ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 3 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Iris Based Cryptosystems for Securing VoIP

[I]Vivekanand Verma, [II]Vinay Soni, [III]Laxmikant Tiwari, [IV]Dr. K N Singh
[I,II,III,IV]Assistant professor, Dept of IT, Dr. C. V. Raman University Bilaspur, India

Abstract
VoIP (Voice over Internet Protocol) is a growing technology that provide user to connect voice and video call to be made over the Internet or any other IP-based network. VoIP cost is typically cheaper or completely free compare than traditional phone cost to the user. VoIP converts analog signal from your phone into a digital signal that travels over the computer network then converts it digital signal to analog signal at the other end so you can talk to anyone with a traditional (PSTN) phone systems. VoIP also is referred to as Next Generation Voice Network, IP Telephony, Voice over Internet (VOI), IP Communications, Voice over Packet, Digital Phone and Voice over Internet Protocol. This paper will focus on VoIP security threats over the Internet or any other IP-based network. Securing VoIP system is more challenging compare than securing other data network over the public network. VoIP has a very different architecture compare than traditional (PSTN) phone systems. Cryptography is one of the best security technologies for computer data. In our discussion we proposed a Biometric-Crypto system which generates a cryptographic key from the fingerprints for Encrypting and decrypting the voice data packets for VoIP Security. If you are connecting VoIP communications then your communication are also vulnerable to hijacking or a man in the middle attack. Biometric-Crypto system is a way to help protect your privacy is to encrypt these conversations.

Keywords
VoIP, cryptography, PSTN, telephony, Fingerprint, Encryption, Decryption, VoI, Biometric cryptosystem.

I. Introduction

VoIP stands for Voice over Internet Protocol. VoIP is an advance technology that allows user to connect voice and video call to be made over computer networks like the Internet. Some VoIP application is support Video call and multimedia conference over computer networks like the Internet. VoIP is another way of making voice calls, with the difference of making the phone calls cheaper or completely free. It converts analog voice signals into digital data packets and supports real-time, two-way transmission of conversations using Internet Protocol (IP).
It supports real-time, two-way transmission of conversations using Internet Protocol (IP).
VoIP needs two types of protocols: signaling protocol and media protocols. Signaling protocols manage call setup and teardown. Examples of signaling protocols include H.323, SIP, MGCP, Megaco/H.248 and other proprietary protocols like UNISTIM, SCCP, Skype, CorNet-IP, etc. Media protocols manage the transmission of voice data over IP networks. Examples of media protocols include RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol), SRTP (Secure Real-time Transport Protocol) and SRTCP (Secure RTCP).

A. Symmetric Encryption

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

B. Asymmetric Encryption

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

C. Iris Recognition

Data acquisition is performed with a special camera (iris scanner) which is able to capture the iris of a person's eye [2]. Breakthrough work to create iris recognition algorithms required for image acquisition and matching were developed by J. G. Daugman [3, 4], University of Cambridge Computer Laboratory. Daugman's algorithms for which he holds key patents are the basis of all todays commercially used iris recognition systems.
The algorithm of filtrating information out of such an image of a person's eye involves several steps, which can be summarized as follows: First the iris has to be extracted out of the whole image of the person's eye. Therefore the center of the iris and the inner and outer boundaries has to be detected. This detection has to be performed carefully because of the dynamic dimension of the pupil and dilation of the person's eyelid. To solve this problem Daugman proposed a method called exploding circles". The main idea of this concept is that there are strong changes of brightness in the image at these boundaries which can be detected using circular integrals. In the beginning an initial center of the pupil is approximated. Then circular integrals are calculated. The derivation of such integrals is very high at the boundaries where the brightness changes drastically. So applying this method for an approximated center, radii to the boundaries between the pupil and the iris and between the iris and the sclera are calculated. These radii are then used to compute a new center of the pupil and the whole method is applied again until convergence is achieved.
In the next step so-called analysis bands" are defined for the extracted iris (in form of a ring). These bands are used to position

© All Rights Reserved, IJARCST 2014

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

points which are then explored using 2D Gabor filters. These 2D Gabor filters are designed to denoise the acquired signal. This process must not be confused with the smoothing of a signal. Then iris ring is unwrapped by mapping polar coordinates to Cartesian-coordinates which results in a rectangular image. In the rectangular image the radii of the previously defined analysis bands is fixed and every explored point is a center of a 2D Gabor wavelet. For this wavelet the coefficients are generated out of which two bits are extracted. This method is applied again until enough bits are extracted

D. Biometric Crypto Systems

Cryptography provides the secure manner of information transmission over the insecure channel. It authenticates messages based on the key but not on the user. It requires a lengthy key to encrypt and decrypt the sending and receiving the messages, respectively. But these keys can be guessed or cracked. Moreover, Maintaining and sharing lengthy, random keys in enciphering and deciphering process is the critical problem in the cryptography system. The above mentioned problem is solved by a Biometric cryptosystems. Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. [1]

II. Design Methodology

Images taken from iris database are used for feature extraction. From iris image 128 bit secret key is selected. This key is used to encrypt the data. The information that is to be sent to the channel is encrypted using this key. At the decryption phase original data is retrieved back. Randomness check is conducted for the key. Working model is shown in Image 1.

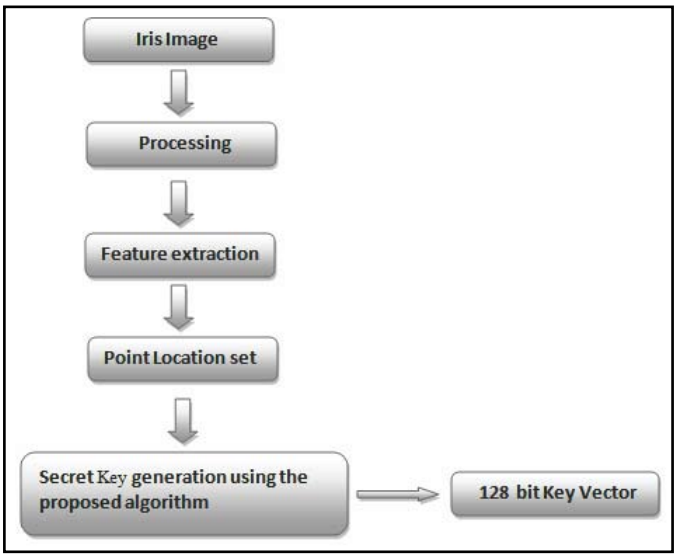


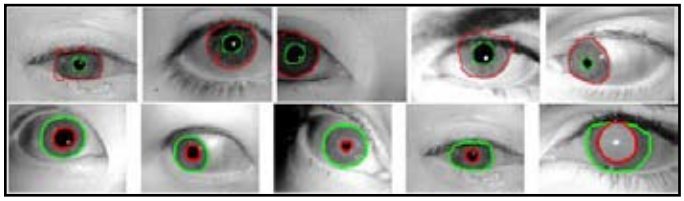
Fig. 1: Generate 128 bit secret key vector from Iris image

III. Key Generation

Iris feature extractions have a different phase. Phases are image scanning, image processing and image data are converting in to binary values. Data Processing consists of segmentation and normalization. Edge maps of the images are generated after these processes. From the normalized image key is generated. [15]

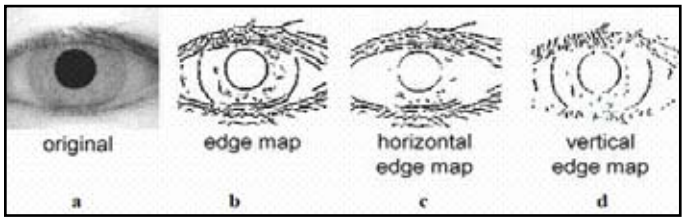
A. Segmentation

Segmentation is the process of dividing the whole image in to different segments. Set of pixel are called segments. The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze.[5,6] . It consists of estimation boundary and noise removal.



Regarding the basis methodologies, various innovations were proposed, as the use of active contour models, either geodesic (e.g., [8]), based on Fourrier series (e.g., [9]) and on the snakes model (e.g., [10]). Here, the previous detection of the eye is a requirement to properly initialize contours and the heavy computational requirements can also be regarded as a weak point. Also, modifications to known form fitting processes were proposed, essentially to deal with off-angle images (e.g., [11] and [12]) and to improve performance (e.g., [13] and [14]).

B. Normalization



In image processing, Normalization changes the range of pixel intensity values. It is a process of contrast stretching. Dogman's Rubber Sheet Model is utilized for the transformation Process, in which iris image is converted to rectangular image. It consists of two resolutions namely radial and angular resolution.
Normalization transforms an n- dimensional grayscale image

$I : \{\mathbb{X} \subseteq \mathbb{R}^n\} \rightarrow \{\text{Min}, .., \text{Max}\}$ with intensity values in the range (Min, Max), into a new image

$I_N : \{\mathbb{X} \subseteq \mathbb{R}^n\} \rightarrow \{\text{newMin}, .., \text{newMax}\}$ with intensity values in the range (newMin, newMax).
The linear normalization of a grayscale digital image is performed according to the formula

$$I_N = (I - \text{Min})\frac{\text{newMax} - \text{newMin}}{\text{Max} - \text{Min}} + \text{newMin}$$

C. 128 bit key

Blocks of 128 bits should be generated. From these only one block of 12 bit is selected as the key. Randomness checking is done for that.

© 2014, IJARCST All Rights Reserved

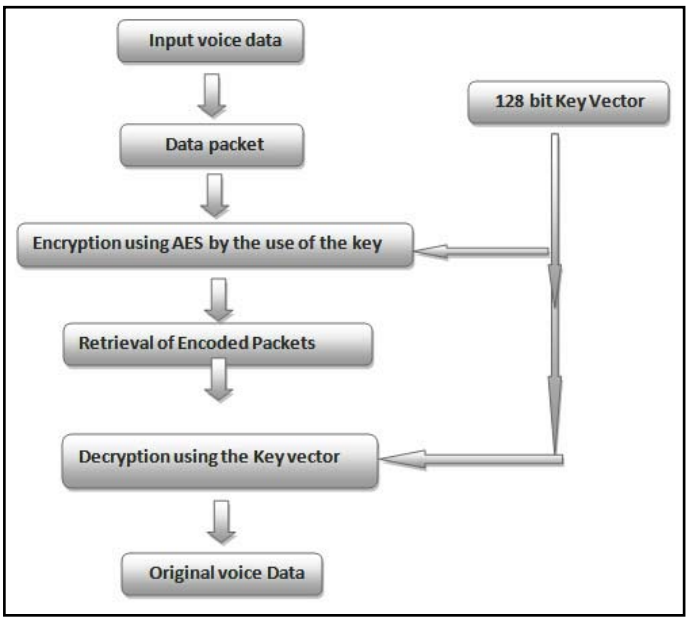


Fig. 2 : Encrypt and Decrypt using 128 bit Secret Key

D. Tests conducted to check the randomness of key

- Five tests are conducted to check the randomness. They are
- The Frequency (Monobit) Test,
- Frequency Test within a Block,
- The Runs Test,
- Tests for the Longest-Run-of-Ones in a Block,
- Non overlapping template match test.

In frequency monobit test proportion of zeros and ones are checked. It should be equal for the sequence to be random In frequency test within a block proportion of zeros and ones is checked within a block. The purpose of runs test is to determine whether the number of runs of one's which means checking the occurrence of continuous zeros or ones of various lengths. The purpose of longest runs of ones in a block test is to determine whether the occurrence of continuous zeros or ones of various lengths within a block. The purpose of none overlapping template match test is to detect generators that produce too many occurrences of a given non-periodic pattern.[8]

IV. Conclusion

Our papers have proposed a system which will encrypt. The VoIP data packets using cryptography with Biometrics based Key Generation technique. 128 bit Secret key is generated from iris image. In future our model Increase levels security on VoIP communication. Our proposed system Try to reduce dependency on old security method for VoIP communication on public network.

References

Journal Papers:

[1]. *Sayani Chandra, Sayan Paul, Bidyutmala Saha, Sourish Mitra "Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 1 (May. - Jun. 2013), PP 16-22*

[2]. *K. Bowyer, K. Hollingsworth, and P. Flynn, "Image understanding for iris biometrics: a survey," Computer Vision and Image Understanding, no. 110, pp. 281{307, 2008.*

[3]. *J. Daugman, "The importance of being random: Statistical principles of iris recognition,"*

[4]. *Pattern Recognition, vol. 36, no. 2, pp. 279-291, 2003.*

[5]. *---------, "How Iris Recognition Works," IEEE Trans. CSVT, vol. 14, no. 1, pp. 21-30,2004.*

[6]. *Barghout, Lauren, and Lawrence W. Lee. "Perceptual information processing system." Paravue Inc. U.S. Patent Application 10/618,543, filed July 11, 2003.*

[7]. *Linda G. Shapiro and George C. Stockman (2001): "Computer Vision", pp 279-325, New Jersey, Prentice-Hall, ISBN 0-13-030796-3*

[8]. *Sruthi B. Asok1, P. Karthigaikumar2, Sandhya R3, Naveen Jarold K4, Siva Mangai5 "IRIS BASED CRYPTOGRAPHY" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2013*

[9]. *Ross, A., Shah, S.: Segmenting non-ideal irises using geodesic active contours. In: Proceedings of the IEEE 2006 Biometric Symposium, U.S.A (2006) 1–6*

[10]. *Daugman, J.G.: New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, vol. 37, no. 5 (2007) 1167–1175*

[11]. *Arvacheh, E., Tizhoosh, H.: A study on Segmentation and Normalization for Iris Recognition. Msc dissertation, University of Waterloo (2006)*

[12]. *Zuo, J., Kalka, N., Schmid, N.: A robust iris segmentation procedure for unconstrained subject presentation. In: Proceedings of the Biometric Consortium Conference. (2006) 16*

[13]. *Vatsa, M., Singh, R., Noore, A.: Improving iris recognition performance using segmentation, quality enhancement, match score fusion, and indexing. IEEE Transactions on Systems, Mans and Cybernetics - B, vol. 38, no. 3 (2008) ??–??*

[14]. *Liu, X., Bowyer, K.W., Flynn, P.J.: Experiments with an improved iris segmentation algorithm. In: Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies. (2005) 118–123*

[15]. *Dobes, M., Martineka, J., Dobes, D.S.Z., Pospisil, J.: Human eye localization using the modified hough transform. Optik, vol. 117 (2006) 468–473*

Websites and PDFs:

[16]. *Ao.Univ.-Prof. Dr. Andreas Uhl "Iris{Based Biometric Cryptosystems" University of Salzburg Jakob Haringer Str. 2 5020 zburg, AUSTRIA Salzburg, im November 2008*

[17]. *http://en.wikipedia.org/wiki/Normalization_(image_processing)[8]*

[18]. *http://www.pccegoa.org/pcce/etc/synopsysETCprojects.htm*

© All Rights Reserved, IJARCST 2014