International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 1 pp. 350-358 Jan 2018-June 2018 www.csjournals.com

Development of Biometric Cryptosystem Using Fingerprint Authentication

[1]Hariom Tyagi, [2]Prof (Dr) Sarvottam Dixit
[1]Research Scholor , [2]Professor
Deptt Of Computer Science & Engineering, Mewar University Chittorgarh, Rajasthan (INDIA)

ABSTRACT: Biometric system is one of the most reliable and very popular technique now a days and Fingerprint authentication is one of the most reliable and robust biometric technique due to its characteristics. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system. Fingerprint characteristics has major and significant role in person authentications. In this thesis work, A fingerprint authentication scheme consists of many stages: image enhancement, binarization, segmentation, ridge thining , minutia extraction. During this authentication we use Gaussian filter for better results. The hybrid security create by using combined biometrics and cryptography, e.g. fingerprint and cryptography scheme. A combination of many biometric features with crypto key is to give approach to enhance the authenticity and reduce the false accept rate (FAR) and false reject rate (FRR) of the fingerprint .For any new user of a biometric system, the combination of crypto biometric systems will overcome the accuracy and vulnerability limitations. A fingerprint authentication with template this is irreversible against almost all types of trials. In cryptography technique, all techniques are very strong and give the best security. We want to secure to our original data from unauthorized person and unauthorized system , for this we use cryptography scheme like Diffie Hellman Key exchange algorithm. Biometric techniques can be used for a large number of applications like, biometrics can help make secure operations, secure transactions and everyday life both safer and more convenient. You can check anywhere in companies, universities etc the biometrics provide applicable identity solutions. The applications of cryptography include E-commerce, all types of chip-based payment cards, digital currencies, generate password and any secure communication. Cryptography system and Fingerprint authentication have been identified as two of the most important aspects of a security environment.In this paper two strong technique is merging and give the better and safe results In this research work we use a 3-tire security system, it means we check a fingerprint for authentication, using Gaussian filter based technique because it gives the less FAR and less FRR ,with the authorized fingerprint and after all authentication there will be generate a security key or secure message for a particular work. If input fingerprint is matched as of authorized person but DBA's fingerprint is not matched then system says "You are a Unauthorized person, please try again". If both fingerprint is matched then is provides the all secure password or cryptography keys or secure message for concerned works. This is developed by MATLAB (Matrix Laboratory). The proposed algorithm is tested on FVC2004 databases and compared to all participators in FVC2004.

1. INTRODUCTION: BIOMETRIC CRYPTOSYSTEM

Biometrics means refers to two different fields of study and application. Biometrics is a most used methods of recognizing a person based on a physical or behavioral characteristic. Among the features measured are; face, fingerprints, geometry, handwriting, iris, retinal, vein and voice etc. The purpose of this , we want to high level of security and transaction fraud decrease. Biometric-cryptosystem based solutions are able to provide for confidential and financial transactions and personal data privacy [16].

Cryptography is the most reliable practice and study of hiding information. Cryptography refers almost exclusively to encryption, the process of converting original message, i.e. plain text, into cipher text. Decryption is the reverse process , convert from cipher text to plaintext. The operation on a plain text and cipher text is controlled by the algorithm and a key. Keys are important as ciphers without variable keys are easily breakable and therefore less than useful for most purposes in this paper we use a fingerprint as a security key.This idea of cryptography and fingerprint has been introduced as part of a privacy and secure enhancing technology with respect to personal data protection, personal secure communication, reliability and robustness against user input and a needed secure system. However it is an vulnerable to attacks, e.g. cracking, and tracking of information sources but he/she face next secure channel, cryptography.

There are the various methods that can be pass out to secure a key with a biometric technique. Firstly it involves key storage and template matching. In this method, we use here, firstly a fingerprint image is captured by using device and compared with a template. If the user is authentic, then we again check the authenticity by using the key exchange algorithm like Diffie Hellman Key Exchange algorithm, after that the secrete message is released

2. IDENTIFICATION AND VERIFICATION PROCEDURES

2.1 False Rejection Rate (FRR) : The FRR is the frequency that an authorized person is rejected access. This is also called **False non-match Rate (FNMR).** It measures the percent of valid inputs being rejected [7, 18].

$$FRR(n) = \frac{\text{number of all rejected verification checks up for a qualified or like authorized person n}}{\text{number of all verification checks up for a qualified or like authorized person n}}$$

2.2 False Acceptance Rate (FAR): The FAR is the frequency that a non-authorized person is accepted as authorized. Because a false acceptance can often lead to damages, FAR is generally a security relevant measure. This is also called **False Match Rate (FMR).** It measures the percent of invalid matches[7, 18].

$$FAR(n) = \frac{\text{number of all successful independent fraud checks up against a people}}{\text{number of all independent fraud checks up against a people}}$$

2.3 Equal Error Rate (EER): The common value of the FAR and FRR when the FAR equals the FRR. This is the value where both the FAR and FRR are kept as low as possible at the same time. A low EER value indicates a high accuracy of the system [7, 18].

3. BIOMETRIC TECHNIQUES

Currently, there are many different techniques available to identify/verify a person based on biometrics.

3.1 Physical characteristics: The following are examples of biometric techniques based on physical characteristics:

3.1.1 Fingerprint authentication: The fingerprint matching, either for the one-to-one verification case or one -to-many identification case, is straightforward and easy. The system captures a high-resolution image of the fingerprint, typically using a charge-coupled device (CCD) camera. Not with standing its association with "criminal" applications, clients generally accept the Fingerprint biometric.

3.1.2 Recognition of hand **3.1.3 Face recognition** **3.1.4 Face geometry**

3.1.5 Vein pattern recognition **3.1.6 Retina recognition** **3.1.7 Iris recognition**

3.2 Behavioral characteristics: The following are examples of biometric techniques based on behavioral characteristics:

3.2.1 Voice recognition **3.2.2 Signature recognition** **3.2.3 Keystrokes dynamics**

Some other Physical and Behavioral Biometrics techniques , we discussed here, as follows:

Nail identification, DNA patterns, Sweat pore analysis, Ear recognition, Odor detection, Walking recognition, Gait etc.

4. COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES

It is possible to understand if a human characteristic can be used for biometrics in terms of the following Parameters [8, 24]:

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 1 pp. 350-358 Jan 2018-June 2018 www.csjournals.com

Table 1.1: Comparison between Biometrics Technologies [24]

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	**Medium**	**High**	**High**	**Medium**	**High**	**Medium**	**High**
Hand geom.	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	Medium	Medium	High
Retinal	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	Low	Low
Voice	Medium	Low	Low	Medium	Low	High	Low
Thermo-gram	High	High	Low	High	Medium	High	High
Ear	Medium	Medium	High	Medium	Medium	High	Medium
Gait	Medium	Low	Low	High	Low	High	Medium
Keystroke	Low	Low	Low	Medium	Low	Medium	Medium
Odor	High	High	High	Low	Low	Medium	Low
Palm print	Medium	High	High	Medium	High	Medium	Medium
Facial-thermo	High	High	Low	High	Medium	High	Low

(i) **Uniqueness** is how well the biometric separates individually from another.
(ii) **Permanence** measures ho well a biometric resists aging.
(iii) **Collectability** eases of acquisition for measurement.
(iv) **Performance** accuracy, speed, and robustness of technology used.
(v) **Acceptability** degree of approval of the technology.
(vi) **Circumvention** eases of use of a substitute.

5. FINGERPRINT AUTHENTICATION

A fingerprint is the feature patterns of a finger. It is believed with strong evidences that each fingerprint is always unique of each person. The Scientific basis behind friction ridge analysis is the fact that friction ridges are persistent and unique. Even identical twins do not have the same fingerprints. [16].
Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are the corrugations formed on the surface of the fingers and thumbs.

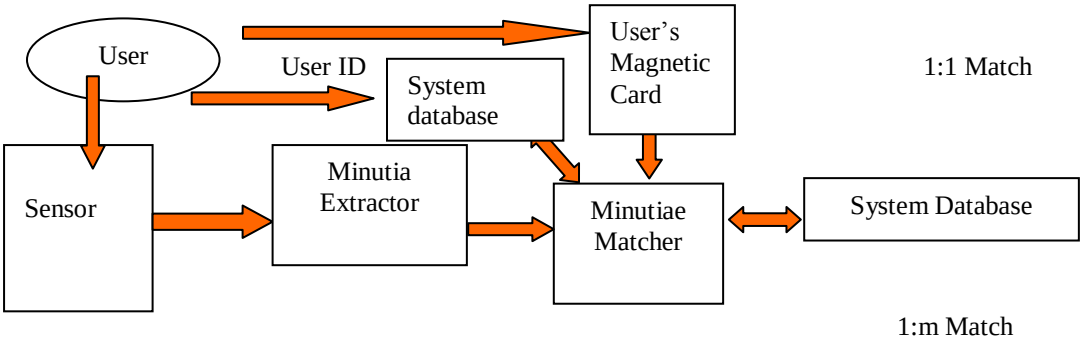


Fig 1.1 : Verification vs. Identification [20]

6. ALGORITHM USED

Minutia-based algorithm

Minutia-based algorithm compare several minutia points (ridge ending, bifurcation, and short ridge) extracted from the original image stored in a template with those extracted from a candidate fingerprint. For each minutia point, a vector is stored into the template in the form:

$$m_i = (w, type, xi, yi, \theta i) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1.1)$$

Where m_i is the minutia vector

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 1 pp. 350-358 Jan 2018-June 2018 www.csjournals.com

type is the type of feature (ridge ending, bifurcation, short ridge) ,x_i is the x-coordinate of the location
y_i is the y-coordinate of the location , θ_i is the angle of orientation of the minutia
w is a weight based on the quality of the image at that location

It is important to note that an actual image of the print is not stored as a template under this scheme. Before the matching process begins, the candidate image must be aligned with the template coordinates and rotation.

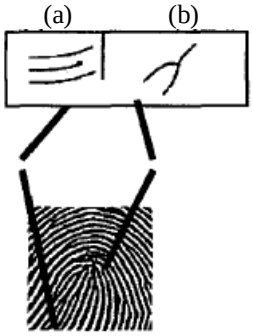


Fig 1.2: Minutia-based representation: (a) ending ridges (b) bifurcation ridges [17]

7. BIOMETRIC SYSTEM DESIGN

To implement a minutia extraction, a three-stage approach is used by researchers. They are preprocessing, minutia extraction and post processing stage see Fig 1.3.

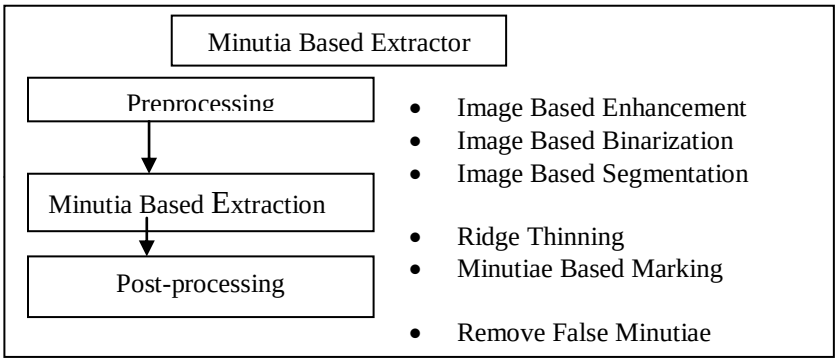


Fig 1.3: Minutia Based Extractor [16]

8. FINGERPRINT IMAGE PREPROCESSING

8.1 FINGERPRINT IMAGE ENHANCEMENT: Histogram Equalization: Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced

The probability density function of a pixel intensity level r_k is given by

$$P_r(h_k) = N_k / N \quad \text{.....(1.2)}$$

Where: $0<=h_k<=1$ and k= 0, 1 ….255

N_k is the number of pixels at intensity level and N is the total number of pixels.

Gaussian Filter: Gaussian filter remove the noise and extra details from the original image. This filter attenuates the variation of light intensity in the neighborhood of a pixel.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 1 pp. 350-358 Jan 2018-June 2018 www.csjournals.com

Fig 1.4: Fingerprint enhancement by Gaussian filter, Enhanced image (right), Original image (left)[11]

It smoothens the overall shape of the image. The enhanced image after Gaussian filter has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges. The shown image at the left side of Fig 1.9 is also processed with histogram equalization after the Gaussian filter transform.

8.2 FINGERPRINT IMAGE BINARIZATION

Binarization is a method of transforming grayscale image pixels into either black or white pixels by selecting a threshold. Fingerprint Image binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white.

8.3 FINGERPRINT IMAGE SEGMENTATION

To separate foreground and background block wise variance threshold is used. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check, while the second is intrigued from some Morphological methods.

8.4 ROI

The bound is the subtraction of the closed area from the opened area. Then the algorithm throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

Fig 1.5: the extracted ridge (left side) and the thinned ridge (right side) [7, 10]

8.5 FINGERPRINT RIDGE THINNING

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. This is done using morphological process. Pruning and ridge filling operation on the thinned image remove false minutiae.

8.6 MINUTIA MARKING

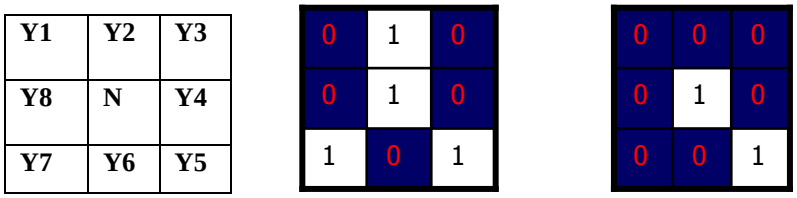
The most commonly employed method of minutiae extraction is the intersection number (IN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. These minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3□3 window [7, 9].

A pixel M with its eight neighboring point (Y1,….., Y_8)are defined as well. The order of neighbors is assigned in a clockwise direction beginning from the upper left-hand corner. X (n) represents the value of pixel Y_n. If Y_n is a white pixel, then its value of X(n) will be 0. In addition, X(n) will be 1 if the pixel is black .The pixel N is determined as a ridge ending if it achieves the following condition [7,8].

$$IN=\Sigma h=1\ldots 8[X(h+1)- X(h)] =2, \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1.3)$$

Where R (9) =R (1)

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 1 pp. 350-358 Jan 2018-June 2018 www.csjournals.com



(a) (b) (c)

Fig 1.6(a): A 3□3 window ,(b) Bifurcation, (c) Termination

The pixel M is determined as a Bifurcation, the condition will be as follows

$$IN=\Sigma_{k=1\ldots 8}[X(k+1)-X(k)]=6 \quad \ldots\ldots\ldots\ldots\ldots\ldots (1.4)$$

In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending, see Fig 1.13(b) &(c).

8.7 FALSE MINUTIA REMOVAL

The preprocessing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. These false minutias will significantly affect the accuracy of matching if they are simply regarded as genuine minutia.

9. MATCH SCORE: MINUTIA MATCH

First we take the query fingerprint image. Then Take the core point is located at the center of the feature map. After then locations of minutiae are mapped to corresponding sectors. Among the region of a sector, if one or more points are ridge endings or bifurcations, the value of the sector is added to denote number and kind of minutiae.

With the help of two equations find out the match score.

$$\sum_{j=b1}^{b2}\sum_{i=1}^{Nj}|S_k(Q_{ij})-T_{ij}|+\sum_{j=b3}^{b4}\sum_{i=1}^{Nj}|S_{2K}(Q_{ij})-T_{ij}|<TH \quad \ldots\ldots\ldots\ldots (1.5)$$

where Qij is the i^{th} sector of j^{th} ring region in a query images, Tij is the corresponding sector in template images,Sk(y)means that x is rotated clockwise with k sector ,k=0,1,2,…..15.

TH is the threshold and the range of ring is 1<b1<b2, b2<b3<b4 and b4<N .

$$\text{matching score}= N\left[\sum_{i=1,2\ldots N}\exp(D_i)\right]^{-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1.6)$$

The matching score can be computed according the formula [7].

$$D_j=\sqrt{\sum_{i=1}^{N_j}(Q_{ij}-T_{ij})^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1.7)$$

Where Dj is the Euclidean distance between the two corresponding ring.

10. METHODOLOGY: BIOMETRIC CRYPTOSYSTEM

After the fingerprint authentication system as per algorithm 10.1 then again we use Diffie-Hellman Key Exchange algorithm for once more authentication see Fig 1.8:

10.1 BIOMETRIC CRYPTOSYSTEM ALGORITHM

```
Input Query Fingerprint
{
  if (Fingerprint matched with template)
    {
    then check the fingerprint of DBA's / Authorized Person of Organization
    if (Fingerprint matched)
          {
           // Again apply the cryptography key exchange scheme for authentication
                Use Diffie-Hellman Key Exchange Algorithm
                After process if K1=K2 then
         // Permission for accessing all secret data or Keys
        then print "You are an authorized person, please proceed"
          Generate or Show Secret message/Cryptography key / any secret data
          //The data generated to be used in concerned work and proceed further
```

} else print "You are not an authorized person for the concerned work"
}
else print "Fake Input Query fingerprint Try Again"
}

Diffie- Hellman Key Exchange Algorithm

Step 1- The user1 and officials agree on the algorithm parameters p and g,the two prime numbers.
Step2- The both generate their private keys, named x & y.
Step3- User1 computes A= g^x mod n and sends it A to officials.
Step4- Officials computes B=g^y mod n and sends it B to user1.
Step5- User1 computes K1= B^x mod n and send it to officials.
Step6- Officials computes K2= A^y mod n and sends it to user1.
Step7- if K1=K2 then it is secure connection.

11. THESIS WORK

The proposed approach was implemented on the FVC2004-DB1, a public domain database with 400 images (100 fingers 4 impressions each finger), cropped into 640x480 sizes, 500 dpi resolution. We apply the following step by step procedure and get correct result.

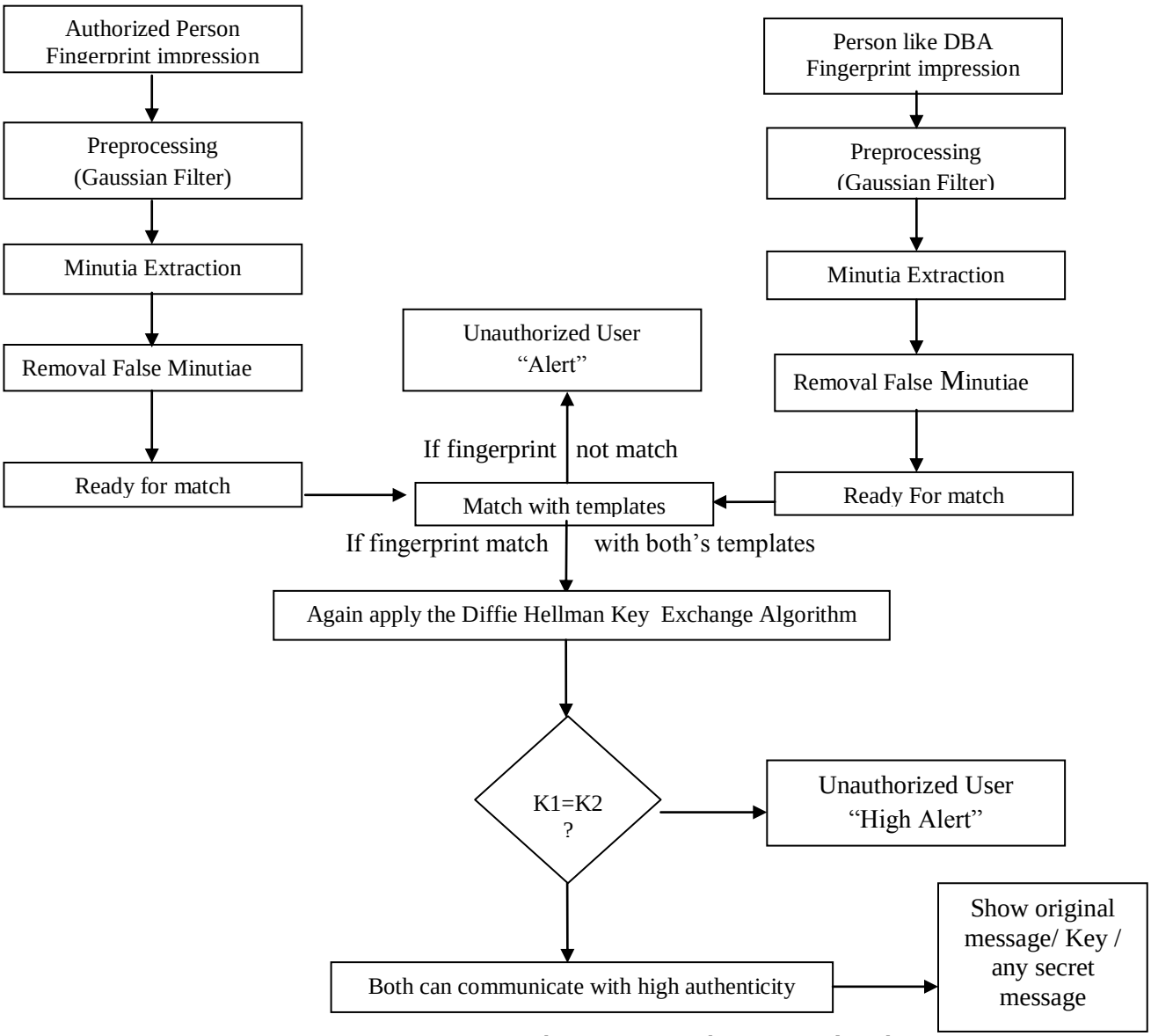


Fig 1.8: Biometric Cryptosystem with Fingerprint Authentication Algorithm

12. EXPERIMENTATION RESULTS

Table 1.1: Simulation results of Gaussian filter based fingerprint matching with different Threshold value.

Gaussian Filter	TH_V=1	TH_V=2	TH_V=3	TH_V=4
FRR	16.0%	12.0%	10.0%	8.8%
FAR	0.20%	0.46%	1.80%	1.92%

The simulation results are shown in Table [1.1]. We get a better result by using Gaussian Filter, it is based on two parameter FAR and FRR.

13. CONCLUSION

Cryptography and Biometrics have been as competing technologies nowadays and very much useful in Digital environment for security purpose. The two developed technologies activities in isolation, sometime in competition to each other. For different types of security problems the adding between these two aspects has create to the establishment of new biometric cryptosystem. Based on this merging system, the biometric cryptosystem categorized into many modes like use RSA algorithm, use public key cryptosystem etc and in biometric we can use another filter and methods. We can also use fingerprint as a key for cryptographic system and in this thesis work if fingerprint matched then we use another method of key exchange, if the keys are matched now then we release the cryptographic key or secret message or any other data released from its secure location, like as a server etc. The biometric cryptosystem can be carried out in three different modes: fingerprint matching, key matching or key generation, binding to both and we can say it is 3-tire security. The biometric matching is very risky process and in this thesis work, we take two important aspects first one is False Accept Rate (FAR) and other one is False Reject Rate (FRR). The increases FAR are more dangerous thing then FRR because if FAR is low then any unauthorized person can enter in our system so we have taken a best filter to reduce the FRR and increase the FRR. In this thesis work the fingerprint image quality assessment by using Gaussian filter analysis. This algorithm used good analysis level in evaluating fingerprint image. The benefit of this algorithm is that it concluded in deciding on the enrolment rejecting or accepting as well as on the type of image enhancements technique that is needed. This is developed by MATLAB (Matrix Laboratory) and related technology.

Refrences

[1] Tabassam Nawaj, Saim Parvaiz,Arash Korrani, Azhar-Ud-Din," **Development of Academic Attendance Monitoring System Using Fingerprint Identification**", International Journal of Computer Science and Network Security (IJCSNS), Vol. 9, No.5, pp.164-168, 20 May 2009.

[2] Peihao Huang,Chia Yung Chang, Chaur-Chin Chan" **Implementation of An Automatic Fingerprint Identification System**",IEEE ,EIT,2007 Proceeding ,p.p. 412-417, 2007.

[3] G.Sambasiva Rao, C.Nagaraju, Dr.L.L.S. Reddy, Dr.E.V.Prasad"**A Novel Fingerprint Identification System Based on The Edge Detection**", International Journal of Computer Science and Network Security (IJCSNS), Vol. 8, No.12, pp.394-397,20 December 2008.

[4] Lei Zhang , Mei Xei, " **Realization of A New Style Fingerprint Recognition System Based on DSP**" Proceeding of 2008 IEEE International Symposium on IT in Medicine and Education,p.p. 1107-1111, 2008.

[5] Shunshan Li, Min Wie,Haiying Tang,Tiange Zhuang ,Michael H. Buonocore"**Image Enhancement Method for Fingerprint Recognition Method**", IEEE proceeding, Engineering in Medicine and Biology 27th annual Conference, Shanghai, Chaina, p.p.3386- 3389, September 1-4, 2005.

[6] Xiaolong Zheng, Yangsheng Wang" **Fingerprint Matching Based On Ridge Similarity** ", IEEE proceeding ,ICASSP,p.p. 1701-1704, Year 2008.

[7]**.** Tsong-Liang Huang, Che-Wei Liu,Jui-Peng lin,Chien-ying li,Ting-Yi Kuo,**"A Novel Scheme for Fingerprint Identification"**IEEE ,CRV- 2005.

[8]. Milene Arantes, Alessandro Noriaki Ide, Jose Hiroki Saito **"A System for Fingerprint Minutia Classification and Recognition"** IEEE, vol. 5., pp-2474-2478, ICONIP-2002.

[9]. A.K Jain, L. Hong, and R. Bolle, **"On-Line Fingerprint Verification",** IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-313. Apr. 1997,

[10]. Maya V. Karki, Dr. S.Sethu Selvi"**a Novel Fingerprint Recognition system with Direction angles Difference ",**IEEE, proceeding on ICCIMA, pp. 501-505, 2007.

[11]. Thai Raymond," F**ingerprint Enhancement and Minutiae Extraction**".
[12]. D. Simon-Zorita, J. Ortega-Garcia, S.Cruz-Llanas and J.Gonzalez-Rodriguez" **Minutiae Extraction Scheme for Fingerprint recognition System"** IEEE**,** pp. 254-257, vol-3 Oct, 2001.
[13]. Jiang and W.Yau,"**Fingerprint Minutiae matching Based on the Local and Global Structure**", proc. 15th Int'l Conf. Pattern Recognition, vol. 2,pp 1038- 1041, Sept. 2000.
[14]. Amengual, J. C., Juan, A., Prez, J. C., Prat, F., Sez, S., and Vilar, J. M. "**Real-Time Minutiae extraction in Fingerprint Images",** IEEE, Proceedings of the 6th International Conference on Image Processing and its Applications, pp.871–875, July 1997.
[15]. A Wahab, S.H. Chin, and E.C. Tan,"**Novel Approach to Automated Fingerprint Recognition",** IEEE ,Proceeding on Vision, image and Signal Processing, vol. 145, no. 3, pp. 160-166, June 1998.
[16]. David Maltoni, Dario Maio, Anil k Jain, Salil Prabhakar," **Hand Book of Fingerprint Recognition",** Springer Verlag, New York, NY, USA, June 2003.
[17]. S.A. Cole. Suspect Identities " **A History of Fingerprinting and Criminal Identification**" ,IEEE, Harvard University Press, Cambridge, Massachusetts,London, England, 2001.
[18]. Marie Sandstrom, "**Liveness Detection in Fingerprint Recognition System",**A Thesis, Linkoping 10th June 2004.
[19]. Markus Huppmann"**Fingerprint Recognition by Matching of Gabor Filter-based patterns**",15th January 2007.
[20]. Wu zhili" **Fingerprint Recognition**", Hong Kong Baptist University, A Thesis 19th April 2002.
[21]. N. Ratha, S. Chen and A.K. Jain, "**Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images**", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.
[22]. D.Maio and D. Maltoni" **Direct Gray-scale Minutiae Detection in Fingerprints",** IEEE Trans. Pattern Anal. And Machine Intell., vol-19(1), pp: 27-40, 1997.
[23]. L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui "**Intelligent Biometric Techniques in Fingerprint and Face Recognition**", , the CRC Press. 1999.
[24]. http://www.biometrics.org.
[25] S. Pannirselvam, P. Raajan **"** An Efficient Finger Print Enhancement Filtering Technique with High Boost Gaussian Filter (HBG)" , International Journal of Advanced Research in Computer Science and Software Engineering, pp- 370- 378,Vol 2, Issue 11, Nov 2012.
[26] Ginu Thomas, K.Rahimunnisa, Sonima Parayil "Efficient Cryptographic Key Generation Using Fingerprint" International Journal of Scientific & Engineering Research,pp 942-945, Vol 4, Issue 4, April-2013.
[27] Mouad .M.H.Ali , Vivek H. Mahale , Pravin YannawarA. T. Gaikwad ," Overview of Fingerprint Recognition System" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 , IEEE, Nov 2016.
[28] Jucheng Yang, Shanjuan Xie, Sook Yoon, Dongsun Park, Zhijun Fang, Shouyuan Yang, "Fingerprint matching based on extreme learning machine" in Neural comput& applic, London:Springer-Verlag, vol. 22, pp. 435-445, 2013.