



Biometric Cryptosystem for VoIP Security using RSA Key Generation

Mrs.R.Sridevi^[1], S.Karthika^[2]

^[1] Assistant.Professor, Department of Computer Science.

^[2] Research Scholar, Department of Computer Science.

PSG College of Arts and Science, Coimbatore, Tamilnadu, India.

Abstract:-This paper presents a narrative key generation scheme using biometric methodology for providing high security over the internet applications such as VoIP technology. The present work deals with modern computing systems security issues, focusing on biometric based asymmetric key generation process. The term VoIP refers-“voice over internet protocol (IP)” in which the “voice” to be transmitted using the internet protocol (IP). The major obstacle to this kind of data sharing is secure access. To deal this problem, this paper proposes a method called Biometric-Crypto system which generates a key from the finger print for both encryption and decryption of the voice data packets for VoIP Security. The key generation process has to be done using a powerful cryptographic algorithm RSA. The secret key is generated from the finger print image using asymmetric cryptographic algorithm RSA and the voice data packets are to be encrypted and decrypted using the secret key. So that only the intended recipient can access the data. This scheme ensures confidentiality for VoIP Technology.

Keywords: Biometric-Crypto system, VoIP, Fingerprint, Minutiae point, ROI, RSA, Encryption, Decryption.

I. Introduction

Cryptography is one of the fundamental building blocks of computer security. It is intended to ensure the secrecy and authenticity of messages. This technique is used to encrypt the data using any key so that it is not in the understandable format to the attackers. The original data can be obtained by decrypting the encoded data using the key. Thus the data confidentiality is well protected by the cryptographic approach.

Information security and privacy has become a major issue in the present world. Biometric-Crypto system is one of the most important techniques for security due to its distinctive nature of biometric traits such as fingerprint and faces. Biometric is the study of methods for uniquely recognizing and establishing the identity of an individual. Biometric characteristics can be divided into two main classes:

- **Physiological Traits:** - It's related to the shape of the body. Such as fingerprint, face recognition, DNA, hand and palm geometry, iris recognition.
- **Behavioral Traits:** - It is related to the behavior of a person. Ex: typing rhythm, gait and voice.

VoIP technology in general refers to the set of software, hardware and industry standards that enables the voice to be transmitted using the internet protocol (IP). The Voice over Internet Protocol (VoIP) specifies the transmission and reception of audio over the Internet. A connection between caller and call recipient is established using the Session Initiation Protocol (SIP). This technology allows voice communication through the internet. Many, small, medium even larger corporations are changing to VoIP services for business communications. VoIP number is portable to anywhere that there is an internet connection. It is not limited by physical distance or any area code.

VoIP is the process of converting voice signals into data packets, using internet protocol (IP) to transmit voice over a data network. It is also known as IP Telephony. VoIP calls can take place between LAN or on WAN as in the case with internal calls on a corporate network.

VoIP technology converts voice into little packets of data and then they travel on a route of several routers, to reach their destination. There are a few distinct benefits that companies receives when utilizing IP telephony. Companies providing VoIP service are commonly referred to as providers, and protocols which are used to carry voice signals over the internet are commonly referred to as VoIP protocols.

This paper proposes a key generation scheme for asymmetric cryptographic algorithm RSA using biometrics. The secret key is generated from the finger print image using RSA algorithm and the voice data packets are encrypted and stored in the database. The recipient receives the encoded data and decrypts it by using private key to receive the original voice. Biometric-Crypto system is used to provide security for VoIP technology. Biometric-Crypto system can operate in one of the following three modes, (i) **Key release:** - In the key release mode the biometric template and the key are stored as separate entities and the key is released only if the biometric matching is successful.

(ii) **Key binding:** - The key and the template are monolithically bound within a cryptography frame work.

(iii) **Key generation:** - In this mode the key is directly derived from the biometric data and is not stored in the data base.

There is a security issue in key release mode because the biometric template is not secure in the pattern but it is easy to implement. Biometric-Crypto system that work in the key binding/generation modes are more secure for data sharing over the internet applications but difficult to implement due to large intra-class variations in biometric data. The fingerprint pattern of biometric-crypto system is used in this approach because it is stable throughout person's life time.

II. Biometric – Crypto System

A biometric authentication system is considered one of the most accurate and robust methods of the identity verification. The functions of biometric systems are measuring and determining the unique characteristics of an individual with one already recorded. It provides high security to the messages based on the key. Biometric cryptosystems combines cryptography and biometrics to benefit from the strength of both fields. This technique eliminates the need to remember password. In Biometric cryptosystem a cryptography key is generated from the biometric template of a user and stored in the database. The key cannot be revealed without a proper biometric authentication.

A. Finger Print Biometrics:-

In this approach finger print image recognition biometric feature is used to generate key for VoIP security. This is most widely accepted biometrics among the technology being used today. Fingerprints are unique to each individual and no two fingerprints are alike. Fingerprints contains pattern of ridges and valleys as well as minutia points. Ridges are the upper skin layer segments of the finger and valleys are the lower segments.

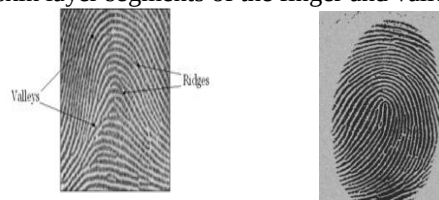


Fig.1. Finger print images

III. Proposed Work

B. RSA Algorithm:-

Encryption is the process of converting original message (plain text) into some unreadable format (cipher text). So that only the intended recipient can access the original message by using the cryptography key. In this paper a cryptographic key is generated from fingerprint image using a powerful cryptographic algorithm RSA for VoIP Security. RSA (Ron Rivest, Adi Shamir, and Len Adleman) is one of the most popular algorithms used in asymmetric key cryptography. RSA is a widely used Public-Key cryptographic algorithm. According to this the Public key is known to everyone whereas the Private-key is known only to the user who is originally owns the data.

RSA Algorithm involves three steps:

- (i) Key Generation: The process of key generation has to be done before the voice data packets are encrypted.
- (ii) Encryption: encryption is the process of converting plain text into cipher text.
- (iii) Decryption: decryption is the process of encrypted text into the original text.

• Key generation :-

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted by using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q .
For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length.
2. Compute $n=p*q$; n is used as the modulus for both the public and private keys. Its length, expressed in bits, is the key length.
3. Compute $\phi(n) = \phi(p) \phi(q) = (p-1)(q-1)$, where ϕ is Euler's totient function.
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; e is released as the public Key exponent.
5. Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\phi(n)$).
6. d is as Private-Key component, So $d*e \equiv 1 \pmod{\phi(n)}$.
7. The Public-key consists of modulus n and the public exponent e .
8. The Private-key consists of modulus n and the private exponent d .

C. Encryption

Encryption is the process of converting original voice into some other format (cipher voice).

Steps:-

1. Sender reads the input voice and encrypts the voice data packets using the receiver's public key to transmit the message.

2. Original voice is encrypted and the encrypted data packets(cipher voice) C is, $C = m^e \pmod n$
3. Now the encrypted voice data packets are stored in the database.

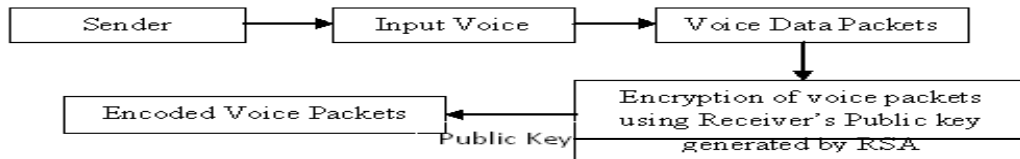


Fig.2 Encryption of voice data packets using Receiver's Public key

C. Decryption

Decryption is the process of converting the encrypted voice data packets into original voice.

Steps:-

1. Receiver receives the encoded data from the database.
2. Decrypt the encrypted voice data packets by computing,

$$m = C^d \pmod n$$
3. By finding the value of m the receiver can get back the original data by reversing the padding scheme.

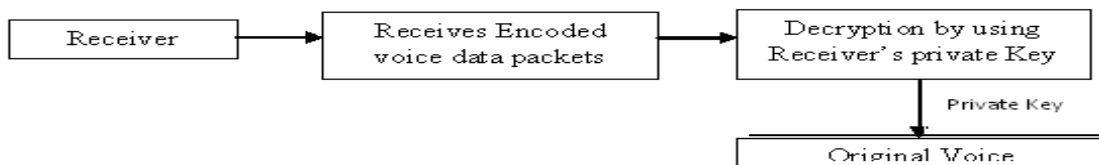


Fig.3 Decryption process using Receiver's Private Key

IV. Cryptographic Key Generation from Finger Print:-

In this approach Fingerprint biometric pattern is selected for generating cryptographic key. After processing the particular image the minutiae points from the fingerprint is extracted based on the calculation of region of interest (ROI) and set that location for generating cryptographic key.

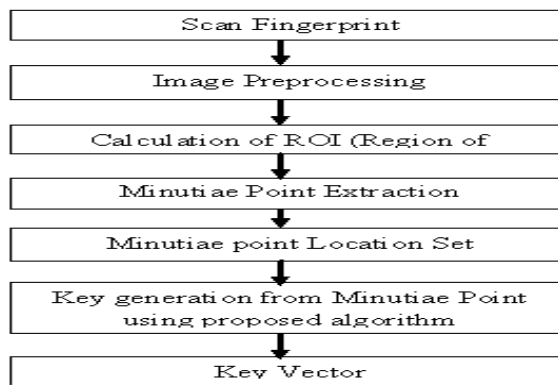


Fig.4 Steps in key generation from fingerprint

A. Image Preprocessing:-

For the fingerprint image preprocessing, Histogram Equalization and Filters are used to enhance the image. And then the Binarization is applied on fingerprint image. The morphological operation is performed to extract Region of Interest (ROI).

Histogram Equalization:-

Histogram equalization increases the contrast of images, especially when usable data of the image represented by close contrast value. It permits pixel value to expand. Histogram equalization converts range from 0 to 255 which will enhance visualization effect.



Fig. 5 Sample Finger Print before and after Histogram Equalization

B. Region of Interest (ROI):-

The steps involved in ROI extraction are Binarization and Morphological Operation.

- **Binarization:-**

Binarization is the process of translating gray level image into a binary image. This enhances the contrast between the ridges and valleys in a fingerprint image. In this process where each pixel in an image is converted into one bit and assign value for that as '1' or '0' depending upon the mean value of each pixel. After performing this operation, the ridges in the fingerprint are highlighted with black color while furrows are white.

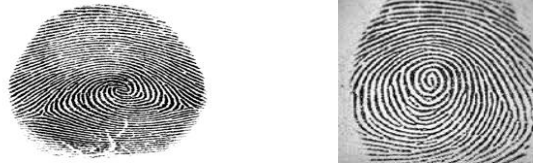


Fig. 6 Fingerprint before and after Binarization

- **Morphological Operation:-**

Morphological operations are used to understand the structure or form of an image. This usually means identifying objects or boundaries within an image. There are three primary morphological functions: erosion, dilation, and hit-or-miss. Two morphological operations called "OPEN" and "CLOSE" are adopted. The "OPEN" operation can expand the images and remove peaks introduced by the background noise. The "CLOSE" operation can shrink the images and eliminate small cavities. Thinning is a morphological operation that is used to remove selected foreground pixels from binary images.

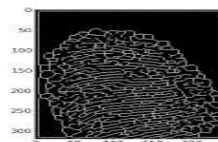


Fig.7 Morphological Operation

D. Minutiae Points Extraction

Thinning eliminates the redundant pixels of ridges till the ridges are just one pixel wide. The method uses an iterative, parallel Ridge thinning algorithm. In each scan of fingerprint image, the algorithm marks the redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. After the fingerprint ridge thinning, marking minutiae points is relatively easy. For each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region, so a check routine requiring that none of the neighbors of a branch are branches is added.

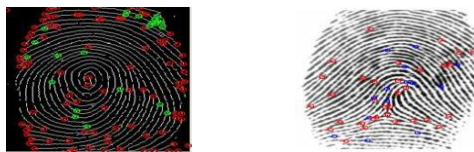


Fig. 8 Minutiae Point Extraction

Matrix and Key Generation from Minutiae Points

The key generation algorithm is as follows:

Assumptions

Mp – Minutiae point set

Sp – Size of Mp

KL-Key Length

Kv – Key Vector

Lk-Length of Key Vector

Z→ (X, Y) - Co-ordinate of a minutiae point.

Step 1: Read the Minutiae Points

Step 2: Find the point H with highest X+Y.

Step 3: Draw a line from origin (0, 0) to the H and call it as L.

Step 4: Sort the Minutiae points and store in an array A.

Step 5: Value= KL/Np
Vector = $KL\%Np$

Step 6: For i=1 to value
For j=1 to Sp

Read point X from Array A and Check the point whether it is above or below the line L.

If it is above the line or on the line put value as '0' else value is '1'. Store them in an array K.

Final Key: - Append the key vector of length vector to value of K.

V. Conclusion

Securing the information system becomes most challenging task because of the security issue. The conventional security system uses password or security key for authentication, but those password and security key can be easily stolen by the theft. To overcome these issues, biometrics of a person is used to secure the system. This paper proposed a method for generating cryptographic key using biometrics. In this Fingerprint pattern biometrics are used, which are stable throughout the person's lifetime. The cryptographic key is derived directly from the biometric data and it is not stored in the database .since it creates more complexity to guess the crypto keys and this scheme also ensure confidentiality to the data.

VI. References

- [1] Arul. P 1 , Shanmugam.A 2 , “ Generate a Key for AES using Biometric for VOIP Network Security”, journal of theoretical and applied Information technology.
- [2] Sunil V. K. Gaddam 1 and Manohar Lal 2, “Effecient Cancellable Biometric Key Generation Scheme for Cryptography” International Journal of Network Security, Vol.11, No.2, PP.57 {65, Sep. 201.}
- [3] B. Goode, “Voice Over Internet Protocol (VOIP)”. *Proceedings of three IEEE, VOL. 90, NO. 9*, Sept. 2002.
- [4] “Voice over Internet Protocol” from http://en.wikipedia.org/wiki/Voice_over_IP.
- [5] R. Ang, R. Safavi-Naini, L. McAven, “Cancellable key-based fingerprint templates,” ACISP 2005, pp. 242-252.
- [6] RSA (algorithm), [http://en.wikipedia.org/wiki/RSA_\(algorithm\)](http://en.wikipedia.org/wiki/RSA_(algorithm)).
- [7] RSA Data Security, Inc.The RSA Factoring Challenge. <http://www.rsa.com/rsalabs/node.asp?id=2092>.
- [8] R.L.Rivest, A.Shamir, and L.Adleman. “A Method for Obtaining Digital Signatures and Public-key Cryptosystems”, *Communications of the ACM*, **21(2)**, 120- 126, Febuary 1978
- [9] Principles of fingerprint (http://www.biometricnewsportal.com/fingerprint_biometrics.asp)
- [10] Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filterbank-based fingerprint matching",*IEEE Transactions on Image Processing*, vol. 9, no. 5, pp: 846-859, May 2000, Doi:10.1109/83.841531.