International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 12 254 – 257

Cryptographic Key generation using Sclera and Finger Print: Proposed Method

Shilpa Das
Department of Electronics and Communication
Vidya Academy of Science and Technology
Trivandrum, India.
shilpagiresh@gmail.com

Arya C
Department of Electronics and Communication
Vidya Academy of Science and Technology
Trivandrum, India.
aryachandradas06@gmail.com

***Abstract*—**Need for information security and privacy is increasing in recent times. Cryptography is intended to ensure the secrecy and authenticity of the message. The long cryptographic keys are very difficult to remember also protecting its confidentiality is one of the major issues to be deal with. These problems can be solved by integrating Biometrics with cryptography. Since biometric identifiers are unique to individuals, they are more reliable in verifying and identifying than knowledge based methods. Biometrics based authentication systems are progressively acquiring more attention in the field of research. Conventional techniques depend upon biometric features like face, fingerprint, iris, voice etc. In this paper we propose a method for cryptographic key generation fusing Finger print and Sclera.

Keywords*-Cryptography; Biometrics; Sclera; Finger Print*

*****

I. INTRODUCTION

The inability of humans to generate and remember strong secrets makes it difficult for people to manage cryptographic keys. Need for information security and privacy is increasing in recent times. For this purpose, biometric authentication is used in several applications and it is progressively acquiring more attention in the field of research. Several biometrics like fingerprint, iris, retina, etc., are used in rendering security to the information or key. The generation of cryptographic key from biometrics is used generally to secure the system. Biometric based cryptographic key generation methods are supposed to be safe and accurate, since these biometric identifiers are unique no need to remember the long keys generated for cryptographic method[1]. Several papers are proposed for biometric based cryptographic key generation methods. Biometrics has undergone intense scrutiny and the results are in - when properly deployed, biometrics work well and are safe, secure, and accurate. In this paper we propose a method fusing two biometric features that is Sclera and Finger Print.

Cryptographic keys are symmetric or asymmetric. Symmetric encryption requires only one key, which is used to encrypt and decrypt data. Asymmetric encryption uses two different keys: one for encryption and one for decryption. The length of a key is normally expressed in bits. A longer key makes it more difficult to crack the encrypted data; however, a longer key results in longer time periods to perform encryption and decryption processes. Several cryptographic techniques like DES, AES and public key architectures like RSA are widely used for the authentication purpose.

The characteristic feature of cryptographic security is conditioned by an authentication step that depends on long pseudo-random keys (128 bits in symmetric encryption), which are very impossible to keep in mind. This feature of inability to remember cryptographic keys has been restraining the security of systems for a long time. The inability of human users to remember powerful cryptographic keys has been a feature restraining the security of systems for decades. It's the natural tendency of humans to set passwords that are usually recognized or deduced by any social engineering methods. Typically people usually store keys in a place that is insecure and can possibly be shared among users and therefore it is not capable of ensuring non-repudiation[2]. Moreover it's a natural human tendency to use same keys or password for a variety of applications and as a result, if one system is hacked it is very easy to hack all the systems corresponding to that key[1]. This practically reduces the security privacy and makes the work easy for the hacker. Cryptographic techniques when combined with the biometric approach are used to solve these problems and provide security. The cryptographic keys are produced from the biometric data and are used in the authentication checking [2].

II. SCLERA AND FINGER PRINT BIOMETRICS

Biometric authentication uses data taken from measurements of a person's body, such as fingerprints, faces, irises, sclera, voice prints, and hand-written signatures and so on, to identify individuals by means of image processing. Such data is unique to the individual and remains throughout one's life. It is important to have reliable personal identification due to growing importance of information technology [3].

The sclera is the part of the eye commonly known as the "white." It forms the supporting wall of the eyeball, and is continuous with the clear cornea. The sclera is covered by the conjunctiva, a clear mucus membrane that helps lubricate the eye. It is thickest in the area surrounding the optic nerve. The sclera is made up of three divisions: the episclera, loose connective tissue, immediately beneath the conjunctiva; sclera proper, the dense white tissue that gives the area its colour; and the lamina fusca, the innermost zone made up of elastic fibers. Human eye image is shown figure 1below.

The sclera forms the posterior five-sixths of the connective tissue coat of the globe. It is continuous with the dura mater and the cornea, and maintains the shape of the globe, offering resistance to internal and external forces, and provides an attachment for the extraocular muscle insertions. The sclera is perforated by many nerves and vessels passing through the posterior scleral foramen, the hole that is formed by the optic nerve [3].

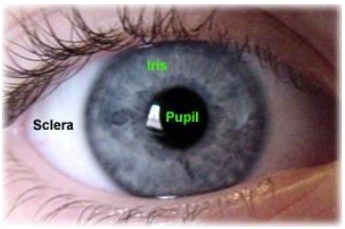

Figure 1: Human Eye image

At the optic disc the outer two-thirds of the sclera continues with the dura mater (outer coat of the brain) via the dural sheath of the optic nerve. The inner third joins with some choroidal tissue to form a plate (lamina cribrosa) across the optic nerve with perforations through which the optic fibers (fasciculi) pass. The thickness of the sclera varies from 1mm at the posterior pole to 0.3 mm just behind the rectus muscle insertions. The sclera's blood vessels are mainly on the surface. Along with the vessels of the conjunctiva (which is a thin layer covering the sclera), those in the episclera render the inflamed eye bright red. Sclera based cryptographic key generation methods offers several benefits over other eye-based biometrics that makes it well-suited for noncompliant recognition situations [3].

A fingerprint is the feature pattern of one finger. Finger print identification has been used as a means of positive identification methods over decades. The standing scientific principle, no two separate fingerprints have ever found to be same, this theory has never been disproved. Each fingerprint contains minutiae or ridge characteristics. Fingerprints are identified to individuals by examining and comparing the ridge characteristics of two different fingerprint impressions to determine if these characteristics occupy the same relative area and position[4].

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.

Figure 2: Arch Pattern

Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.

Figure 3: Loop Pattern

Whorl: Ridges form circularly around a central point on the finger. The Whorl pattern is shown in Figure 4.

Figure 4: Whorl Pattern

The loop is by far the most common type of figure print .The human population has figure prints in the following percentages. Loop – 65 % Whorl -30 % Arch - 05%[5].

In this approach fingerprint and sclera is used as a biometric parameter for generation of encryption key. In this proposed scheme both sender and receiver extract minutiae points from their own sclera, The minutiae points are

 ISSN: 2321-8169
254 – 257

transformed into a cancelable form called cancelable template[9]. The cancelable templates are exchanged between them using steganography, for steganography the cover image used is the finger print of both sender and receiver. The minutiae points collected from sclera and fingerprint an effect cryptographic key is generated, and is shared through a secure communication channel.

III. PROPOSED METHOD

The conceptual diagram of the proposed framework is depicted in Figure .Firstly, the Sclera veins are identified and its feature extracted, binary values assigned for sender's sclera feature extraction. These binary values are encoded with sender's fingerprint. Sender's finger print is used as a cover image for steganographicencoding[6]. Minutie points are extracted from sender's fingerprint. The encoded binary values are transmitted to the receiver side through a secure communication channel and vice versa. At the sender side the binary data received from the receiver is decoded and a secure cryptographic key is generated. The key generated from the sender and reciver side also shares through a secure communication channel.

A. Feature Extraction

Feature extraction is mainly applied in pattern identification in picture processing to diminish the dimension of a picture. At the point when a picture is specifically used for transforming, it is difficult to treat the huge data information of a image. And afterward that input information are transformed to its reduced kind of features which is experienced as the feature vector. At the point when input information is transformed in to set of features is known as the feature extraction. Depending on the physiological status of a person (for example, tiredness or weariness or non exhaustion), the vessels patterns could have different thicknesses at different times, because of the enlargement and choking of the vessels. In this way, vessel thickness is not a stable pattern for recognition[7]. Likewise, some thin vessels patterns may not be visible at all times. The vascular pattern could have different thickness at different times, because of dilution and constriction of the vessels, Therefore, vessel thickness is not a stable pattern for recognition[8]. In addition, some very thin vascular patterns may not be visible at all time. In this paper, local binary patterns are to be used to extract the feature.in this method mainly divide the image into the cell, after that each pixel value is taken from the cell. Then it will calculate the centroid value and this value will be compare with the each neighbor values, if the centroid value is greater than that the neighbor value it will be assign as the 1 otherwise it will be 0.these value should be converted into a decimal value for the feature extraction.

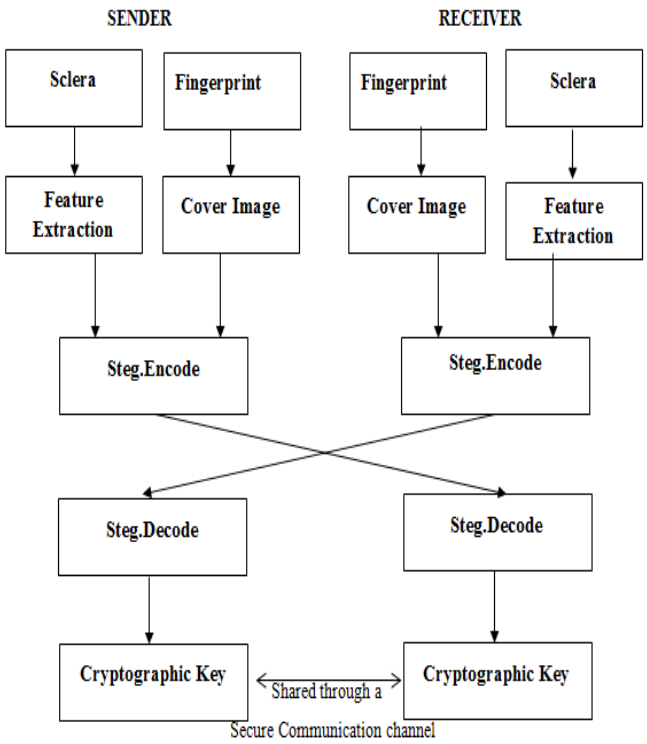

Figure 5: The conceptual diagram of the proposed frame work.

B. Minutia Extraction from fingerprint

The traditional methods of minutia extraction from fingerprint consist of Binarization, thinning and minutiae detection. In binarization the gray scale image is converted into binary image using some rectangular mask. The main objective behind thinning process is to find the ridges of one pixel width. The process consists of successive erosions until a set of connected lines of unit-width is reached. The lines are also called skeletons. From the binary thinned image, the minutia are detected by using 3x3 pattern masks. Binary values are assigned for this minutia points[6].

C. Steganographic encoding

The cancelable template of one party (say sender) needs to be sent through a shared communication channel to other party (say receiver) and vice versa. Sender (and receiver) uses steganography-based data hiding technique to hide the cancelable template data that is obtained from the sender's sclera image into a cover image(sender's finger print)[10].The cancelable template is converted into binary stream ($s_1,s_2,s_3,...s_L$), where L is the number of bits in cancelable template after the conversion, which is to be hidden into cover image using LSB steganography.

D. Steganographic decoding

In this phase, hidden data are extracted from the stego image.In this proposed paper the cancelable template obtained from the reciver side will be decoded for cryptographic key generation.

E. Cryptographic Key Generation

The final process of the proposed technique is the creation of K-bit cryptographic key from the obtained receiver's biometrics. The binary value obtained from the receiver side is represented by R_c.

$$R_c = [R_{c1}, R_{c2}, R_{c3}, \ldots\ldots\ldots\ldots\ldots R_{cn}]$$

Similarly for the receiver side

$$S_c = [S_{c1}, S_{c2}, S_{c3}, \ldots\ldots\ldots\ldots\ldots S_{cm}]$$

The k- bit cryptographic key generated in the sender side by

$$K_S = R_{c1} \oplus \ldots\ldots\ldots\ldots \oplus R_{cn}$$

The length of each component key (R_{cn}) shall be equal to the length required for K_s.

$$K_R = S_{c1} \oplus \ldots\ldots\ldots\ldots\ldots \oplus S_{cm}$$

The length if the generated keys K_s and K_R(256 bit) should be same.These keys are shared through a secure communication channel.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, a framework for sclera and finger print based cryptographic key generation is proposed, so as to provide better security. Securing the information system becomes most challenging task because of the increased number of theft. 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 this issues the fusion of biometrics can be used. In this paper the features obtained from the Sclera and fingerprint are used for cryptographic key generation. Experiments on real biometric data, particular fingerprints and Sclera, are being conducted and willbe reported in the near future.

REFERENCES

[1] Arun Ross and Anil K. Jain, "Multimodal Biometrics: An Overview", in proceedings of the 12th European Signal Processing Conference, pp.1221-1224, 2004.

[2] Nagar, A.; Nandakumar, K ; Jain, A. K.; Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose, Jan.2010

[3] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," Proceedings of the 2001 IEEE Symposium on Security and Privacy, pp. 202-213, May 2001.

[4] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, A. Rubin, "The Design and Analysis of Graphical Passwords," 8th USENIX Security Symposium, Washington, D.C., August 1999.

[5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, "Biometric Encryption™," Chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nicholls, pp. 649-675, 1999.

[6] L. Hong, A.K. Jain and S. Pankanti, "Can multibiometrics improveperformance?", in Proceedings of IEEE Workshop on AutomaticIdentification Advanced Technologies, pp. 59–64, NJ, USA, 1999

[7] Eliza Gail Maxwell; Tripti C.;,Int J of SCE, ISSn -2231-2307, Volume-3, Issue-4, September 2013

[8] Jain A. ; hong L.; bolle, R.;, IEEE trans and pattern analysis and machine intelligence, 19(4):302-314,1997

[9] JohnDaugman.;, IEEE Trans on circuits and systems for video technology, vol. 14, no. 1, January 2004.

[10] Thomas, N.L.; Yingzi Du.; Zhi Zhou.;, Proc. SPIE 7708, Mobile Multimedia/Image Processing, Security, and Applications 2010.