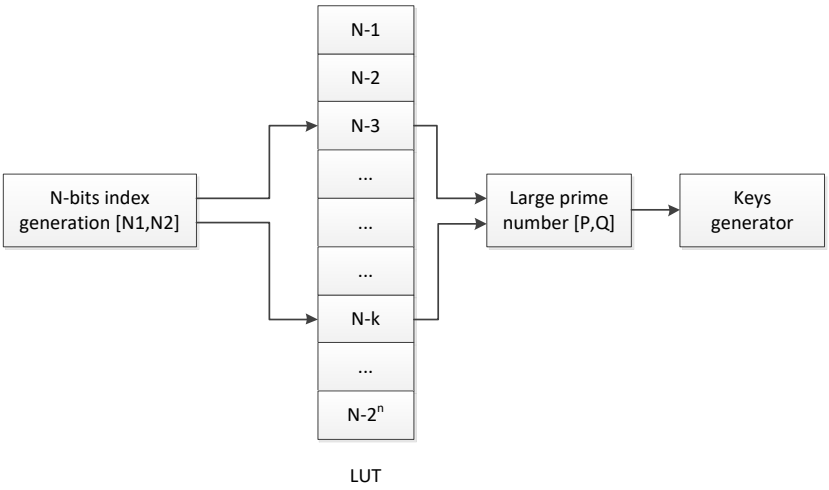

Fig.1. Public/ private keys generator

3.1 Encryption method

In the remote education system proposed in this paper, two encryption methods were used to protect the storage and transmission of data. They were the asymmetric encryption method--RSA and the symmetric encryption method--AES. The RSA algorithm was used to protect the data files in the form of text, voice, pictures, videos, etc. transmitted and exchanged by the lecturers through the network, while the AES algorithm protected the voiceprint feature data submitted by the user during the registration phase.

3.1.1 RSA

- Rivest, Shamir and Adleman developed the world's first public/private key-based encryption algorithm in 1977, the well-known RSA algorithm, which was released in [7]. This algorithm is also the most widely accepted and implemented universal public/private key encryption algorithm. The main points of the algorithm include that,
- p and q are two very large private prime numbers;
- n=p×q is a public number;
- Φ(n) is an Euler function;
- e is a number less than $\emptyset(n)$and is publicly owned by it;
- d is a private number, and $e \times d = 1 \bmod \emptyset(n)$.

Here, e is the public index and d is the private index. In the RSA algorithm, the sender and the receiver must know the value of n in advance. The sender knows the value of e, and only the receiver knows the value of d. Thus the public key is defined as {e,n} and the private key is defined as {d,n} . The plaintext M is encrypted by equation (1):

$$C = M^e \bmod n \tag{1}$$

The ciphertext C is encrypted by equation (2):

$$M = C^d \bmod n \tag{2}$$

The main characteristic of this algorithm is that given d and n, it is determined that d is not achievable.

3.1.2 AES

AES is an algorithm that implements encryption and decryption using symmetric encryption. In other words, AES can encrypt and decrypt files with a single key. As a new generation of data encryption standard, AES algorithm has the advantages of strong security, high performance, high efficiency, being easy to use and flexibility. The AES algorithm mainly includes three aspects: round variation, iteration number and key expansion. The key lengths supported by the AES algorithm are 128 bits, 192 bits, and 256 bits, respectively, and the length of the data block is fixed to 128 bits. In the AES algorithm, different key length corresponds to different numbers of iterations: the number of iterations of the 128-bit key length is 10, while that of 192 bits is 12, and that of 256 bits is 14.

3.2 Voice authentication

The remote education system encryption scheme proposed in this paper selected voice as the biometric data extracted by the user. The main reason was that most devices from intelligent terminals to PCs have audio collection functions, which is more convenient to collect biometric data such as fingerprints, irises, etc. At present, the voiceprint recognition function can be realized in a variety of ways, but the principle of our selection is that the voice recognition method should be simple and effective, can be quickly quantified, and is ready to generate public/private keys.

In the encryption scheme of a remote education system, we chose the vector quantization model as the speech recognition technology by utilizing users' voiceprint feature data. This model is a simple text-independent speaker model in speech recognition technology. It extracts and encodes the speech features of each person into a codebook. In the identification, the test features are encoded according to the codebook to quantify the generated codes as the judgment standard, and the distortion degree has the characteristics of high recognition accuracy and fast judgment speed. Vector quantization models are often used to the techniques of calculating acceleration and the techniques of lightweight practical implementation. When combined with the techniques of adaptive background model, the vector quantization models have a very high recognition accuracy.

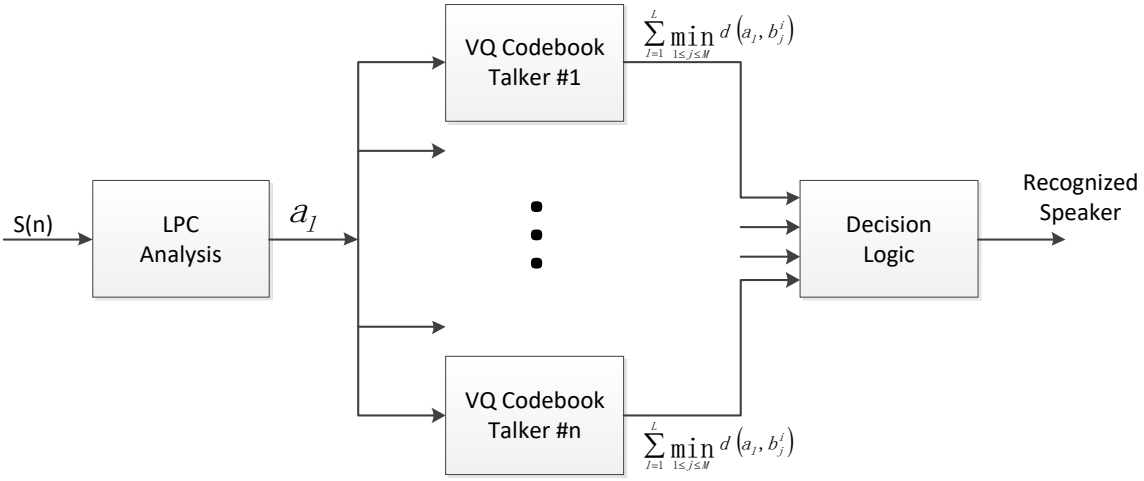

Fig.2. VQ speaker recognition block diagram

3.3 The Generation and Distribution of Public/Private Key

This paper proposed to encrypt the data transmission in the remote education system by using personal voiceprint information to realize a complete PKI system. The RSA encryption algorithm uses a fixed-length random number algorithm to do public and private key calculations. The system remotely reads the user voice data during the registration phase, extracts the voiceprint feature information on the server side, calculates the public key and the private key, encrypts the transmitted data and files, and destroy the private key after encryption. In addition, the original data will be saved to the server. With this mechanism, the system generates a private key only when necessary. The key is used to encrypt and decrypt data and files and to authenticate the user. After a successful operation, the private key is destroyed. With this method, the private key will neither be lost nor stolen.

In the public key generation phase, the user registers on the system platform, and the terminal collects personal voice data and extracts the voiceprint feature vector on the server side. After the user's voiceprint feature extraction is completed, the system uses the feature vector to generate and publish public key data. In the private key generation phase, that is, in the user using phase, the user collects the voice data of fixed text by the recording device on the smartphone, tablet, laptop, and PC terminal during the first login to the system, and then the voice data is transmitted to the server for authentication by the speaker.

4. Experimental Results

In order to verify the encryption scheme of the remote education system, we collected the voice data of 20 users, 10 of whom were female and 10 were male, and each of them had 10 piece of voice data. The recorded content was the text that each user read the same content for 10 seconds in different scenes. The audio data was first processed by a bandpass filter from 200 Hz to 3.2 kHz and then sampled at a frequency of 6.4 kHz. The accuracy of the voiceprint data was 98.14%.

The system transformed the user voiceprint data into two index values of the prime lookup table to generate public/private keys. In the experiment, we used the 4096-bit feature vector length of user voiceprint. In order to calculate the values of p and q in RSA algorithm, we created a prime lookup table by using two 128-bit data subsets. With this technique, the system could not generate duplicate prime numbers, that was, the generated public/private key pairs were unique. The experimental results showed that the False Acceptance Rate (FAR) of the system was 9.47%and the False Rejection Rate (FRR) was 0.

5. Conclusion

In remote education systems, the lecturers transmit and exchange data files in the form of text, voice, pictures, videos, etc. through the network. This paper proposed a system authentication process using voiceprint information, and encrypted and decrypted files based on RSA algorithm. The experiment proves that the system can effectively protect the user's private information, thereby improving the security of the system, and at the same time, the users do not need to memorize complicated passwords, nor do they need to use hardware devices such as smart cards, which brings great convenience.

References

[1] Soong, F., A.E., A. R., Juang, B.-H., and Rabiner, L. “A vector quantization approach to speaker recognition,” *AT & T Technical Journal 66*, pp. 14–26, 1987.

[2] Vincenzo Conti S.V., “Fingerprint Traits and RSA Algorithm Fusion Technique,” *Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, Palerm,* pp. 351–356, 2012.

[3] Feng Hao, Ross Anderson, John Daugman, “Combining cryptography with biometrics effectively,” *Technical Report No. 640, UCAM-CL-TR-640, ISSN,* pp.1476-2986, 2005.

[4] Chen, B. and Chandran, V., “Biometric Based Cryptographic Key Generation from Faces,” *the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications*, pp. 394 - 401, December 2007

[5] Gang Zheng, Wanqing Li and Ce Zhan, “Cryptographic Key Generation from Biometric Data Using Lattice Mapping,” *the 18th International Conference on Pattern Recognition, vol.4,* pp. 513 - 516, 2006

[6] Beng.A, Jin Teoh and Kar-Ann Toh, “Secure biometric key generation with biometric helper,” *the 3rd IEEE Conference on Industrial Electronics and Applications, Singapore,* pp.2145-2150, June 2008

[7] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems” *Communications of the ACM*, February 1978

[8] Sadikin, Mohamad Ali. Wardhani, Rini Wisnu. “Implementation of RSA 2048-bit and AES 256-bit with Digital Signature for Secure Electronic Health Record Application,” *Implementation of RSA 2048-bit and AES 256-bit with Digital Signature for Secure Electronic Health Record Application,* 2017.