ISSN 2277 – 5528
Impact Factor- 4.015

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

MULTIMODAL BIOMETRIC TO GENERATE THE KEY FOR DATA SECURITY USING RETINA AND FINGERPRINT FEATURES

Mohammed Tajuddin[*1] and C. Nandini[2]
[*1]Dept. of CSE, DSCE, Bangalore
[2]Dept. of CSE, DSATM, Bangalore

ABSTRACT

Single biometric systemsare prone to have problems such as noisy data, non-universality and unacceptable error rate. Hence, multimodal biometrics systems are widely used to consolidate the result which isobtained from two or more biometrics.Thisenables one to avoid the unacceptable error rate and reduces the failure rate. Thus, multimodal biometric systems have emerged as an innovative alternative approach to develop a more reliable and efficient security system. The aim of this paper is to put forth application of key generation for data security over the internet. This is achieved using cryptographic key which is not easy tobe guessed or to crack by intruders during the transmission over the internet

***Keywords**:* Multimodal, Biometric, Encryption and Decryption.

I. INTRODUCTION

In single biometric system have limitation like uniqueness, noisy image, noise data, high error rate, non-universality. Biometric images are captured with various devices such as optical sensor for fingerprint, retina images sensor camera and gait trait with digital camera. Biometric system are based on human body features are used to authenticate the person depends on single biometric or multimodal biometric data for authentications. Retina and fingerprint biometric haveunique features and more reliable image patterns and these patterns does change and are permanent in lifetime, only in case of accident they may damage.Hence we are using retina and fingerprint biometric information to generate the cryptographic key which will used for the cryptographic application for the encryption and the decryption process.In multimodal approach reduces the true rejection rate(TRR). The TRR and FAR analysis is performed and the results are suggested better and the proposed approach achieve 80% correct.

II. RELATED WORK

The challenge is to provide the authorized users with secure and easy to access to information and the services across the network system. A reliable management system is a critical component in several applications that provide the services to only legitimated enrolled user. In an organization an application including the physical access controls to secure facility. The primary task is to identify the system is the determination of an individual identity. This action may necessary for many reasons but in most applications. The primary intention is to provide the security to the data. In traditional method identification of a person based on the password and the ID cards but this representation of the identity can easily be lost or stolen. Biometric offers a reliable and natural solution to the problem to identify the person by using certain physiological or behavior traits associated with a person [1].

Multimodal biometric systems are based on different biometric features and are introduce different fusion algorithms for these features. Many researchers have demonstrated that the fusion process is effective, because fused scores provide much better discrimination than individual scores. Such results have been achieved using a variety of fusion techniques. A unimodal fingerprint verification and classification system is proposed, the system is based on a feedback path for the feature-extraction stage, followed by a feature-refinement stage to improve the matching performance. This improvement is illustrated in the contest of a minutiae-based fingerprint verification system. The Gabor filter is applied to the input image to improve its quality [2].

III. RESEARCH WORK

Multimodal biometric to generate the cryptographic in this paper we introduces fingerprint is the feature pattern and it is unique. Each person has its own fingerprint with the permanent uniqueness features. A fingerprint contains a ridge and furrows which are parallel and having same width.

ISSN 2277 – 5528
Impact Factor- 4.015

Figure 3.1 Original Fingerprint image

Fingerprint is not distinct by their ridges and furrows but they are distinct by minutia, which are the features on the ridges.The original RGB image is converts to gray, gray image to thin image by using the morphological operation. To the thinned image move the structuring element from the origin. The Approach is used for the extraction of minutia is if the pixel with 1 value has its neighbor with 1 value in its 8 neighbor structuring element, it is endpoint and if it has three neighbors with 1 value it is the bifurcation points. The structuring element moves pixel by pixel in a thinned image to find the endpoint and the bifurcation point in an image.

0	0	0
0	1	0
0	0	1

Figure 3.2 Structuring elements to find the endpoints.

0	0	0
0	1	0
1	0	1

Figure 3.3 structuring elements to find the bifurcation points.

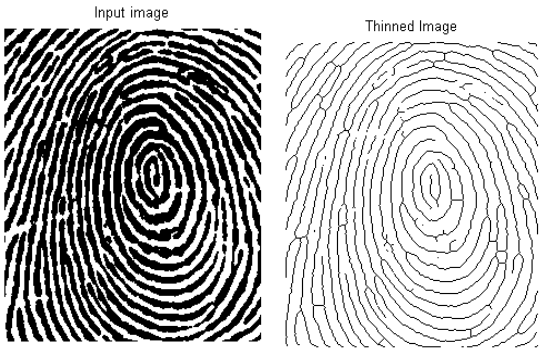

Figure 3.4 Original & thinned Image

ISSN 2277 – 5528
Impact Factor- 4.015

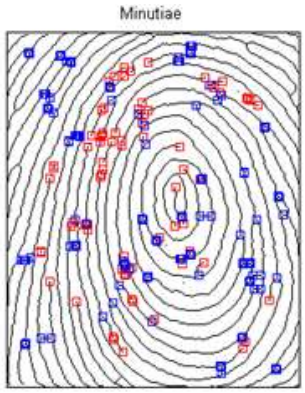

Figure 3.5 Red color endpoint & Blue color bifurcation point

The biometric images are used to generate the cryptographic key for data security over the internet. In fingerprint minutia points feature is used to find the end point and the second feature is the bifurcation points in minutia pattern.

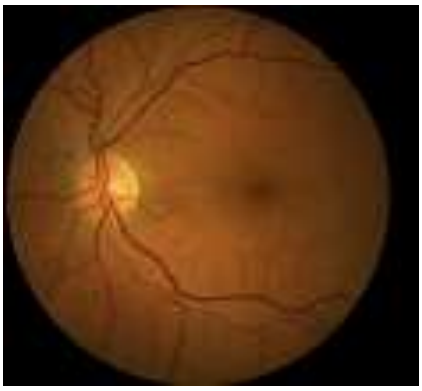

Figure 3.6 Input Retina image

Read the input retina image then convert that image gray and the gray image convert it into thinned image using the morphological operation. The conversion of images from one form to other form is done using Mat Lab programming.

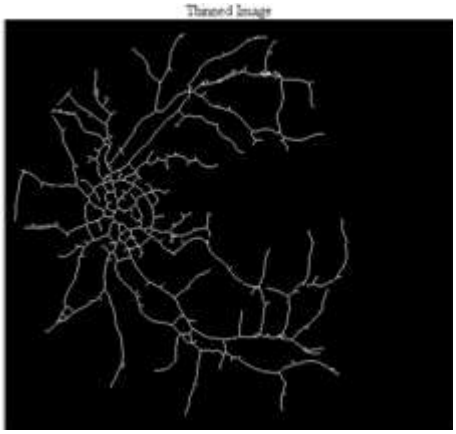

Figure 3.7 Thinned image of figure 3.6

Find the number of termination points, the number of bifurcation points and the number of island in a thinned image. To find the termination point move the structuring element as shown in Figure 3.2 from an origin if the pattern

matches with the structuring element represent one termination points.Using structuring elements as shown in figure 3.2 & 3.2, If the pixel with 1 value has its neighbor with 1 value in its 8 neighbor structuring element, it is the termination point and if it has three neighbors with 1 value it are the bifurcation points

IV. KEY-GENERATION APPROACH

In our approach we have selected retina and fingerprint biometric features for the generation of cryptographic key, the system design diagram as shown in 3.8

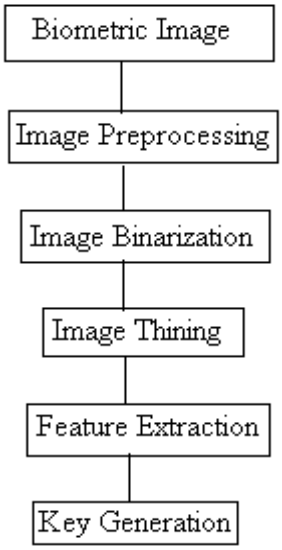

Figure 3.8 System Design Diagram to generate the key.

Key generation from the fingerprint termination points using discrete cosine transform method.
Key1 =

Where p(x, y) is the x^{th}, y^{th}element of the image represented by the matrix p, N is the size of the block that the discrete cosine transform is done on. The above equation calculates one entry (i,j) of the transformed image from the pixel values of the original image matrix. The above process is continuingfor all the values of (x, y) of Table 4.1 and its mean will be the key from termination points. Similarly to generate the cryptographic key using retina end points.
Key2=

To generate other keys using bifurcation points of both the fingerprint and retina information that we will consider as key3 and key4 as shown in figure 3.9. To find keys the mathematical representation as follows, by using all the connected lines of a bifurcation point.

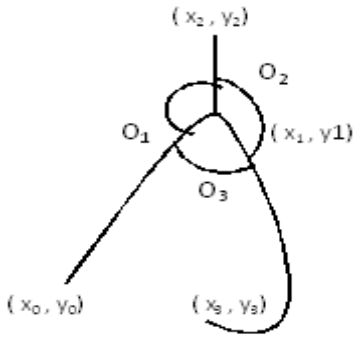

Figure 3.9 Bifurcation point of retina image

ISSN 2277 – 5528
Impact Factor- 4.015

The point slope form approach to find the slope of m passing through the point. If P(x,y) is any point (x≠x1) then P € L where L is line, if and only if the slope of the line AP is m. By referring Figure 3.9 two point form the equation of a line passing through the point (x_0, y0) to (x_1, y_1) is($y - y_0$) = m1($x - x_0$) where the slopem1= (y_1- y_0) / (x_1- x_0) , the two point form the equation of line passing through(x_1, y_1) to (x_2, y_2)is($y - y_2$) = m2($x - x_2$) where m2= (y_2- y_1) / (x_2- x_1) and similarly the line passing through (x_1, y_1) to (x_3, y_3) is we found ($y - y_3$) = m3($x - x_3$) where m3= (y_3- y_1) / (x_3- x_1). To find the theta by using thevalues of m as follows.

$\Theta_1 = \tan^{-1}$
$\Theta_2 = \tan^{-1}$
$\Theta_3 = \tan^{-1}$

therefore theta will become the key,
$\tan^{-1}$

Key3 is calculated by using the results of a retinaimageand key4 theresultant information of a fingerprint image. By using these four key generated from the biometric retina and fingerprint, the final key will be the sum of all the four keys, this key we can apply to any cryptographic application to encrypt and to decrypt the message. The generated keys can also be used in cloud application to store the data in public cloud in secure mode.

Algorithm to generate the secure key for cryptographic and cloud applications.

1. Read the fingerprint & Retina Image
2. Extract the features of fingerprint & retina such as end points & bifurcation points.
3. key1 from the end points of fingerprint
4. key2 from the bifurcation points of fingerprint
5. key3 from the end points of retina
6. key4 from the bifurcation points of retina
7. finally key will be
   key = key1⊕key2 ⊕kay3 ⊕key4

V. EXPERIMENTAL RESULT

The proposed work isimplemented in MATLAB to find the number of endpoints and the bifurcation points in a fingerprint images and the retina images the data set is taken from Varia, Stare, Drive and some hospitals. We tested it by taking many retina images as well as fingerprint images to generate the cryptographic key only one sample out as shown in table 1 to table 4. We also tested by rotating the input images with some angles. When we rotate the image the number of end points and the number of bifurcation points will remain same and only differ in angles of the end points and the bifurcation point three angles.

Table1: End points in fingerprint.

Name: fingerprint result		
Date: 2016-06-21		
Number of Terminations: 21		
Number of Bifurcations: 78		

Terminals		
X	Y	Angle
1	143	1.00
159	1	174.00
1	186	2.00
240	3	246.00
7	255	9.00
200	17	295.00
21	262	24.00

ISSN 2277 – 5528
Impact Factor- 4.015

300	32	159.00
32	263	33.00
201	34	300.00
38	264	41.00
278	45	285.00
122	288	151.00
300	203	274.00
206	154	209.00
275	214	172.00
220	275	226.00

Table 2: Bifurcation points in fingerprint

Bifurcations :

X	Y	Angle1	Angle2	Angle 3
5	108	6.00	84.00	9.00
242	9	118.00	9.00	226.00
10	293	13.00	89.00	13.00
172	16	236.00	18.00	73.00
20	126	22.00	67.00	23.00
119	25	141.00	30.00	129.00
31	99	32.00	145.00	44.00
163	44	170.00	46.00	38.00
52	138	56.00	80.00	53.00
199	57	231.00	58.00	153.00
61	198	61.00	192.00	62.00
116	62	141.00	64.00	153.00
68	191	69.00	106.00	69.00
72	71	115.00	73.00	158.00
77	36	79.00	158.00	85.00

Table 3.Terminal points in retina.

Name: Retina
Date: 2016-06-23
Number of Terminations: 27
Number of Bifurcations: 86

Terminations :

X	Y	Angle
37	140	40.00
167	42	89.00
52	134	227.00
93	60	227.00
66	197	67.00

ISSN 2277 – 5528
Impact Factor- 4.015

84	75	190.00
116	40	117.00
213	122	40.00
122	46	125.00
250	131	38.00
141	196	147.00
105	149	197.00
153	220	157.00
42	169	52.00
168	254	170.00
142	112	98.00
234	156	87.00
96	87	76.00
45	197	113.00
127	235	182.00

Table 4.The bifurcation points in retina

---------- Bifurcations : ----------				
X	Y	Angle1	Angle2	Angle3
10	140	11.00	122.00	11.00
131	13	155.00	13.00	178.00
25	172	26.00	215.00	41.00
37	48	266.00	52.00	95.00
55	245	58.00	239.00	60.00
271	61	146.00	70.00	176.00
71	108	70.00	275.00	72.00
258	76	165.00	76.00	180.00
79	171	82.00	149.00	85.00
98	91	96.00	95.00	181.00
95	40	96.00	199.00	102.00
134	103	33.00	105.00	280.00
107	181	110.00	273.00	113.00

Table 3 & Table 4 infers the few sample value such as the number of end points and the number of bifurcation points in an thinned retina of Figure 3.7 all these results are obtained in MatLab.

VI. CONCLUSIONS

Due to the drawback of single biometric systems which are pronetonoisy data, non-universality and unacceptable error rate. Therefore, multimodal biometric systems have come into existence. This research has aimed to achieve the generation of secure key with multiple biometric features usingmultimodal approaches, which isa unique method. This paper hence provides the details of merging the features of two biometrics to generate the unique key by taking the permanent features of both the biometrics retina and fingerprint. The technique mentioned above is an alternate method to generate the cryptographic key using discrete cosine transformation. The proposed method is reliable and efficient for biometric verification system for cryptographic application and also in cloud applications in order to store the information both in public and private clouds.

ISSN 2277 – 5528
Impact Factor- 4.015

REFFERENCES

1. *Ms. Priyanka S. Patil , Prof.(Dr.) A. S. Abhyankar, "Multimodal Biometric Identification System Based On Iris & Fingerprint", IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197 Volume 1, Issue 6 (Mar. – Apr. 2013), PP 76-83*
2. *Mohammed Tajuddin, C. Nandini"Secured crypto biometrics system using retina", IARJSET, Vol 2 Issue 1 January 2015, ISSN2394 – 1586.*
3. *Mohammed Tajuddin, C. Nandini, "More Secured Cryptographic Key Generation through Retinal Biometric using EBI Algorithm", IJEIR, VOL 3, Issue 5 , ISSN 2277-5668.*
4. *]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.*
5. *B.RajaRao, Dr.E.V.V.KrishnaRao, S.V.RamaRao,M.RamamohanRao, "Finger Print Parameter Based Cryptographic Key Generation", IJERA, ISSN: 2248-9622 ,Vol. 2, Issue 6, November- December 2012, pp.1598-1604.*
6. *Digital Image processing by Gonzalez, 3rd Edition.*
7. *Dr. Shubhamgi, D.C Manohar Bali," Multi Biometric Approaches to Face and Fingerprint biometrics , IJERT, ISSN 2278 – 0181, 2014*
8. *A. Hoover , V. Kouznetsova and M.G, " Locating blood vessels in retina images by piecewise threshold probing of a matching filter response", IEEE Transaction medical Imaging, Vol 19, No 3, PP 203 -210.*
9. *Umut Uludag, SharathPankanti, Salil Prabhakar, AnilK. Jain, "Biometrics Cryptosystem Issues and Challenges", Proceeding of IEEE, Vol 92, No 5, pp 948 - 960, June 2004.*
10. *Sunil .V .K, Gaddam I and Manohar Lal, "Efficient cancellable biometric key generation schemefor cryptography", IJNS, Vol 11 No.2 , PP 57, Sept 2010.*
11. *Mohammed Tajuddin ,C. Nandini," Cryptographic Key Generation using Retina Biometric Parameter", IJEIT, Volume 3, Issue 1, July 2013, ISSN: 2277-3754.*
12. *C. Nandini andB.Shylaja " Effective Cryptographic Key Generation from Fingerprint using Symmetric Hash Functions ", IJRRCS, Vol 2, No 4, ISSN 2079 –2557, Aug 2011.*
13. *MohitAgarwal,"Design approaches for multimodal biometrics system", IIT Kanpur.*
14. *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*
15. *P. Reid, Biometrics and Network Security: Prentice Hall PTR, 2003.*