ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 1, January 2015

Secured crypto biometric system using retina

Mohammed Tajuddin[1], C. Nandini[2]

Associate professor, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, India[1]

Professor and Head, Department of Computer Science & Engineering, Dayananda Sagar Academy of Technology & Management, Bangalore, India[2]

Abstract: Crypto biometric system is widely used in many information security applications to generate cryptographic key using the human retina characteristics. Biometric features will improve the security of cryptographic system. In this paper three retina biometric features are used to generate the key. They include the end points, bifurcation points and islands. This work emphasizes upon unification of three features which enables to generate the secured cryptographic key. This work introduces a unique method to generate a more secured cryptographic key. This mode of operations in network security creates more complexity for hackers to crack. Thus, security is further enhanced using the above technique.

Keywords: Cryptography, Biometrics, Endpoints, Bifurcation, island, Morphological operation, Encryption and Decryption.

I. INTRODUCTION

The process of transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form. There are many cryptographic algorithms to perform the transformation of message from one form to another form. The main goal of cryptography to provide is confidentiality, integrity and availability. The goal of confidentiality is data exchange between two users must be on trusted network, the information while exchange remains unchanged and secret. Integrity the information is always exchange between two users, but changes should be made by authorized users only. Integrity preventing the modification and to detect any modification made to the information. The confidentiality and integrity should not hinder the availability of data. The data must be available to the authorized users only. Types of cryptography algorithms secret key cryptography, public key cryptography and hash function. In secret key cryptography only one key is used for encryption and decryption where as in Public key cryptography one key encryption and another key for decryption of message.

Since security has become an increasingly important factor with the growth of E commerce. The Symmetric in which the same key value is used in both the encryption and decryption calculations are becoming more popular. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt the message in blocks of 128 bits.

AES is used because it is simple to implement by using cheap processor and uses minimum amount of memory. It has better resistance against existing attacks and increases security with less power and high throughput. AES uses four types of transformations, they are substitution, permutation, mixing and key adding [7].

- AES, like DES, uses substitution. However, the mechanism is different. First, the substitution is done for each byte. Second, only one table is used for transformation of every byte, which means that if two bytes are the same, the transformation is also the same.

- Another process found in a round is shifting. Shifting transformation in the AES is done at the byte level: the order of the bits in the byte is not changed [8].

- In the encryption, the transformation is called Shift Rows and the shifting is to the left. The number of shifts depends on the row number (0, 1,2, or 3) of the state matrix. This means the row 0 is not shifted at all and the last row is shifted three bytes.

- The mixing transformation changes the contents of each byte by taking four bytes at a time and combining them to recreate four new bytes.

- The operation in the Add Round Key is matrix addition. Since addition and subtraction in this field are the same, the Add Round Key transformation is the inverse of itself.

Cryptographic technique is being widely used for ensuring the secrecy and authentication of information. The secure protection depends upon the cryptography key, which is only known to the authorized users. Maintaining the secret key is one of the challenging issues over the internet [10]. The security of information in encryption system is depends on the technique used to generate the secrecy key for encryption and decryption instead of the encryption algorithm. The encryption system unable to

DOI 10.17148/IARJSET.2015.2104

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 1, January 2015

protect the cipher text once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space [6]. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the level of security is higher. In encryption, the key is piece of information which specifies the particular transformation of plaintext to cipher text, or vice versa during decryption.

Biometrics is an emerging field of technology using unique and measurable physical and behavioral characteristics that can be processed biometric features for identification of a person. The biometric attributes include facial appearance, fingerprint, gait, geometry handwriting, iris, retina, veins and voice. Retina biometric identification is an automatic method that provides true identification of the person by acquiring an internal body image which is difficult to counterfeit [1]. Retina identification has found application in high security environments. Retina biometric is unique biometric pattern that can be used as part of a verification system.

The rest of the paper is organized as follows: Section II provides the brief description of a generation of key from retina biometrics. Section III provides the background principles related to the working of the proposed model. All experimental results and related discussion is provided in Section IV. This paper is concluded by summing up the work in Section V.

II GENERATION OF KEY USING RETINA BIOMETRIC:

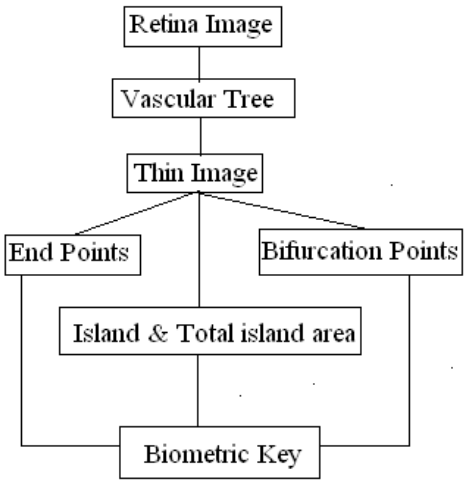

Figure 1 Design Diagram

Figure 1 indicates the system design to generate the cryptographic key from retina biometric features. The figure further indicates that the key is generate from the retina biometric features such as the number of end points with angle, the number of bifurcation points and the number of islands with the sum of area of all the islands. The above features are unique to all the retina biometric images, which is the unique method to generate the cryptographic key for encryption and decryption of message using cryptography algorithms. Accept the retina biometric from the database, convert the retina biometric to gray image, the values of gray image in the range 0 to 255 and then gray image to binary image in the form of 0's or 1's. From the binary image extract the blood vessels by setting the threshold value, the resultant tree is known as vascular tree as shown in figure (2).

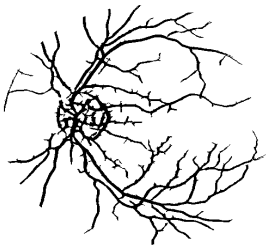

Figure 2. Vascular tree

Next activity is to thin the generated vascular tree by using morphological operation such as dilation, erosion and open etc. the broad blood vessels are converted to thin line connected components, since we can find the end points from the thinned image as shown in figure 3.

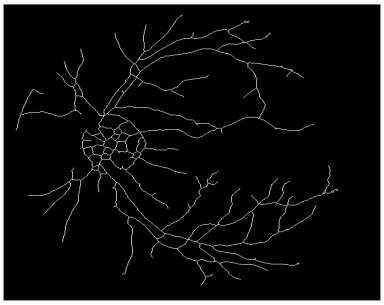

Figure 3 Thin Image

Figure 3 indicates the number of end points by using 8 pixel neighborhood structuring element which is further depicted in Figure 4. Move the structuring element from the origin pixel by pixel to find the connect components of a line, if the structuring element unable to find the neighbor element with 1 indicates a end point and the counter will increment by 1 and the pixel coordinate x and y axis with angle will be considered as shown in table 2. The same image is further investigated to identify the number of bifurcation points. As per the conventional assumption to detect a line is to check for two adjacent pixel values to be 1. Applying the same principles here, the number of bifurcation points is obtained for the image. Table 3 indicates the bifurcation points, x and y values for those points using MATLAB code and also the theta angles which is viewed from three perspectives of bifurcation points. Table 3 thus indicates that for the sampled retina image there exists 20 bifurcation points.

DOI 10.17148/IARJSET.2015.2104

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 1, January 2015

1	1	1
1	1	1
1	1	1

Figure 4 Structuring element 8 pixels

With the process of detecting end points and bifurcation points for the retina image, the work now focuses towards identification of island which is a closed loop in the thin image. One additional features not only the number of islands but also the total size each island area is considered to generate the biometric key. There may be a possibility of more than one image with same number of island, but the total size of each island of retina image will be unique as shown in figure 5.

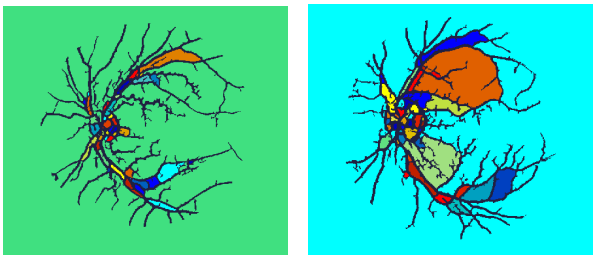

Figure 5. Two Different retinal image islands

By using principal components analysis to find the island of an image and also find the sum of area of islands which is unique for each image as shown in figure 5. The extracted features are unique, since these features generate a unique biometric key and it used to encryption and decryption using AES algorithm.

Key Generation method by using the three retina features such as number of end points with angle, Number of bifurcation points with three degree and the number of island with the sum of the island area.

The following steps are used to generate the unique biometric key.

1. Read in the input retina image.
2. Feature extraction
3. N_1 is the number of end points

$k_1 = \sum_{k=0}^{n} [x^k * y^k] + \theta$

4. N_2 is the number of bifurcation points.

$k_2 = \sum_{i=0}^{n} [x^i * y^i]$

5. N_3 is the number of islands with the sum of island area S_1.

$k_3 = \sum_{i=0}^{n} [x^i * y^i]$ + area

6. Key = $\sum_{k=1}^{3} k$
7.

III. ENCRYPTION PHASE

In this paper, biometric features are used to generate biometric key for the crypto systems. In the encryption process retina biometric features are used to generate the cryptographic key, the generated biometric key is converted to 128 bit key. In symmetric cryptography, a single key is used for both the encryption and decryption phases. According to this methodology, a key must be same to both encrypting and decrypting process. For encryption and its reverse process, in this work we use the Advanced Encryption Standard (AES) algorithm. The overview of the proposed retina encryption phase is shown in figure 6.

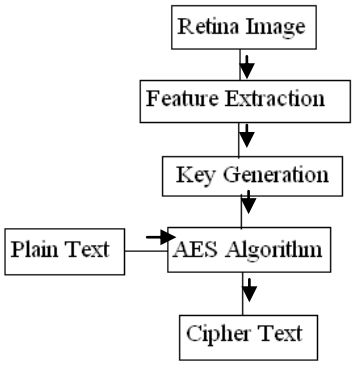

Figure 6 Encryption phase using AES

The cipher text is the result of encryption performed on the plain text using an AES algorithm is called cipher. The cipher text is also known as encryption or encoded information because it contains a form of the original plain text that is unreadable by a human or computer without the proper cipher to decryption using the same AES algorithm.

The generated cipher text again transforms back to original message by using decryption with AES algorithm as shown in figure 7.

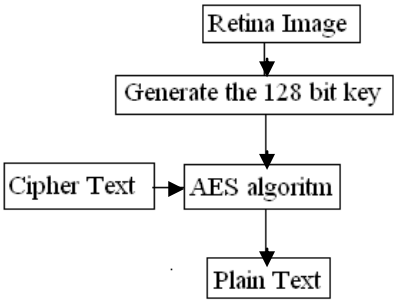

Figure 7 Decryption phase

IV RESULTS OF THE EXPERIMENTATION

Figure 8. Vascular tree from DRIVE dataset

DOI 10.17148/IARJSET.2015.2104

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 1, January 2015

Results are obtained from different datasets such as DRIVE and stare. These are the following results such as number endpoints as shown in table 2 Name of the image: img6.bmp, with few endpoints with the angle from the origin.

Table 2. The number of end points

X	Y	Angle
23	100	23.00
160	28	158.00
29	154	33.00
109	33	140.00
34	134	34.00
157	38	118
38	139	40.00
128	41	141.00
41	156	42.00
125	44	136.00
44	149	45.00
119	46	122.00
47	127	48.00
125	48	193.00
61	106	77.00
185	77	191.00
80	194	81.00

Table 3. The Bifurcation points with angles

X	Y	Angle1	Angle2	Angle 3
10	176	11.00	196.00	12.00
97	12	105.00	13.00	153.00
15	127	19.00	166.00	24.00
231	24	71.00	27.00	227.00
33	185	35.00	193.00	38.00
227	40	118.00	40.00	130.00
48	118	49.00	114.00	52.00
131	51	198.00	53.00	199.00
55	124	55.00	136.00	58.00
206	59	138.00	58.00	266.00
61	36	60.00	158.00	62.00
139	64	156.00	65.00	41.00
65	146	68.00	114.00	67.00
152	68	155.00	67.00	53.00
68	162	72.00	99.00	71.00
102	71	164.00	71.00	225.00
72	249	73.00	145.00	73.00
150	73	153.00	73.00	169.00
73	161	73.00	243.00	74.00
274	75	166.00	76.00	95.00

Table 3. shows the bifurcation points and three angles. The table further illustrates sampled experiment results where bifurcation angle is considered from the centre of the matrix.

The last feature of retina biometric is to count the number of islands and its area. Figure 9 shows that from the experimental results, it is observed that the numbers of islands are 35 and the total area of the islands is 325220. In the similar mode, it is thus possible to calculate the number islands with area for the two figures as shown in Figure 5.

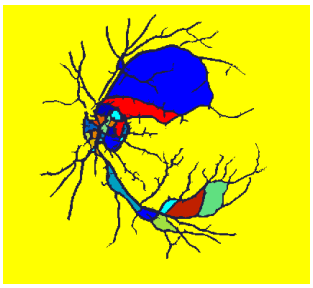

Figure 9. Retina islands

Further, a comparison is made with various methods and our proposed research work in terms of accuracy and true positive ratio (TPR). Figure 10 and Figure 11 indicates the comparison results which prove that our method of providing authentication and security using biometric retina method is better than other methods.

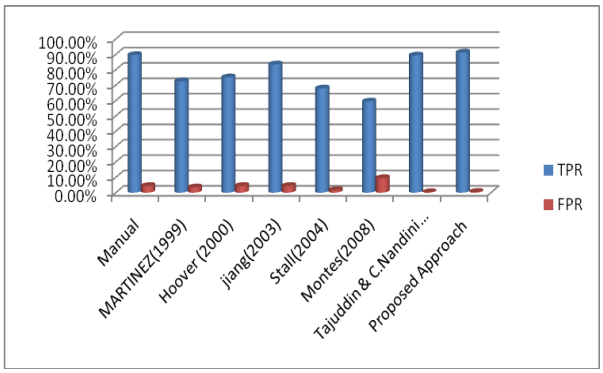

Figure 10. Comparison with other approachs wrt TPR & FPR

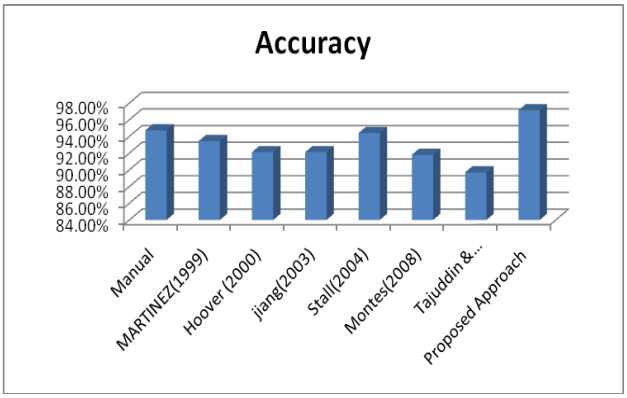

Figure 11. Comparison with other approachs wrt accuracy

DOI 10.17148/IARJSET.2015.2104

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 1, January 2015

V CONCLUSION

Attaining high security in key generation is always one of the challenges in network security applications. Aim of this part of research is to ensure enhanced authentication while generating cryptographic key using retinal images. This paper provides the details of dynamic key generation using unification of three significant biometric features such as the number of end points with angle, number of bifurcation points with three degree and the number of islands with total area of island. The paper thus provides information about the most prominent and unique biometric features of retina which has certain unique characteristics such as uniqueness, stability, non invasiveness, permanence compare to other biometrics. However, complexity of algorithm is more in the present approach to secure the information across communication channel. Nevertheless, the proposed system is reliable and efficient for biometric verification system and with this approach it is now possible for retinal biometric to be applied even in network associated application including cloud based applications.

REFERENCES

[1]. Hill, R. B. 1978. Apparatus and method for identifying individuals through their retinal vasculature patterns, US Patent No. 4109237
[2]. Xinmiao Zhang and Keshab K. Parhi, "Implementation Approaches for the Advanced Encryption Standard Algorithm" IEEE 2002.
[3]. Hui QIN, Tsutomu SASAO, Yukihiro IGUCHI, "An FPGA Design of AES Encryption Circuit with 128-bit Keys" GLSVLSI'05, ACM 2005
[4]. Chih-Peng Fanand and Jun-Kui Hwang, "FPGA Implementations Of High Throughput Sequential And Fully Pipelined AES Algorithm" International journal of Electrical Engineering, vol. 15, no. 6, pp. 447-455, 2008.
[5]. Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, "Efficient and High Performance Parallel Hardware Architecture for the AES-GCM" IEEE Transactions on Computers, vol. 61, no. 8, August 2012.
[6]. A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman and B.B. Zaidan, " Approved Undetectable-Antivirus Steganography forMultimedia Information in PE-File ",International Conference on IACSIT Spring Conference (IACSIT-SC09) , Advanced Management Science (AMS), Listed in IEEE Xplore and be indexed by both EI (Compendex) and ISI Thomson (ISTP), Session 9, P.P 425-429.
[7]. Behrouz A. Forouzan, "Cryptography and Network Security", *Tata McGraw-Hill*, 2007.
[8]. Ramya M., MuthuKumar A., KannanS. "Multibiometric Based Authentication Using Feature Level Fusion", *IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012)*, pp. 203-207, Mar 30, 31, 2012.
[9]. Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, "FPGA Implementation of AES Encryption and Decryption" International Conference on Control, Automation, Communication and Energy conservation -2009
[10]. R. Jubiaya , M Keirthi, " IRIS Authentication Based on AES Algorithm", IJIRSET, Volume 3, special issue 3, March 2014.
[11]. X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm" , IEEE Transactions on Very Large Scale Integration Systems, vol. 12, issue 9, pp. 95 967, Sep. 2004.
[12]. Jin Gong ,Wenyi Liu, Huixin Zhang, "Multiple Lookup Table-Based AES Encryption Algorithm Implementation" Elseveir-2012 vol. 25 pg no. 842 – 847.
[13]. Saurabh Kotiyal, Himanshu Thapliyal and Nagarajan Ranganathan, "Design of A Reversible Bidirectional Barrel Shifter" IEEE international conference 2011.
[14] .J. Vijaya, M. Rajaram, "High Speed Pipelined AES with Mixcolum Transform "European Journal of Scientific Research" 2011. Vol. 61 No. 2, pp. 255-264.
[15]. 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.
[16] .Mohammed Tajuddin , C. Nandini," Cryptographic Key Generation using Retina Biometric Parameter", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013, ISSN: 2277-3754.
[17]. Mohammed Tajuddin, C. Nandini, "More Secured Cryptographic Key Generation through Retinal Biometric using EBI Algorithm
[18]. Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha pratim sarkar, "Secret sharing schemes for protection of digital images", Article in CSI communication October 2014.
[19]. Kai- Shun Lin and Chia-Ling Tsai, " Retinal Vascular Tree Reconstruction with Anatomical Realism", IEEE transaction on Biomedical Engineering, Vol 59, No 12, December 2012.
[20]. Stallings, W.: Cryptography and Network Security, Prentice Hall, (2010).

DOI 10.17148/IARJSET.2015.2104