ISSN:0975-9646

Protecting the Finger Print Template by Fusion of Ridges and Texture

Vidyasree.P[1] , Dr.G.VenkataRamiReddy[2]

[1]*Scholar of SIT JNTUH ,*
[2]*Asso.Professor of CSE-SIT, JNTUH*

Abstract -In the real life scenarios usage of single modal biometrics are significantly getting increased but due to spoof attacks , data quality and the noise, these factors are degrading the performance of single modal biometrics. In this aspect multimodal biometrics are being used but these are very cost effective due to fusion of different traits as a single trait. And this multimodal biometrics is also an huge process which doesn't suits for the small applications like attendance or for checkin or checkout or security lock for mobiles etc . In these situations providing the security for those applications by fusion of two or more features of a single trait as one feature. This type of fusion can be done at feature level or score level or at decision level etc. By the fusion of different features performance and accuracy levels are high compared to access of individual features in a single trait. This method helps in reducing the cost, providing the authentication in identifying the legitimate user and also ensures to access the user requesting services. These system can provide security to access the buildings, computer laptops, mobile phones and ATM's etc.

Keywords – Authentication, Features, Fusion, single modal biometrics.

1. INTRODUCTION

Security is the main factor in any area of the current society. Traditionally security is gained by the username and password or by the id cards which restricts the access of the system. But the passwords are getting hacked by the hackers and easy password are easy to guess and difficult passwords are difficult to remember by the authorized users and the id cards are morphed by the impostors. To address these problems biometrics played a very prominent role helps in providing the authentication to legitimate user[4]. By certain psychological and behavioral traits of a person helps in biometric identification and verification. Identification refers to one to many relationship whether he is an authenticated[5] person or not and the verification refers to the one to one relationship to know whether the data is belonging to particular person or not. These identification and verification phases are chosen according to the requirement[6]. Biometric helps in identifying " Who are you?" rather than "What you possess?" which is done on the ID cards.

Biometric systems make use of finger prints [1], iris , hand, palm,[14] DNA, voice etc traits are being used inorder to find out the authenticated person. These traits are used according to the situations and security levels[8,9]. These are difficult to lose ,forge, spoof and hack the biometric data and also overcomes all the difficulties of traditional methods like cost, reduces the large database storage of passwords, remembrance of passwords for different applications. Traditionally different passwords are used to secure the different applications in this aspect the users has to remember too many passwords which leads to headache and wastage of the memory in the database and the user always has to do the data mining because in order to retrieve the right password and to open the application. In this scenario according to the human's psychology they will keep the same password for different applications, if the hacker knows one password he can hack the data of the different applications. The main limitations of the traditional method are :

- Cost of data storage.
- Remembering the huge number of passwords .
- Consumption of time to reset the password.
- Loss of data by forging ID cards and passwords.

In the first limitation the traditional methods are very much cost effective as the passwords reset and recollecting the passwords makes more than two hits to the database which makes in increasing of the cost. And the second limitation is remembering the huge number of passwords makes the user to get confused and feel tensed this may also leads to different health problems. And the third limitation is time factor which very important concept as traditional methods take lot of time whether to recollect or reset the passwords . In that duration the user can complete two or more works and can save the time. And the last limitation is loss of data which indicates the loss of security now a days hackers are using different techniques to hack the user's private data. In order to addresses these problems effectively biometrics plays an prominent role which leads to increases the users convenience and also can use different traits as passwords for different applications and also it eradicates the of recollecting the password. Biometric templates are created at enrollment time and these intervention are based on the users requirement, templates[15] are get stored in the database for further use for identification or for verification and this leads to two different problems with two different inherent complexities. Biometric are get deployed in many civilian applications for example, At Amsterdam airport passengers iris get scanned at the enrollment phase and used in passport and visa verification to speed up the process[8,9]. These scanned code is given in users identity card where the passengers are used at the entrance and here is send for the verification where the passenger has to see in to camera where the iris get scanned and code get generated. This iris code is used for comparison of already registered iris code which was stored in database during the

enrollment phase and the person get identified whether he/ she is an original passenger or fraud. Same procedure is get carried out for the workers in the airport to check whether the particular worker is an valid employee or not.
Simple biometric system has four modules:

1. Sensor module :
   In this module sensor captures the image of biometric data. For example fingerprint[1] impressions of the user is captured by the finger print sensor.
2. Feature Extraction module :
   The minutiae points size, orientation and position are get extracted in this level if we consider the finger print . In this level features of each and every trait get extracted and send to further process.
3. Matching module :
   The minutiae points which was extracted from query is compared with the minutiae points of already registered template [15]by generating matching score.
4. Decision – Making module:
   The user is accepted or rejected is decided in this phase based on the matching score.

The above process is carried out for every biometric trait and also it also applicable for fusion of biometric traits. Providing the security for small applications by finger and palm print[14] etc. In this paper, we made analysis on traditional methods like passwords and ID cards etc and their drawbacks, how the biometrics are addressing the problem of traditional methods and internal process of the biometrics We will design an example for proposed process with help of finger print and face recognition systems later the proposed scheme can be applicable for fusion of palm, iris, face or other kinds of biometric recognition systems. The rest of the paper is organized as follows. Section 2 analyzes the detail description of fingerprint recognition system. Section 3 states different fusion methods in different phases. Section 4 Shows an example for gaining the high level security with the help of fusion of different features from single trait and finally Section 5 concludes the paper .

2. DETAIL ANALYSIS ON FINGERPRINT RECOGNITION SYSTEM:

In biometric traits, fingerprint recognition system is very important trait as it provides high level reliability and the fingerprint[2] indicates the ridges flow and the tip of the finger these features provide the authentication and they are widely used in criminal's investigation by experts[5,6]. Fingerprints varies from one individual to another individual and also it will not be same with other fingers of the same individual[2]. There are some anomalies in the fingerprint tip by changing the position and orientation of the finger[10] matching is being performed. These anomalies are termed as minutiae and these minutiae lays on the ridges which are unique from one person to another person.
Now days sensors are embedded in the laptops mouse and keyboards etc, in this aspect very small contact area is being selected from the finger tip , its senses only limited portion from the fingerprint images[12] so it generates a high complicated problems as it does not read the full images. When at the registration phase the full image is get scanned but this embedded sensors only partial portion this may leads to false rejection error it may tell the valid user as the invalid user. In order to avoid this problem fusion mechanism[16] are being implemented additionally it also provides the high accuracy rate.

2.1 NECESSITY OF MULTI REPRESENTATION

1. COST:
By considering the whole trait all the features must get extracted and verified at the authentication this leads to high computation cost.

2. Time:
It requires lots of time to handle the whole trait either for authentication or for verification. In this aspect excess of time may be taken for processing speed may be reduced.

3. False Rejection/ False Acceptance
If there is any cut or any wound on the finger it takes an authenticated user as an invalid user or chance of accepting the unauthenticated as an valid user because the template resembles as template of another user. It may result in loss of security.

4. Computational speed
Due to extraction of all features and verifying all the features every time may result in loss of speed of the system.
These vulnerabilities are handled by different types of fusion[17] .Let us discuss different fusion levels in detail.

3. DIFFERENT TYPES OF FUSION LEVELS

Fusion is a technique which integrates the information of single biometric trait[13] or by two or more traits[3]. This fusion can be performed at various levels.

- Fusion at Image acquisition level.
- Fusion at feature level.
- Fusion at score level
- Fusion at decision level.

1. Fusion at Image acquisition level:
Fusion is performed after getting an images from the sensor or any other devices, either it may be an two different traits or the different images from the single trait. After the fusion preprocessing is done from the fused image and then it continues the remaining process fig1.

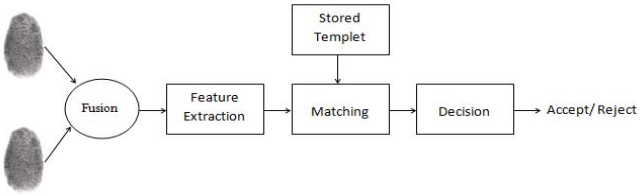

FIG 1: Image acquisition level fusion

2. Fusion at Feature extraction level :
The data from the different traits or different data of the single trait get extracted from the sensors and then features get extracted these features from different sources get fused and performs the remaining process fig 2.

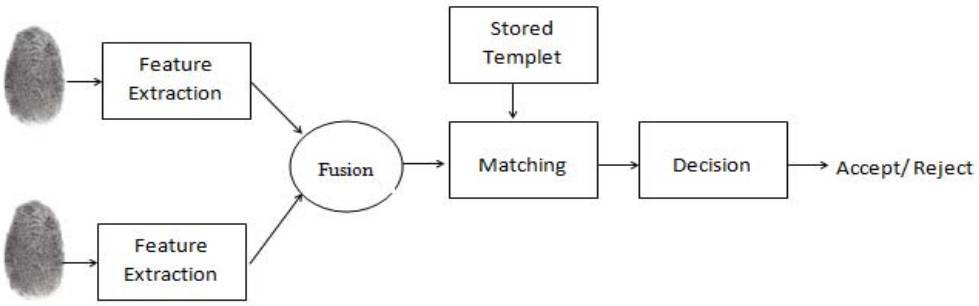

FIG 2: Feature level fusion

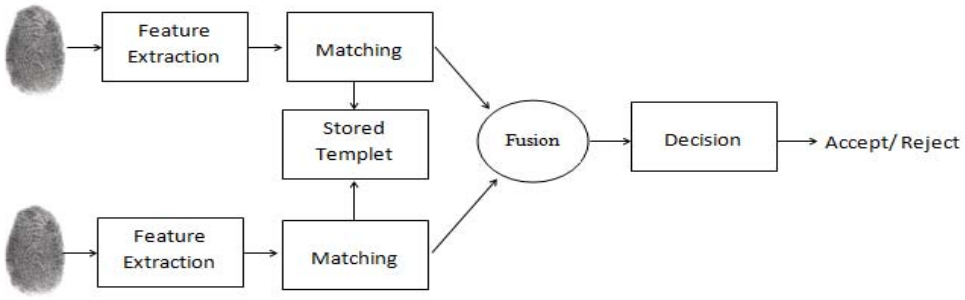

FIG 3: Matching level fusion

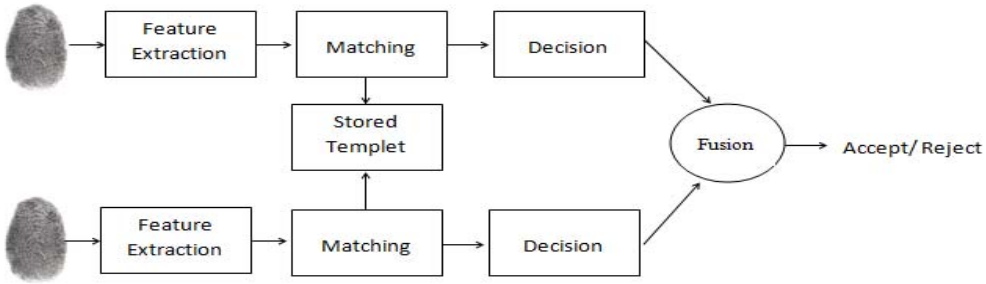

Fig 4: Decision level fusion

3. Fusion at matching Level:

The system give the similar score by indicating the proximity of the input with the query image and to gain the veracity these scores get fused which are extracted from different sensors or different traits or different input from the same trait these help in reducing the FAR and FRR errors fig3.

4. Fusion at Decision Level:

At this level each and every decision get noted which was generated from different biometric [3,13]sources from the individual process and majority votes policy are taken to make a final decision on the basis of decisions like accept or reject fig 4 .

Security is highly gained by these different fusion techniques but opting the apt fusion technique leads to enhance the accuracy level in finding the authenticated user. Spoofing of the template[14] due to considering the whole texture if any feature is known to the intruder the data can be easily hacked. These type of problems are avoided by our proposed system.

4.PROPOSED TEMPLATE PROTECTION BY FUSION

In the proposed system template security is gained through fusion of texture and ridges. In this scenario first the user has to get registered with some specified primary details and these are get verified and get handled accurately. At the time of registration the finger print of the authenticated user get enrolled. This enrolled template get preprocessed and extract the features at that time only fusion must be performed. For extraction of the ridges using the Hough transformation and for extraction of the texture using SFTA algorithm i.e. Segmentation-based Fractal Texture

Analysis. Extracting the features from the finger use the function as

sfta(I,nt)

Where I is the input gray scale image and nt is the size if the feature vector and it returns the 1 by 6*nt vector.

I= imread('fig.png')

V=sfta(I,4)

In this process the input image is extracted and was decomposed into different set of binary images and the segmented texture[11] patterns are derived from the fractal dimensions of the resulting regions of the processed image. And the ridges are get extracted using Hough transformation after the fusion of these two features random triangles are get generated using the random function and hashing is done on the fused points in the triangle. If there are five points the hash value is written as 5 and get binarized as 111110000 and this binary get stored in to the database.

After the authentication phase when the user get verified and termed as authenticated user or not by one to one technique by undergoing whole process and finally computed binary value get verified with the enrolled binary value if they got matched user is an authenticated one or else user is an unauthenticated user. By this proposed system time can be saved and cost can be minimized as the system process only on single trait no need to require different devices as in the multi model system. Gaining high security using the multi representation fusion helps in increasing the accuracy level as extracting the more features from small part of the finger cannot be detected by the intruders as they are taken as random Fig 5.

Authentication

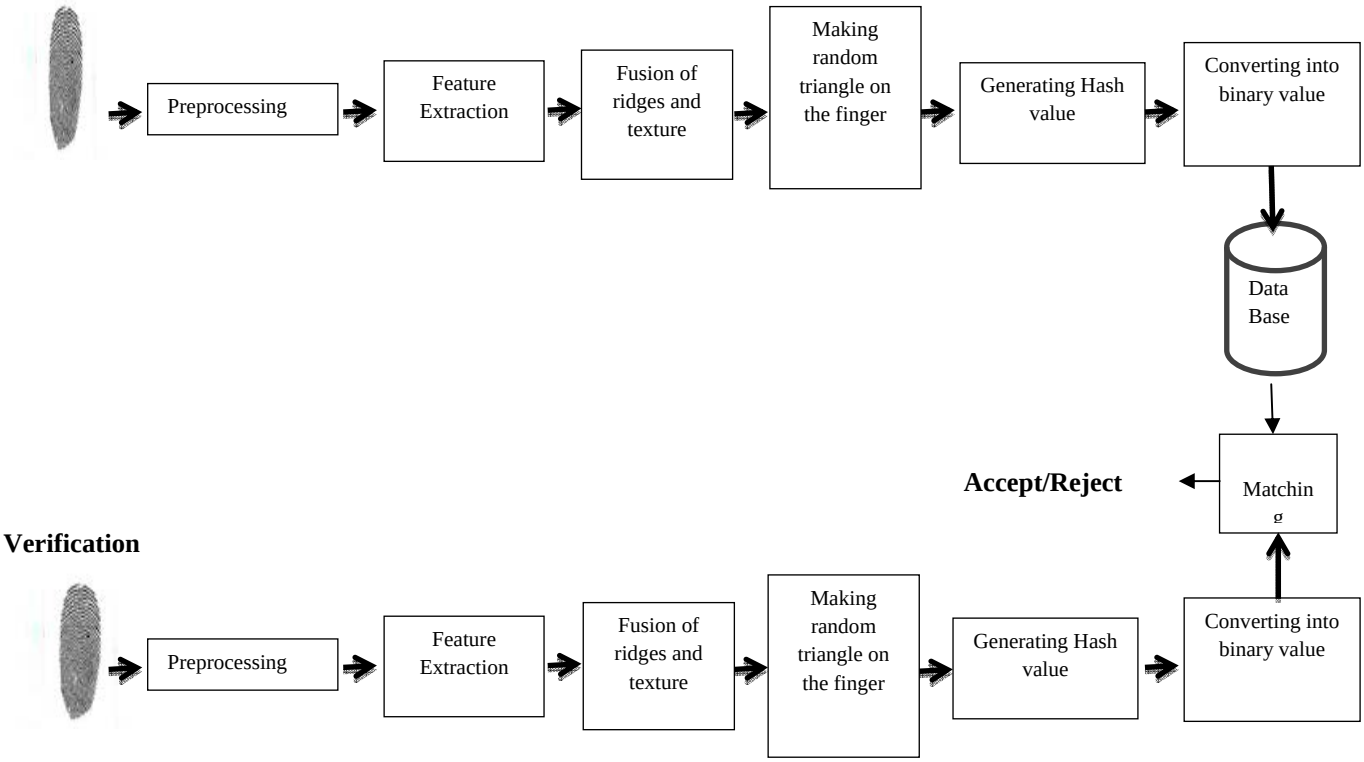

Fig5: Architecture for proposed system by fusion of ridges and texture

In the above figure user get registered and get preprocessed and that image is given as input to the feature extraction phase where the texture and ridges [11]of the finger get extracted using the sfta and Hough transformations and get fused in the feature level. And on this fused image random triangle is done and the few fused points in that triangle get noted for example they are 8 points it represents the hash value and binary value get generated as 1111111100000000 and make certain triangle for the same finger and range is calculated. As at the verification phase when the user get done through the same process and the average of the match score is with in the range the user is an authenticated or else the user was an unauthenticated and get rejected.

5.CONCLUSION

Security is only concept where different techniques and different methods are evolving to enhance them in various levels. Apart from that not only security accuracy also consider as a primary factor in present society. So in this aspect achieving these two concepts by our multi representation technique where different features get fused which results in reduce of cost and the random triangle hashing helps in achieving the accuracy. And also helps to reduce the false acceptance and false rejection error rate and this also helps to reduce the fraud done by the intruders and this paper provides the conceptual approach which is used to enhance the security and accuracy levels by using simple techniques and methods.

ACKNOWLEDGMENT

First, we want to thank our director Dr.GOVARDHAN & library of JNTUH, who have given their constant support in enriching our knowledge of research in the area of Biometrics. We would like to express our gratitude to all the referees authors of the research papers, who have helped directly or indirectly the possibility to complete this paper.

REFERENCES

[1] A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," IEEE Transactions on PAMI, vol. 19, pp. 302–314, April 1997.

[2] L. Hong, "Automatic personal identification using fingerprints," PhD Thesis,Michigan State University, 1998.

[3] A. K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[4] J. L. Wayman, "Fundamentals of biometric authentication technologies," International Journal of Image and Graphics, vol. 1, no. 1, pp. 93–113, 2001.

[5] L. O'Gorman, "Seven issues with human authentication technologies," in Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID),(Tarrytown, New York), pp. 185–186, Mar 2002.

[6] R. Yasin, "Password pain relief," Information Security Magazine, April 2002. Available at http://www.infosecuritymag.com/2002/apr/cover.shtml.

[7] J. Daugman, "Statistical demands of identification versus verification." Available at http://www.cl.cam.ac.uk/users/jgd1000/veri/veri.html.

[8] "Schiphol backs eye scan security." CNNWorld News, March 27 2002. Available at http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/.

[9] J. Daugman, "Recognizing persons by their iris patterns," in Biometrics:Personal Identification in a Networked Society (A. K. Jain, R. Bolle, and S. Pankanti, eds.), pp. 103–121, Kluwer Academic Publishers, 1999.

[10] J. Berry and D. A. Stoney, "The history and development of fingerprinting," in Advances in Fingerprint Technology (H. C. Lee and R. Gaensslen, eds.), pp. 1–40, Florida: CRC Press, 2nd ed., 2001.

[11] A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint matching using minutiae and texture features," in Proc. International Conference on Image Processing (ICIP), (Thessaloniki, Greece), pp. 282–285, Oct 2001.

[12] L. Hong, Y.Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithms and performance evaluation," IEEE Transactions on PAMI, vol. 20, pp. 777–789, Aug 1998.

[13]. Dr.S.ViswanadhaRaju,P.Vidyasree, Madhavi Gudavalli" Reinforcing The Security In India's Voting Process Through Biometrics" International conference on Advanced computer science and information technology Chennai September 2014.

[14]. Dr.S.ViswanadhaRaju,P.Vidyasree, Madhavi Gudavalli" Ameliorating The Security Of Palm Print Biometric Template Using FEC"National conference by NCETCS'14 in JNTU vijayanagaram.

[15] .Dr.S.ViswanadhaRaju P.Vidyasree, Madhavi Gudavalli" Enhancing Security Of Stored Biometric Template In cloud Computing Using FEC"International conference on cloud computing Tirupathi January 2014.

[16]. Madhavi Gudavalli, Dr.S.Viswanadha Raju and Dr.D.Srinivasa Kumar, "An Overview on MultiModal Biometrics-Sources, Architecture & Fusion Techniques", CIIT International Journal of Biometrics & Bioinformatics, Vol 3, No 11, PP. 516-519 , December 2011.

[17]. Madhavi Gudavalli, Dr.S.Viswanadha Raju, Dr.A.Vinaya Babu and Dr.D.Srinivasa Kumar, "MultiModal Biometrics-Sources,Architecture & Fusion Techniques: An Overview ", IEEE-International Symposium on Biometrics and Security Technologies(ISBAST'12), Taipei, Taiwan, March 26-29, 2012.