International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

# Secure VoIP Network by Fusion of Irises

**S. Bhuvaneshwari[1], Dr. P. Arul[2]**

[1]PhD Scholar, Department of CS, GAC, TRICHY-22

[2]Assistant Professor, Department of CS, GAC, TRICHY-22

**Abstract:** ***In a world that is more digitally connected than ever before faces an inevitable problem of securing our most integrated data and message..Currently, Voice over Internet Protocol (VoIP) becomes one of the most dominant and attracting technologies in the world of telecommunications. The chief problem is to protect our data in a unique way that could only be worked upon by the sender and the recipient. Using biometric we can generate an exclusive key that will be unique for each and every individual. Here we propose to make a mutual contribution of the participants(sender and receiver) to share their biometrics to have very secured VoIP communication. After generating the keys from the irises of the two participants, this will be combined with the pseudo random numbers, to produce a strong encryption keys . And the resulting key can be used for encrypting our message. This method is proposed because even if one the iris biometric is stolen, the attacker can't access the data unless the data encrypted with multimodal biometric key . And for more security Therefore billions of unique keys can be generated, making VoIP technology hard for an attacker to guess the key . This key act as a symmetric key for both encryption and decryption. This proposed system is composed of two modules 1)Feature extraction of Iris 2)Cryptographic key generation. 3)Fusion of iris 4)Fusion of PNRG with Fused iris key.***

**Keywords:** Biometrics, Cryptosystem, Iris Extraction, Minutiae point, Fusion

## 1. Introduction

Today with exponential increase of **Voice over Internet Protocol** (VoIP) technologies it arises as dominant technology in the World of telecommunications. Because it allows any person to make a phone call through internet connection.

### A. VoIP Communication

In VoIP technology, the voice signal is first separated into frames, which are then stored in data packets, and finally it transport over IP network using voice communication protocol [1]. Usually both the caller and callee send and receive phone call over the internet. Security issues are most important and integral part of VoIP applications development. The main obstacles that prevent VoIP businesses are the security issues that prevailed in this technology, i.e. the hackers/intruders can intercept incoming and outgoing phone numbers, break in someone's voice mail, or even listen to the confidential conversations over IP networks [2].Many research organizations are trying to tackle the issue to have a secured VoIP communication. Instead of being the digital information is packetized and transmitted over a network, these data packets are encrypted and decrypted by Biometric cryptosystems make secure transmission.

### B. Biometric Encryption

This is the one of the safest way to provide confidentiality and integrity to the VoIP data. Biometric technique [3] provides the distinct characteristics of a person which is always prevalent. A person's individuality can be differentiated from one or more behavioral or physiological features by this authentication technique. Various techniques that are under the biometric research include facial, palm prints, retinal and iris scans, and hand geometry, signature capture and vocal features [4]. Biometric-Crypto system is a method of integrating biometrics features with cryptographic system [5]. In this biometrics-based key generation technique, a biometric input is obtained. From the unique biometric identity of a person, the keys can be generated, and with the help of these keys the VoIP data can be encrypted.

### C. Iris Biometric Key Generation

Among the biometric key generation methods iris biometric is considered to be one of the most accurate and robust. The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Iris features can be easily extracted from eye images [6].Each individual has a uniquely different and highly intricate iris pattern in each eye, which is completly developed at a very young age and remains unchanged throughout one's lifetime. This is combined with the fact that iris patterns are almost impossible to replicate, makes iris scanning one of the most secure and reliable biometric techniques available. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database [7]. Here John Daugman's iris recognition algorithm is used to generate iris code. He invented the Iris Code, a 2D Gabor wavelet-based iris recognition algorithm that is the basis of all publicly deployed automatic iris recognition systems and which has registered more than a billion persons worldwide in government ID programs. This biometric template contains an objective mathematical representation of the unique information stored in the iris code.

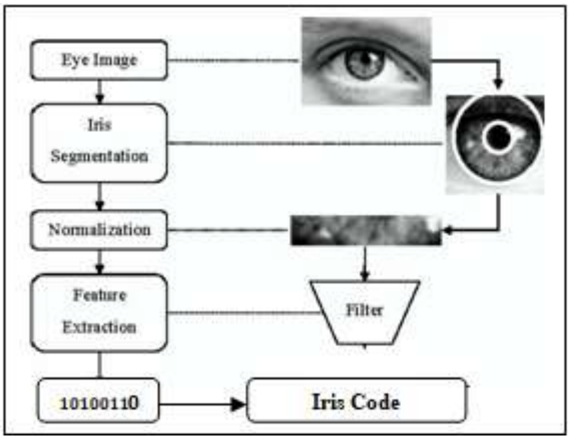


**Figure 1:** Iris code Extraction process

**D. Multibiometrics System**

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems. Biometric identification systems which use or are capable of using a combination of two or more biometric modalities are called multimodal biometric systems[8]. Some of the limitations can be overcome by the use of multimodal biometric systems of same biometric trait.

Multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user [9]. It make a mutual contribution of the participants to share their biometrics to have very secured VoIP communication. In cost wise the addition of another type biometric technology can drive up the price of the solution. Multimodal Biometrics of different traits is difficult to acquire and implement, since different algorithm are needed to retrieve the data from each of the biometrics.

## 2. Literature Review

The proposed work is inspired from a number of researches which are related to biometric cryptography key generating techniques. The VoIP calls are also vulnerable to hijacking or a man in the middle attack [10]. In such a scenario, an attacker would intercept a connection and modify call parameters. This is an especially scary attack, since the participants likely wouldn't notice a change. One way to protect your privacy is to encrypt these conversations so that they aren't simply floating around out there for potential hackers to latch onto [11]. An algorithmic function's strength and the key's secrecy determine how secure the encrypted data is. In most cases, the algorithm isn't the secret; it's known to the public. The secret is the key values taken from the biometric and combine with a random sequence forms the keys for encryption/decryption. John Daughman algorithm resulted with the genuine iris codes with a 99.5 percent achievement rate, which upshot with 140 bits of biometric key which is sufficient for a 128-bit AES. In the current development, biometric cryptosystems [12] take advantage from the strong points of both fields. In such systems, while cryptography endows with high and modifiable security levels, biometrics provides non-repudiation and removes the requirement to memorize passwords or to carry tokens [13].Since Human iris possesses genetic independence and contains extremely information-rich physical structure and unique texture pattern which makes it highly complex enough to be used as a biometric key. Statistical analysis reveals that the iris is the most mathematically unique feature of the human body because of the hundreds of degrees of freedom it gives with the ability to accurately measures its texture [14]. Reliable biometric verification and identification techniques based upon iris patterns have been presented by John Daugman [15], Wildes et al. [16], Boles [17]. One important characteristic of the iris is that, it is so unique that no two irises are alike, even among identical twins, in the entire human population [18]. The human iris, an annular part between the pupil (generally, appearing black in an image) and the white sclera has an extraordinary structure and offers a plenty of interlacing minute characteristics such as freckles, coronas, stripes and more. These visible characteristics, which are generally called the texture of the iris, are unique to each subject [19].

In cryptography, the use of pseudorandom number generators is insecure. When random values are required in cryptography, the goal is to make a message as hard to crack as possible, by eliminating or obscuring the parameters used to encrypt the message (the key) from the message itself or from the context in which it is carried [20]. Pseudorandom sequences are deterministic and reproducible; all that is required in order to discover and reproduce a pseudorandom sequence is the algorithm used to generate it and the initial seed. To overcome this difficulty we are fusing the pseudo random sequence with the biometric iris code which will be more secure for data that transmit over open unsecure network.

## 3. Proposed Approach for Generating A Biometric Iris Key

The proposed system includes five main modules: 1) Biometric image acquisition, 2) Segmentation, 3) Iris Normalization, 4) Feature point extraction of iris 5)Key Generation. The algorithm is based on the methods given by Daugman [15] .The proposed solutions for each of these modules are described in the following subsection with more detail.

**A. Biometric Image Acquisition**

In the iris recognition process the first step is the image acquisition of a person's eye. The eye image is captured in the near infrared light with the wavelengths between 700–900 nm. Usually special infrared illuminators and band pass lens filters are used to acquire a image of good quality. The infrared light reveals the detailed structure of the iris better than the visible [15].

**B. Segmentation**

Iris segmentation is an essential module in iris recognition because it defines the effective image region used for subsequent processing such as feature extraction. Generally, the process of iris segmentation is composed of two steps 1) Estimation of iris boundary and 2) Noise removal. Below figure.1 the process of iris code extraction from an iris image. Figure 1 Iris code Extraction process.

- ***Estimation of iris boundary:*** For boundary estimation, the iris image is first fed to the canny algorithm which generates the edge map of the iris image. The detected edge map is then used to locate the exact boundary of pupil and iris using Hough transform.

***Canny edge detection*** The Canny edge detection operator was developed by John F. Canny in 1986. It uses a multi-stage algorithm to detect a wide range of edges in images. Canny edge detection starts with linear filtering to compute the gradient of the image intensity distribution function and ends with thinning and thresholding to obtain a binary map of edges. One significant feature of the Canny operator is its optimality in handling noisy images as the method bridges the gap between strong and weak edges of the image by connecting the weak edges in the output only if they are connected to strong edges. Therefore, the edges will probably be the actual ones. Hence compared to other edge detection methods, the canny operator is less fooled by spurious noise [21].

***Hough Transform***

The classical Hough transform was concerned with the identification of lines in the image, but later, the Hough transform has been extended to identify positions of arbitrary shapes, most commonly circles or ellipses. From the edge map obtained, votes are cast in Hough space for the parameters of circles passing through each edge point. These parameters are the centre coordinates *x* and *y*, and the radius *r*, which are able to define any circle according to the equation,

$$x^2 + y^2 = r^2$$

A maximum point in the Hough space will correspond to the radius and centre coordinates of the circle best defined by the edge points.

- ***Isolation of Eyelids and Eyelashes:*** In general, the eyelids and eyelashes occlude the upper and lower parts of the iris region. In addition, specular reflections can occur within the iris region corrupting the iris pattern. The removal of such noises is also essential for obtaining reliable iris information. Eyelids are isolated by fitting a line to the upper and lower eyelid using the linear Hough transform. A second horizontal line is then drawn, which intersects with the first line at the iris edge that is closest to the pupil; the second horizontal line allows maximum isolation of eyelid region. The eyelashes are quite dark compared with the surrounding eyelid region. Therefore, thresholding is used to isolate eyelashes.

## C. Iris Normalization

Once the iris image is efficiently localized, then the next step is to transform it into the rectangular sized fixed image. The transformation process is carried out using the Daugman's Rubber Sheet Model.

- Daugman's Rubber Sheet Model: Normalization process involves unwrapping the iris and converting it into its polar equivalent. It is done using Daugman's Rubber sheet model[21] and is shown in *figure*2.

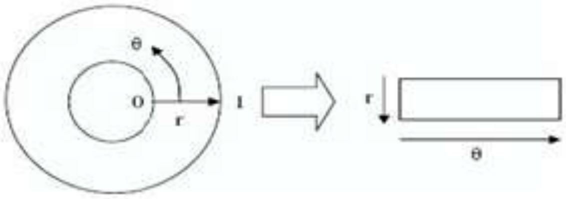

**Figure 2:** Daugman's Rubber Sheet Model

For every pixel in the iris, an equivalent position is found out on polar axes. The process comprises of two resolutions: Radial resolution, which is the number of data points in the radial direction and Angular resolution, which is the number of radial lines generated around iris region. Using the following equation, the iris region is transformed to a 2D array with horizontal dimensions of angular resolution and vertical dimension of radial resolution.

$$I[x(r,\theta), y(r,\theta)] \rightarrow I(r,\theta)$$

Where, $I(x, y)$ is the iris region, $(x, y)$ and $(r, \theta)$ are the Cartesian and normalized polar coordinates respectively. The range of $\theta$ is $[0\ 2\pi]$ and $r$ is $[0\ 1]$. $x(r, \theta)$ and $y(r, \theta)$ are defined as linear combinations set of pupil boundary points. The formulas given in the following equations perform the transformation,

$$x(r,\theta) = (1-r)x_p(\theta) + x_i(\theta)$$
$$y(r,\theta) = (1-r)y_p(\theta) + y_i(\theta)$$
$$x_p(\theta) = x_{p0}(\theta) + r_p Cos(\theta)$$
$$y_p(\theta) = y_{p0}(\theta) + r_p Sin(\theta)$$
$$x_i(\theta) = x_{i0}(\theta) + r_i Cos(\theta)$$
$$y_i(\theta) = y_{i0}(\theta) + r_i Sin(\theta)$$

where $(x_p,y_p)$ and $(x_i,y_i)$ are the coordinates on the pupil and iris boundaries along the $\theta$ direction, =( $x_{p0}, y_{p0}$), ( $x_{i0}, y_{i0}$) are the coordinates of the pupil and iris centers[21].

## D. Feature point Extraction of iris:

The normalized 2D form image is broken up into 1D signal, and these signals are used to convolve with 1D Gabor wavelets. The frequency response of a Log-Gabor filter is given as,

$$G(f) = \exp\left(\frac{-(\log(f/f0))^2}{2(\log(\sigma/f0))^2}\right)$$

Where $f_0$ represents the centre frequency, and σ gives the bandwidth of the filter [21]. The Log-Gabor filter outputs the biometric feature (texture properties) of the iris.

We extract minutiae-based features from the iris images of both sender and receiver. For the reference in our subsequent discussion, we denote them as follows.

*$I_s$ = Set of minutiae points extracted from sender's iris.*
*=$[m^s_1, m^s_2, \ldots m^s_{Ns}]$; where $m^s_i=(x_i,y_i)$, $m^s_i$ is the $i^{th}$ minutiae points of sender's iris, i = 1 to $N_s$*
*and $N_s$ is the size of $I_s$*

*$I_r$ = Set of minutiae points extracted from sender's iris.*
*=$[m^r_1, m^r_2, \ldots m^r_{Nr}]$; where $m^r_i=(x_i,y_i)$, $m^r_i$ is the $i^{th}$ minutiae points of receiver's iris, i = 1 to $N_r$*
*and $N_r$ is the size of $I_r$*

Note that, for all iris images, the selection of minutiae points are according to their quality value, it will be selected and the rest will be discarded.

### E. Fusion of Iris Code Using Feature Level Fusion

In feature level fusion, signals coming from different biometric channels are first processed after which the feature vectors are extracted separately from each biometric trait. The feature vectors are then combined to form a composite feature vector using a specific fusion algorithm and then used for further classification. In feature level fusion, some reduction techniques need to be used in order to select only the useful features.

Features contain richer information of biometric traits. Thus fusion at the feature level provides better recognition results. It has also been observed that feature level fusion provides more accuracy when the features of different biometric modalities are compatible with each other.

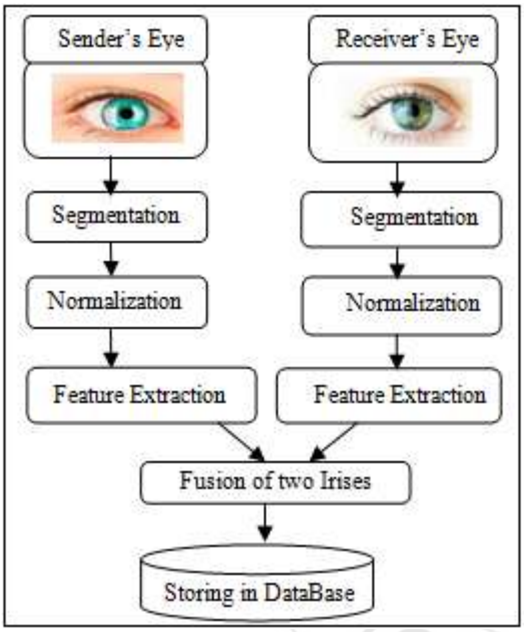


**Figure 3:** Iris code Fusion process

### F. Key Generation

Our basic design depends on two factors 1) Fusion of Iris Code and 2) Fusion of PRN. If the biometric becomes known, this does not help the attacker, because the key is fused with randomly generated numbers. We make the key completely not dependent on the iris biometric, as this cannot be kept very secret. However, it is still costly to steal an iris code [23]. A near-infrared camera is needed and it is difficult to capture a person's iris image close-up without being noticed; most likely, iris code thefts will be conducted using subverted equipment in apparently genuine settings. In such a threat model, the attacker would get a password too, if one were in use; so we must rely completely on the token being tamper-resistant. In the following section, a key generation system is depicted based on the algorithm using minutiae points of iris biometric and pseudo random numbers.

***Algorithm:***

Mp → Minutae point set
Kl → Key Length
Np → Size of minutae point set
S → Seed value
Sl → Seed limit
M → (x, y) coordinate of a minutae point
Kv → Key vector

***Steps involved:***

**Step 1:** Representation of the minutiae points extracted:

$$Mp\ \{mi\}i = 1.....Np \quad (1)$$

**Step 2:** Definition of the key vector (initial):

Kv = {xi : p(xi)} where, i = 1 ... Kl

$$p(x) = Mp[I \% Np] + Mp[(i + 1) \% Np] + S \quad (2)$$

**Step 3:** The changing values of S is given as follows where the initial value equals the number of minutiae points:

$$S = Kv(i) \% S1, -1 < i < Kl \quad (3)$$

**Step 4:** Conversion of the key vector (Kv) to a matrix Km of size $\frac{Kl}{2} * \frac{Kl}{2}$ as follows ;$K_{m=}\frac{(aij)Kl}{2} * \frac{Kl}{2}$

**Step 5:** Generation of the key vector (intermediate):

KIV = {Ki : (m(Ki)} where, i = 1.... ......Kl,

$m(k)=|A_{ij}|, A_{ij=}K_m$ I,j ; i+ size, j+ size,

$$-1< i < \frac{Kl}{2} \quad (5)$$

***Note:*** The submatrix Aij is generated from the key matrix

**Step 6:** Generation of the private key (final key vector):

$$Kv = 1, \text{ if } KIV[i] > \text{mean (KIV), else } 0 \quad (6)$$

Thus the key have generated for cryptography process for VoIP network using minutiae points of sender's and receiver's iris. Here we tackled the most difficult problem of merging cryptography with biometrics. On the basis of this system, it may be inferred that an attacker, in case of a biometric cryptosystem, will be unable to generate a key without having the complete knowledge of the key.

IV Conclusion

With the increasing need for secure transmissions over unsecured channels, the integration of biometrics with cryptosystem has become one of the secure channels for passing the confidential data. Thus the proposed method encrypts voice packets biometrically, to have a secured VoIP Communication. Integration of the iris biometric with cryptographic is well-suited for this VoIP technology, which provide a better approach for a secured transmission of packets in between one network to another network. If unfortunately one the iris biometric is stolen, the intruder will not able to access the data since iris of sender and receiver are fused ,and also pseudo random numbers are fused with the biometric key. Therefore billions of unique keys can be generated, making VoIP technology hard for an attacker to guess the key.

## References

[1] "Voice over Internet Protocol" from http://en.wikipedia.org/wiki/Voice_over_IP

[2] Persky, D. (2007). VoIP Security Vulnerabilities. *Sans Institute 2007.* Retrieved July 13, 2009

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle "Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal, vol. 40, pp. 614-634, 2001.

[4] T. Zhang, X. Li, D. Tao, and J. Yang, "Multi-modal biometrics using geometry preserving projections", Pattern Recognition, vol. 41, no. 3, pp. 805-813, 2008.

[5] Yan Yan and Yu-Jin Zhang, “Multimodal Biometrics Fusion Using Correlation Filter Bank", in proceedings of 19th International Conference on Pattern Recognition, pp. 1-4, Tampa, FL, 2008.
[6] S. C. Chong, A. B. J. Teoh, and D. C. L. Ngo, “Iris Authentication Using Privatized Advanced Correlation Filter,” in ICB, pages 382–388, 2006
[7] A. Czajka and A. Pacut, “Iris recognition with adaptive coding”,*Rough Sets and Knowledge Technology*, *Lecture Notes in Artifical Intelligence*, vol. 4481, Springer, 2007, pp. 195–202. [8]
[8] P. Balakumar and R. Venkatesan, Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris , IJCSI International Journal of Computer Science Issues, 8(5), 2011, 349-356.
[9] Feng Hao, Ross Anderson and John Daugman, "Combining Crypto with Biometrics Effectively", IEEE Transactions on Computers, vol. 55, no 9, 2006.
[10] Peter Thermos; Ari Takanen, “Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures”, Addison-Wesley Professional, August 2007, ISBN-10: 0-321-43734-9.
[11] P.Arul, Dr.A.Shanmugam, "Generate a Key for AES Using Biometric for VOIP Network Security", Journal of Theoretical and Applied Information Technology, vol. 5, no.2, 2009.
[12] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain,“Biometric Cryptosystems Issues and Challenges”, in Proceedings of the IEEE, vol. 92, pp. 948-960, 2004.
[13] Jain AK, Bolle R, Pankanti S. Biometrics: personal identification in network society. Kluwer Academic Publishers; 1999.
[14] Daugman John. High confidence visual recognition of persons by a test of statistical independence. IEEE Trans Pattern Anal Mach Intell 1993;15(11):1148–61.
[15] Daugman JG. Statistical richness of visual phase information: update on recognizing persons by iris patterns. Int J Comput Vision 2001;45(1):25–38.
[16] Wildes RP.Iris recognition: an emerging biometric technology. Proc IEEE 1997;85(9):1348–63.
[17] Boles WW. A wavelet transform based technique for the recognition of the human iris. In: Proceedings of the international symposium on signal processing and its application, ISSPA, Gold Coast, Australia; August 1996. p. 25–30.
[18] Debnath Bhattacharyya, Poulami Das,Samir Kumar Bandyopadhyay and Tai-hoon Kim, "IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition", International Journal of Database Theory and Application, vol. 1, no. 1, pp. 53-60, December 2008.
[19] J. Daugman, “Statistical Richness of Visual Phase Information: Update on Recognizing Persons by Iris Patterns,” International Journal of Computer Vision, vol. 45, no. 1, pp. 25-38, 2001.
[20] https://en.wikipedia.org/wiki/Pseudorandomness
[21] Bremananth R and Chitra A, „An efficient biometric cryptosystem using autocorrelators‟ International Journal of Signal Processing 2;3, pp.158-164, 2006..
[22] John Daugman, “How Iris Recognition Works”, in Proceedings of International Conference on Image Processing, vol.1, pp. I-33- I-36, 2002.
[23] Beng.A, Jin Teoh and Kar-Ann Toh, "Secure biometric-key generation with biometric helper”, in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications, pp.2145-2150, Singapore, June 2008.