ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Cryptographic Key Generation using Retina Biometric Parameter

Mohammed Tajuddin
Department of Computer Science and Engineering,
Dayananda Sagar College of Engineering,
Bangalore.

C. Nandini
Department of Computer Science & Engineering,
Dayananda Sagar Academy of Technology and
Management, Bangalore

Abstract:- Crypto Biometrics system is recently emerging as an effective process to generate a cryptographic key. Conventional cryptographic key generation is using password which can be guessed or cracked. Further, the large size of strong key results in delay while encryption / decryption. Biometric field has however emerged in the recent days to reduce process delay and enhances the level of accuracy. This paper thus aims to analyze various biometric parameters that can be applied in realizing enhanced networking security. The proposed approach further reduces the cost associated with lost key and provides increased security. The key is directly generated from the human biometric information such as retinal blood vessels which is not stored in the database. This mode of operations in network security creates more complexity for hackers to crack or to guess the cryptographic key or biometric key.

Keys: **Cryptography, Biometrics, Endpoints, Bifurcation, Morphological Operation.**

I. INTRODUCTION

Cryptographic system has been widely used to secure information across network. Whether symmetric cipher system or an asymmetric ciphers system, its security depends upon the secrecy of the secret key or private key. However, there exist several cryptographic algorithms to secure the information such as RSA, DES, 3DES and AES etc[1][7]. Despite of their strengths, every algorithm suffers when the length of the keys is small, which is prone to easy guessing and hacking. Additionally, in conventional cryptography methods, the authentication of message is based on the key and is not based on the human components. Hence, there is a wide possibility of accepting the right key from the unauthorized user or attacker as key generation can be guessed or cracked. Other major inconvenience caused with key generation to achieve network security is complex nature of keys to remember and also difficulty in storing them securely in the database. Crypto-Biometrics system has recently emerged as an effective means to resolve the issues faced by traditional cryptography system [1, 4]. It is intended to find the key with the user biometric information in order to overcome the above-said issues through distortion, discrimination and security approaches. Distortion is the ability to accommodate the variance of biometric [4]. The system is expected to output the same key for the same user even if the biometric captured is at diverse conditions. Discrimination is the ability of the system to distinguish all the users of the database and output different key for different users [4]. Security of the system ensures that neither the key nor the original biometric of the user can be traced or guessed and the user's biometric information is unique [4]. Biometric based cryptography is therefore highly potential to provide security in advanced technologies [4]. Biometrics gives a unique measurable biological characteristics information for recognizing or verifying the identity of a person [4]. Since, cryptography is important for the network security, crypto-biometric has become one of the promising research area. In this approach, a unique cryptographic key is generated directly from the biometric information of the user namely retina biometric. This approach ascertains security to the digital data and due to uniqueness of biometrics; it is very difficult to generate the duplicate. The organization of the paper is as follows. Section 2 explains the study made in the related work. Section 3 provides information about the research work. Section 4 gives the conclusion of the work.

II. RELATED WORK

Key generation mechanism has proven to be one of the significant parameter to improve network security.[10,11] Public-key algorithms are based on mathematical functions and are asymmetric in nature, involving the use of two keys, as opposed to conventional single key encryption. However, the major drawback of key generation approach to achieve security is that password can be lost, stolen or easily hacked. Thus, research progress is witnessed to demonstrate the use of biometric to produce the key [12]. Several researchers are working in the domain of crypto biometrics since several years to achieve network security [13]. Fingerprint minutiae points are used to generate the key. However, currently research is popular in fingerprint biometric for the generation of key to achieve encryption and decryption of messages [13] [14]. C. Nandini [3] a unique technique for generation of cryptographic key. The authors have used hashing technique in the finger trivia using completely different set of symmetric hash function for various users that is both secured and fast. The authors have extracted k-plets from every finger print image and calculate the hash values primarily based on the closest neighbor of a minutia purpose within the k-plet. A mix of those hash values are used to come up with a key.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

However, recent research has proven that biometrics using eye biometric is even more accurate. [15]

III. CRYPTOGRAPHIC KEY GENERATION FROM RETINA BIOMETRIC

Since, eye biometric has proven to be one of the accurate modes of key generation parameters; this work focuses upon retina biometric as an encryption key. The retina biometric features are unique and remain unchanged in lifetime [16].

- The strength of the retinal biometric recognition is better than all other biometric technologies.
- The blood vessels pattern of the retina rarely changes during the person's life (Unless disease or accident).
- The size of actual template is only 96 bytes, which is very small when compared to any standards in terms of verification and identification processing times, and is much shorter than they are for larger file.
- The rich unique structure of the blood vessels pattern of the retina allows up to 400 data points to be created.

Due to the above said unique biological characteristics of retina, the retinal recognition is primary used in combination with access control system at high security facilities. This includes military installations, nuclear facilities and laboratories [16]. The encryption process begins with the acquisition of required biometric template. Initial step involves extraction of the features from the retina biometric to generate a cryptographic key that can be used for encryption a plain text message. From the retina image, extract the features such as blood vessels pattern (vascular tree) which undergoes the thinning process. From the above extraction, next step includes identification of the endpoint of each pattern and also the bifurcation points. The thus obtained endpoints are used to generate the key for encryption/ decryption of message. Figure 1 depicts the entire process of key generation using retina biometrics.

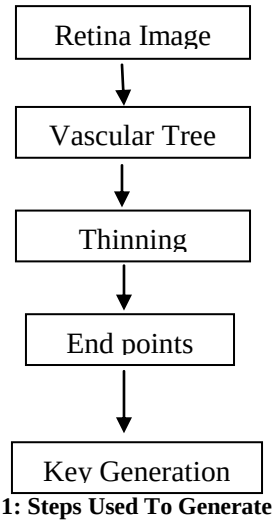

Fig 1: Steps Used To Generate the Key

However, this paper limits to perform the investigation using grey scale images instead of colored image. Mat Lab programming converts the colored retina image to grey scale, which is in turn converted to binary image using binarization technique. Figure 2 depicts vascular tree which is converted to grey by using MATLAB code. Since, vascular tree contains large number of blood vessels, this work focuses upon the study to be made on thick blood vessels. The main intention is to extract the thick blood vessels, which are major blood vessels in the retina and perform thinning operation using threshold value. The threshold value that is kept in this study is 1.39 as intensity value. A blood vessel whose intensity is above 1.39 is retained since it provides better resolution than those blood vessels whose intensity lies below the set threshold value [15].

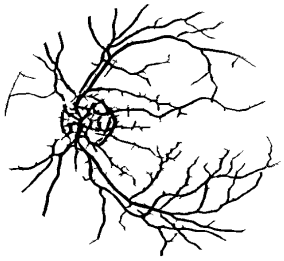

Fig 2: Vascular Tree

Subsequently, the skeleton of the vascular tree is obtained from the segmented binary image by thinning process where pixels are eliminated from the boundary towards center without destroying the connection in an eight connected scheme [13]. Pruning process is applied to eliminate short, false spurs, due to small undulations in the vessels boundary. False spurs are deleted if they are smaller or equal to the largest vessels diameter expected in the particular image as shown Figure 2. Followed by the retention of valid blood vessel pixels, the next step is to apply the Morphological operations in order to understand the structure or form of the image. This identifies the boundary within the image. There are morphological functions such as Dilation and Erosion. Dilation function is used to expand the image and erosion function shrinks the image in MATLAB code. Having obtained the boundary from the identified blood vessel, the after that activity is to perform the thinning process. This process finds the center point in the vascular three and compresses the boundary without disconnecting the other edges. Thinning is a morphological operation that is used to remove selected foreground pixels from the binary image. Figure 3. Shows the thinned image which is obtained due to the morphological operations performed upon the vascular tree. Finally, this part of the research work directs towards unique contribution of identification of endpoint from the origin by using the morphological operation and the structuring element strategy. The objective of structuring element technique is to identify a pixel with value 1 as a termination point and no other pixels with that value in its

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

neighborhood of 8 pixels. Such a pixel indicates an endpoint.

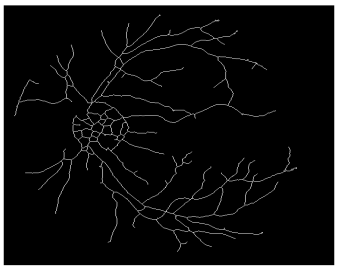

Fig 3: Thinned Image

1	1	1
1	1	1
1	1	1

The structuring element will be thus moved from the origin of an image, pixel by pixel at a time in x and y axis. As structuring element match with the thinned image pixel, it finds an edge between two pixels, and continues this process for the entire image to find the number of endpoints in an image. Whenever the structuring element does not match with the neighbor then set endpoint with red in color and green color are the bifurcation points using MATLAB code as shown in figure 4.

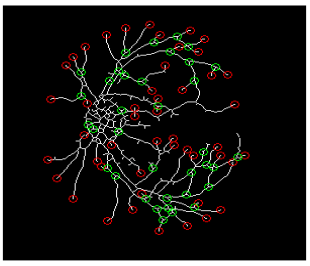

Fig 4: Endpoint in thinned image.

The output of endpoint(x, y) coordinates values of each endpoint and degree theta. Table 1 indicates the sample end points of thinned image.

Table 1. Sample output of retina image

X	Y	Theta (degree)
67	78	230
132	95	154

Key generation

The above (x, y) coordinate value of each pixel is used in the following algorithm to generate the key.

Step 1: Read the x and y coordinate values of an endpoint from the thinned image

Step 2: Compute the sum using the formula,

$$sum = sum + \sum_{i=0}^{n-1} (xi * yi) \bmod p \quad \text{(Eq.1)}$$

Where p is a prime number and 'i' is the coordinate value of each endpoint pixel.

Step 3: Find the equivalent binary value of the sum that becomes the key for encryption and decryption of message.

IV. EXPERIMENTAL RESULTS

The above said process of key generation approach is programmed in MATLAB 10 and tested the proposed approach on retina images. The vascular tree is extracted from the retina image after binarizing. A unique key cryptographic key is generated from the retina biometrics template of a user. However, Table 2 depicts the various end points of the thinned image of the retina as shown in Figure 4 along with its angle.

Table 2 Various End Point Values of the Retina Image

Name: final
Date: 2013-05-06
Number of Terminations: 32

Terminations:

X	Y	Angle
45	182	48.00
111	54	204.00
63	71	70.00
61	70	228.00
81	153	82.00
49	84	116.00
94	184	98.00
190	103	35.00
104	254	106.00
165	122	27.00
129	241	131.00
121	131	131.00
137	198	138.00
222	146	23.00
148	101	153.00
125	153	160.00
154	110	155.00
266	156	35.00
161	71	169.00
157	170	165.00
175	49	178.00
100	183	170.00
183	260	186.00
30	189	177.00
194	55	194.00
233	200	40.00
202	251	207.00
83	213	167.00
216	177	216.00
241	223	82.00
228	185	230.00
117	240	177.00

Having applied the algorithm on the data set as obtained in Table 2, leads towards the generation of key. The key value which generated from the retina image of Figure 4 is 10000101100011 which depend on prime number P. The retina image of different persons and the number of endpoints of each retina image as shown in table 3.

Fig 5

Fig 6

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Fig 7

Table 3 Endpoint of Different Images

Image	The Number of endpoints
Figure 5	30
Figure 6	18
Figure 7	23

V. CONCLUSION

Securing information across the network is one of the key challenges of the day. Security traditionally was achieved through cryptography approach. However, the recent advent in technology has enabled biometric techniques to generate key to achieve security. The aim of this paper is to provide secure way to generate the key using retina biometric technique since retina is unique and reduces the probability of duplicates. This research introduces an algorithm that directly generates the unique key from the human biometric information such as retinal blood vessels and is not stored in the database. This approach does not create redundant end points in addition to being more complex in nature to crack or to guess the cryptographic key. The paper however limits to key generation and can be further explored from the number of bifurcation points, degree of bifurcation point and the number eye land present in the retina images.

REFERENCES

[1]. Umut Uladag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain, "Biometrics Cryptosystem Issues and Challenges", Proceeding of IEEE, Vol 92, No 5, pp 948 - 960, June 2004.

[2] Je - Gyeong, Jong- Won Seo & Hyung -Woo Lee Div, "Biometrics Digital Signature Key Generation and Cryptography communication based on fingerprint ", Computer Information of software, Hanshin University.

[3] C. Nandini & B.Shylaja " Effective Cryptographic Key Generation from Fingerprint using Symmetric Hash Functions ", International Journal of Research and Reviews in Computer Science, Vol 2, No 4, ISSN 2079 - 2557, Aug 2011.

[4] S. Soutar , D. Roberge , A. Stoianov , R. Gilroy and B.V.K.V. Kumar, " Biometric Encryption ", In R.K. Nichols, editor ICSA Guide to cryptography, pp 649 - 675, McGraw Hill New York 1999.

[5] A. Jain, R. Bolle and S. Pankanti "Biometric Personal Identification in Network Society", Kluwer Academic Publisher New York, Boston, Dordrecht, London, Moscow, pp 1 - 64, 2002.

[6] A.K Jain , A. Ross and S. Prabhakar , " An introduction to biometric Recognition", IEEE Transaction on circuit and system for video Technology, Vol 14, pp 4-20,2004

[7] A. Jaya Lakshmi, I. Ramesh Babu, "Design of security key Generation algorithm using Fingerprint based Biometric Modality", ISSN: 2250-3021, Vol 2, Feb 2012.

[8] P.Balakumar, R.Venkatesan, "A Survey on Biometric Based Cryptographic key Generation Scheme", ISSN 2249 - 9555, Vol 2 , No1, 2012.

[9] B.Santhi,K.S.Ravichandran,"A Novel Cryptographic Key Generation Method using Image Features", Research Journal of Information Technology Maxwell Scientific Organization, ISSN 2041 - 3114, pp 88 -92, 2012.

[10] Literature Review of Cryptography and its Role in Network Security Principles Lloyd Calloway, 8 September 2008.

[11] F. Amin, A. H Jahangir and H. Rasifard, "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security" , World Academy of Science, Engineering and Technology, Vol 17, 2008.

[12] N.Lalithamani,K.P.Sonam,"Imevocable cryptographic key Generation From Fingerprint Template An Enhanced and Effective Scheme", European Journal of Science Research,ISSN-1450-216X, Vol 31 No.3 ,2009, PP 372 - 387.

[13] R.Sesshadri, T.Raghu Trivedi,"Efficient Cryptographic Key Generation using Biometrics". IJCSTA, Vol 2, ISSN: 2229-6093.

[14] Rashi Bais, K.K Mehta, "Biometric Parameter Based Cryptographic Key Generation", IJEAT, ISSN: 2249-8958, Vol-1, Issue - 5, June 2012.

[15] Kai- Shun Lin, Chia-Ling Tsai, "Retinal Vascular Tree Reconstruction with Anatomical Realism", IEEE transaction on Biomedical Engineering, Vol 59, No 12, December 2012.

[16] V. S . Meenakshi and G. Padmavathi, "Security Analysis of password Hardened Multimodel Biometrics", World Academic of Science Engineering and Technology, 2009.