Minutiae extraction System from Fingerprint

Thaseen Bhashith[1], Pushpa R N[2], Sreedevi S[3]
[1,2,3]Assistant Professor, Department of Computer Science and Engineering
Jawaharlal Nehru National College of Engineering, Shivamogga, Karnataka, India

Abstract- An individual is identified based on her or his unique physiological attributes such as retina, fingerprints, ace and iris or behavioral attributes. Fingerprint recognition is one of the most trustworthy identification techniques of all the biometrics technologies[4]. Most of the time a part of the fingerprints (minutiae) is available left unintentionally at the surfaces of the crime scene. They are an important evidence to identify criminals in law enforcement agencies. This minutia is usually of poor quality consisting of complex background with a lot of unknown patterns. Traditional methods are usually based on the local features such as gray scale variance and gradients, which are sensitive to noise and cannot work well for images[1]. First, a texture image is obtained by decomposition of image with a total variation model. Second, it is propose to detect the ridge segments from the texture image, and then compute the density of ridge segments and ridge orientation consistency to characterize the global and local fingerprint patterns. Then, fingerprint segmentation is performed by combining the ridge density and orientation consistency for images. Finally these minutiae are matched with the fingerprints. Experimental results and comparison demonstrate the promising performance of the proposed method.
Keywords – Minutiae, KNN, fingerprint images, minutiae extraction, ridge endings, ridge bifurcation, fingerprint recognition, Euclidean Distance

I. INTRODUCTION

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be an image or characteristics associated with that image. Image processing involves changing the nature of an image in order to either 1. Improve its pictorial information for human interpretation. 2. Render it more suitable for autonomous machine perception. Digital image processing involves using a computer to change the nature of a digital image. It is necessary to realize that these two aspects represent two separate but equally important aspects of image processing. Humans like their images to be sharp, clear and detailed whereas machines prefer their images to be simple and uncluttered. Image defects which could be caused by the digitization process or by faults in the imaging set-up can be corrected using Image enhancement techniques.

AThe purpose of minutiae extraction is to identify the diplomat features of minutiae from the image. It is very complicated to opt for the prominent and accurate demonstration of the images. It must include the following properties. I Easy to compute. II amenable to matching algorithm. III Compactness. IV Retain discriminating of raw digital fingerprint images and, V Robust to noise and distortion.

The first property reveals that the demonstration should not be too complex in computation. The second property, it is given that the demonstration should be appropriate for a matching algorithm. The third property insists that the demonstration should be represented concisely and clearly. The fourth property says that the individuality of fingerprints should be maintained by demonstration, i.e. the demonstration can be established by the identity alone. The last property postulates that the demonstration should be strong enough to tolerate noise and distortions, i.e. it represents the quality of fingerprint images. Figure 1 shows a minutiae extraction system which involves three stages. Before extracting the features, preprocessing includes the different steps like minutiae segmentation, orientation, minutiae enhancement, classification and ridge thinning [12].

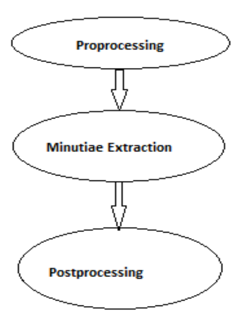


Figure 1: Minutiae extraction system

Preprocessing: Once the image is in good condition, the measurement extraction operations can be used to obtain useful information from the image. The pixel connectivity describes a relation between two or more pixels. For two pixels to be connected they have to fulfill certain conditions on the pixel brightness and spatial adjacency. First, in order for two pixels to be considered connected, their pixel values must both be from the same set of values V. For a grayscale image, V might be any range of gray levels, V= {22, 23, ….., 40}, for a binary image V={1}. To formulate the adjacency criterion for connectivity, the notation of neighborhood is introduced. For a pixel p with the coordinates (x, y) the set of pixels given by:

N4 (p) = {(x+1, y), (x-1, y), (x, y+1), (x, y-1)}

is called its 4-neighbors. Its 8-neighbors are defined as

N8 (p) = N4 U {(x+1, y+1)}, (x+1, y-1), (x-1, y+1), (x-1, y-1)}

From this it can be inferred that the definition for 4-connectivity and 8-connectivity is: Two pixels p and q, both having values from a set V are 4-connected if q is from the set N4(p) and 8-connected if q is from N8(p). A pixel p is connected to a pixel q if p is 4-connected to q or if p is 4-connected to a third pixel which itself is connected to q. Or, two pixels q and p are connected if there is a path from p and q on which each pixel is 4-connected to the next one. A set of pixels in an image which are all connected to each other is called a connected component. Finding all connected components in an image and marking each of them with a distinctive label is called connected component labeling. An example of a binary image with two connected components which are based on 4-connectivity can be seen in Figure 2. If the connectivity were based on 8-neighbors, the two connected components would merge into one.

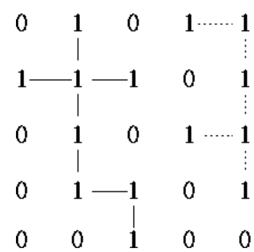
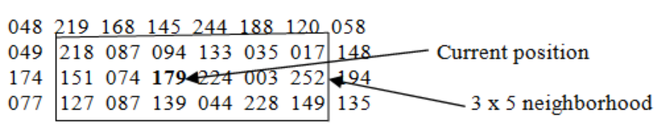


Figure 2: Two connected components based on 4-connectivity.

Each of the pixels that represent an image stored inside a computer has a *pixel value* which describes how bright that pixel is, and/or what color it should be. In the simplest case of binary images, the pixel value is a 1-bit number indicating either foreground or background. For a gray scale images, the pixel value is a single number that represents the brightness of the pixel. The most common *pixel format* is the *byte image*, where this number is stored as an 8-bit integer giving a range of possible values from 0 to 255. Typically zero is taken to be black, and 255 is taken to be white, values in between make up the different shades of gray.

To represent color images, separate red, green and blue components must be specified for each pixel, and so the pixel value is a vector of three numbers. Often the three different components are stored as three separate grayscale images known as *color planes*. Multispectral Images can contain even more than three components for each pixel, and by extension these are stored in the same kind of way, as a vector pixel value or as separate color planes.

Often, all that is stored for each pixel is an index into a color map in which the actual intensity or colors can be looked up. Although simple 8-bit integers or vectors of 8-bit integers are the most common sorts of pixel values used, some image formats support different types of value, for instance 32-bit signed integers or floating point values. If this approach is used then it is usually necessary to set up a color map which relates particular ranges of pixel values to particular displayed colors. A selected pixel say 179 in its 3 x 5 neighborhood is represented as shown below.



Minutiae Extraction: Most fingerprints' minutia extraction methods are thinning based where the skeletonization process converts each ridge to one pixel wide. Minutia points are detected by locating the end points and bifurcation points on the thinned ridge skeleton based on the number of neighboring pixels[9]. The end points are selected if they have a single neighbor and the bifurcation points are selected if they have more than two neighbors. The main problem in the minutiae extraction method using thinning processes comes from the fact that minutiae in the skeleton image do not always correspond to true minutiae in the fingerprint image. These local ridge characteristics are not evenly distributed[9]. Most of them are depend on the impression condition and quality of minutiae. The two prominent local ridge characteristics are ridge ending and ridge bifurcation. Each of the ridge endings and bifurcations types of minutiae has three attributes: X-coordinate, Y coordinate and the local ridge direction (θ).

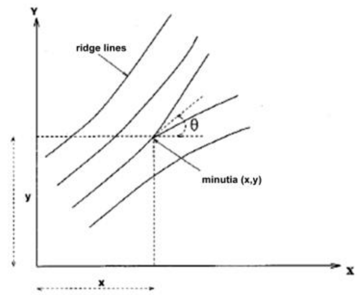


Figure 3: Components of minutiae features

Another high-level feature is the ridge density. Ridge density can be defined as the number of ridges per unit distance. In order to make it invariant to position, the ridge density between two singular points is computed. Some points of interest are Core and Delta points. The Core point is the top most point on the inner most ridge and a Delta point is tri-radial point in with three ridges radiating from it is as shown in the figure 4.

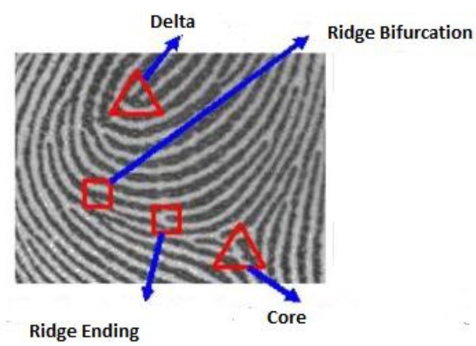


Figure 4: Ridge bifurcation, Ending, Core and Delta

Post-Processing: A post-processed image is the starting point of minutiae extraction. Though it is a very defined image, it will have deformations and forged minutiae that required to be filtered out. Since minutiae are very rarely adjacent, an algorithm may abolish one of two adjacent minutiae. Scars sweat or dirt may cause irregular minutiae that appear as false minutiae when acquiring the fingerprint image. Algorithms should trace any points or patterns that do not produce sense, such as a spur on an island which maybe a false minutia. Then is has to identify a ridge crossing at right angles to two or three others that maybe a scar or dirt.

With post-processing stage, an outsized proportion of false minutiae are abandoned as shown in Figure 5. In false minutiae, a) a noisy line between two ridges constitutes the bridge, b) two very close lines with the same direction create the interrupted ridges, c) a fork is produced by two lines d) connected by a noisy line the short lines whose direction is orthogonal to ridges' direction are known as spurs, e) the pseudo rectangle between two ridges composes ladders, f) a genuine bifurcation with a noisy line between two ridges produces the triangles.

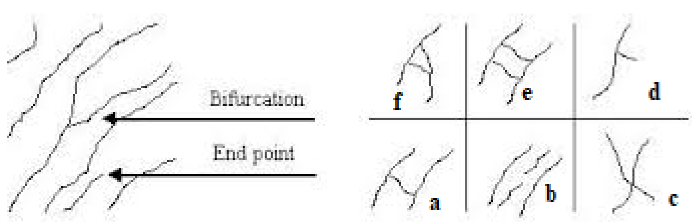


Figure 5: a) True Minutiae b) False Minutiae

II. PROPOSED ALGORITHM

System design defines the architecture and behavior of modules and data. System design shows the step by step implementation of the modules that defines the entire system. System design of extraction and analysis of minutiae for a fingerprint as shown in Figure 6 which includes the following stages

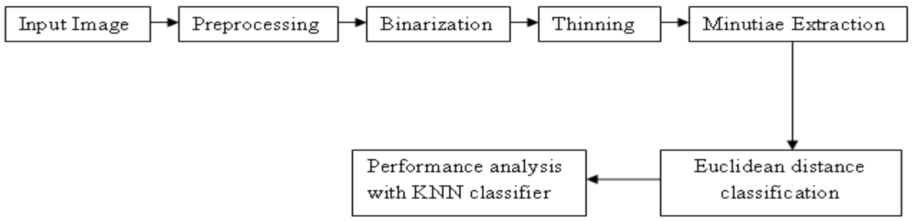


Figure 6: Implementation of extraction and analysis system of minutiae for a fingerprint

Input Image: The first step is to acquire the input image from the database. Database are then given as input to the pre-processing techniques which can be like shown in the Figure 7.

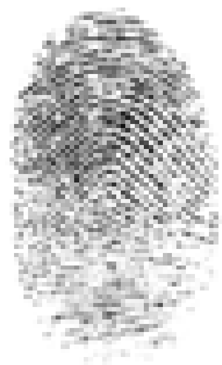


Figure 7: Original Image

Preprocessing: The main objective of the preprocessing technique is to boost the image knowledge by suppressing the unwanted distortions and enhancing the image options. Image enhancement technique includes two processes for the reduction of noises and for the better acquisition of image.

Binarization

Ridge Thinning

Binarization is a necessary process for minutiae extraction. Intensity of the ridges is neutralized using adaptive binarization that transforms a 256 level image into 2 level image (Black-0, white-1). The grayscale image is transformed into black and white colour image with respect to the determined threshold value.

Threshold value > pixel value = Black

Threshold value < pixel value = White

Ridge thinning is a method of reducing the thickness of every line of patterns into one picture element. It improves the standard of the fingerprint binary image. Also, ridge thinning removes the redundant data, which would have resulted in longer process time and sometimes different results. A sample thinned image is depicted in Figure 8.

(a) (b)

Figure 8: Results of preprocessed fingerprint image
(a) Binarized image (b) Thinned image

Minutiae Extraction: A valid demonstration of a fingerprint is the pattern of the minutiae details of the fingerprint. It satisfies the basic properties like compactness, agreeable to matching algorithms, robust to noise and distortions and is easy to compute. A total of 150 diverse local ridge characteristics, called minutiae details, have been identified as shown in the Figure 7. Most of them are not enduring and cannot be consistently recognized, and they depend deeply on the impression conditions.

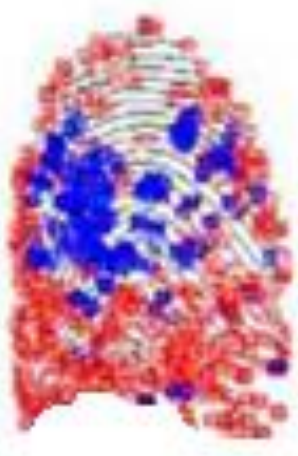
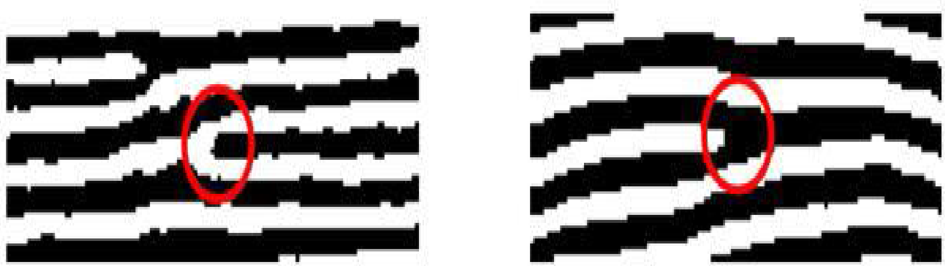


Figure 7: Minutiae Extraction

Ridge endings are the points where the ridge curve terminates, and bifurcations are where a ridge splits from a single path to two paths at a Y-junction. Figure 8 illustrates a ridge ending and a bifurcation. Here the black pixels correspond to the ridges, and the white pixels correspond to the valleys.



(a) (b)

Figure 8 : (a) Ridge ending (b) Ridge bifurcation

Accurate minutiae detection is an essential component for all minutiae based fingerprint recognition systems. Without accurate minutiae detection, the results and performance of a system are not reliable.

Euclidean Distance Classifier: In comparison of binary pictures distance play a necessary role within the fields of native features, morphological operations and distance between 2 points in a picture. Euclidean distance could be a natural distance between 2 points that is usually mapped with a ruler. The distance between trivia points during a fingerprint image is calculated. If x values are x1, x2 till xn and values of y are y1, y2 till yn are the two points in Euclidean space then the distance from P to Q is given by

$$d(x,y) = d(y,x) = \sqrt{\sum_{i=0}^{n}(y_i - x_i)^2}$$

Matching method determines whether or not the two trivia sets are from identical fingers or not. Exploitation of Euclidean distance in minutiae based fingerprint matching offers correct matching results. Euclidean Distance could be a distance matching technique that is generally perusal in mathematical geometry and accuracy. If the distance is Zero then the input image and the query image is perfectly matched.

KNN Classifier :KNN is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure. It is one of the most used learning algorithm. KNN is a non-parametric lazy learning algorithm. Its purpose is to use a database in which data points are separated into several classes to predict the classification of a new sample point.

Method:

- Determine parameter K, the number of nearest neighbors.
- For each case in the target data set i.e the set to be predicted, locate the K closest neighbors of the training data set. An Euclidean Distance measure is used to calculate how close each member of the training set is to the target row that is being examined.
- Sort the distance and determine nearest neighbors based on the K-th minimum distance.
- Gather the catogaries of the nearest neighbors.
- Use simple majority of the category of nearest neighbors as the prediction value of the new query instance.
- Repeat this procedure for the remaining cases in the target set.

III. EXPERIMENT AND RESULT

Experimental database consist of 200 unique fingerprint images of males and females both. The fingerprints of 6 numbers for each person were collected. The fingerprint images collected were in the range of age from 10 to 90 years. After implementation and execution of the system, the snapshots of Graphical User Interface (GUI) is as in Figure 9.

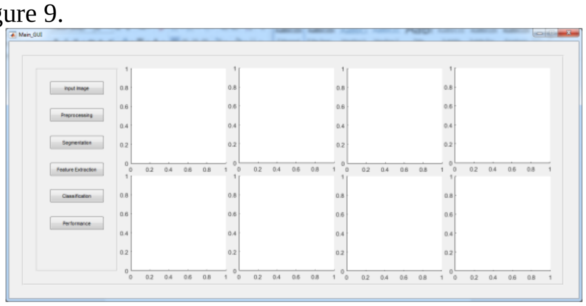


Figure 9: User interface of the system

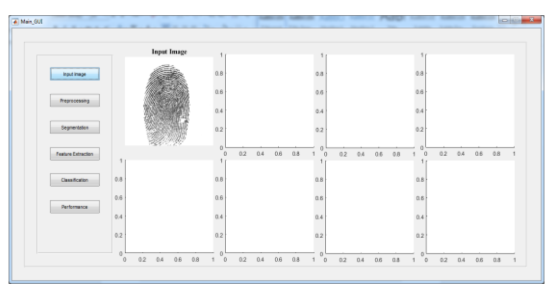


Figure 10: Input image for minutiae extraction

Figure 10 shows the user interface of the system that allows the user to interact with the system. It allows to input the image from the database to perform preprocessing. Fingerprint images are stored in the database. User can select one of the fingerprint image as input by clicking on the input image button as shown in the figure 10.

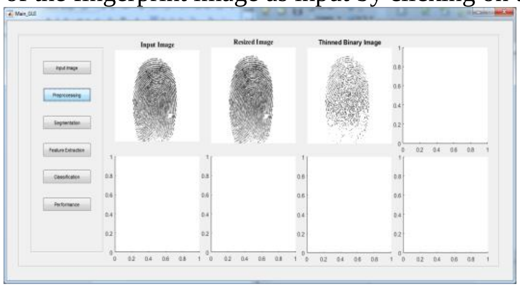


Figure 11: Input, resized and thinned binary image

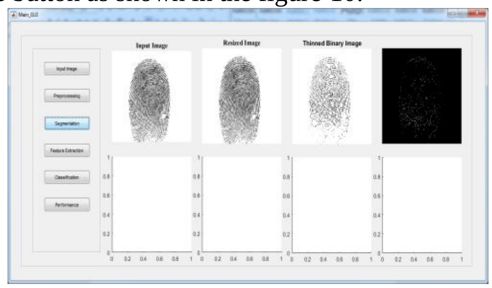


Figure 12: Minutiae extraction processing from the fingerprint

For the input fingerprint image, binarization and thinning as a part of preprocessing method as shown in the Figure 11.

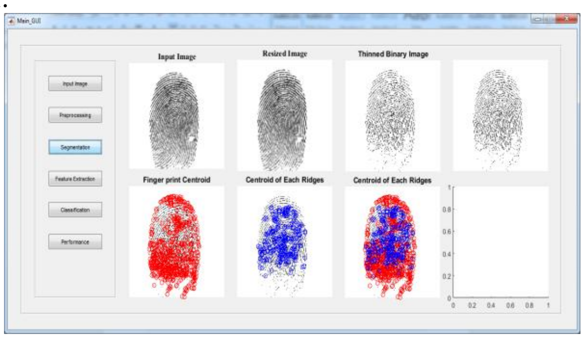


Figure 13: The centroid of the input fingerprint

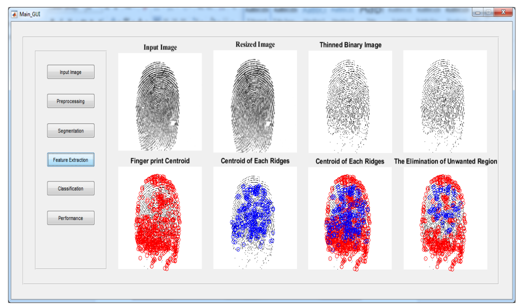


Figure 14: elimination of unwanted region from the fingerprint

Minutiae extraction processing from the thinned fingerprint image is as in the Figure 12. The extracted minutiae and its centroid is shown in the figure 13.Centroid of outer and inner ridges in the fingerprint image is calculated. Figure 14 shows the combined centroid of each ridges in the fingerprint image after eliminating unwanted region from fingerprint.

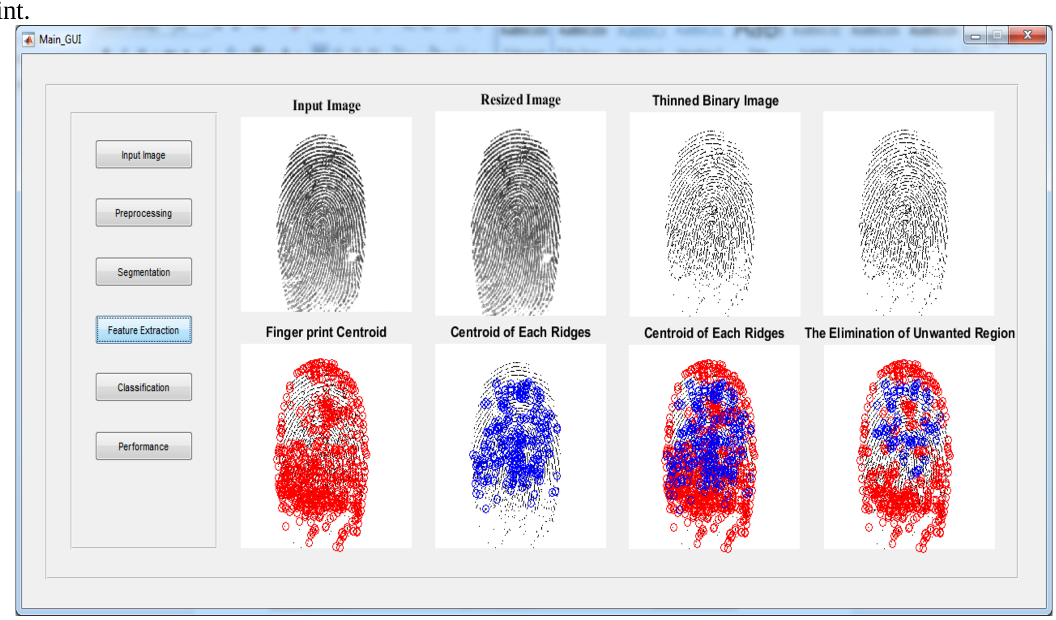


Figure 14: elimination of unwanted region from the fingerprint

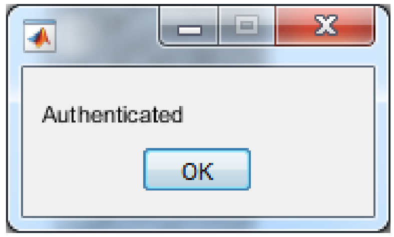


Figure 15: Authenticated message dialogue box

After obtaining the unwanted region from the combined centroid of fingerprint image, the authenticated message dialogue box is displayed if the extracted minutiae matches the input fingerprint image as in the figure 15.

The performance analysis in terms of accuracy, specificity and sensitivity after authenticated with input image is displayed as in the figure 16.

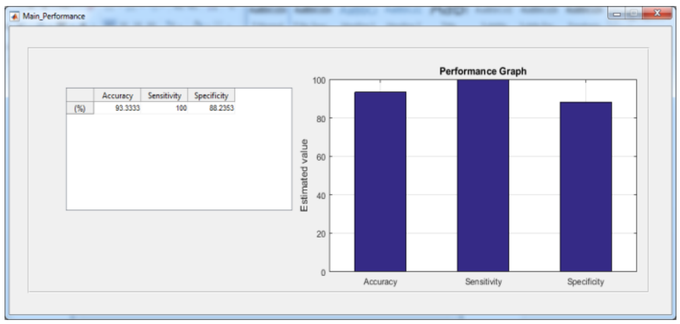


Figure 16: Performance Graph

IV.CONCLUSION

The recent and global attitude towards terrorism has influenced people and their governments to take action and be more proactive in security issues. This has resulted in renewed attention to the research on biometric methods[4]. Nowadays, there are many biometric security systems that use different human biometric characteristics for recognition. Examples include fingerprint, signature, face, hand, voice, iris, etc. Out of these, fingerprint is more frequently used because of its high uniqueness and ease of capturing. The primary objective is to propose a model that is based on fingerprints using minutiae features to identify persons efficiently in terms of accuracy. As the database of the genuine users increase, accuracy declines. This may be overcome by combining more modalities under different levels of fusion. The key issue in any of the personal authentication system is the matching time and feature extraction time. Hence efficient algorithms with multimodalities are still a challenging issue in biometric based personal authentication systems.

V. REFERENCE

[1] K. Nilsson and J. Bigun, “Localization of corresponding points in fingerprints by complex filtering,” Pattern Recognit. Lett., vol. 24, no. 13, pp. 2135–2144, 2003.

[2] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,” Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.

[3] D. Cai, X. He, and J. Han “Subspace learning based on tensor analysis”, 2005.

[4] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, “Multi-biometric templates using fingerprint and voice,” Proc. SPIE, vol. 69440I, pp. 69440I-1–69440I-9, 2008.

[5] D. S. Huang, W. Jia, and D. Zhang “Palmprint verification based on principal lines”, 2008.

[6] A. Nagar, K. Nandakumar and A. K. Jain “Biometric Template Transformation: A Security Analysis”, 2010.

[7] S. Li and A. C. Kot, “Attack using reconstructed fingerprint,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

[8] A. Ross and A. Othman “Mixing fingerprints for template security and privacy”, 2011.

[9] Roli Bansal, Priti Sehgal and Punam Bedi “Minutiae Extraction from Fingerprint Images - a Review “ IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011 ISSN

[10] Y. Wang and J. Hu “Global ridge orientation modeling for partial fingerprint identification”, 2011.

[11] Guruprakash.V, Arthur Vasanth. J “Combined Fingerprint Minutiae Template Generation”, 2014.

[12] Manhua Liu, Shuxin Liu, and WeiwuYan “Latent Fingerprint Segmentation Based on Ridge Density and Orientation Consistency” Hindawi Security and Communication Networks Volume 2018, Article ID 4529652, 10 pages https://doi.org/10.1155/2018/4529652.