EXPERIMENTAL STUDY OF FINGERPRINT VERIFICATION USING MINUTIAE POINT MATCHING

Ginne M James

Department of Computer Technology, Sri Krishna Arts and Science College, (India)

ABSTRACT

A biometric is a unique, assessable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being in effective way. Statistically analyzing these biological characteristics has become known as the science of biometrics systems. Nowadays, biometric technologies are typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, palm, iris, face, and speech. In this research work, recognition of fingerprint for human identification using minutia point matching.Experiments were conducted using DB4 fingerprint database comprising four datasets of images of different sources and qualities. The fingerprint images are read and processed for enhancement of ridges also for accurate extraction of minutiae features. The result proven minutiae based fingerprint verification is perform well in the field of security. The Euclidian distance is measured for similarity finding.

Keywords: Biometrics, DB4, DNA, Whorls, Arches, Binarization and etc,.

I. INTRODUCTION

Fingerprint recognition is a more complex pattern recognition problem. Because it is difficult to design accurate algorithms capable of extracting most important features and matching them in a robust way, especially in poor quality fingerprint images and when low-cost acquisition devices with small areas are accepted. Automatic fingerprint recognition is a fully solved problem since it was one of the first applications of machine pattern recognition problem. On the contrary, fingerprint recognition is still a challenging and important pattern recognition problem in the research field.

Personal identity refers to a group of attributes that are linked with an individual such as name, social security number etc [1]. Biometric technology holds out the promise of a trouble-free, safe technique to make remarkablyaccurate authentications of persons. It provides a secured method of recognition that cannot be stolen, misplaced or forgotten, which is being gradually more required in safety atmospheres and applications such as access control and electronic transactions of data [2]. As biometric techniques make it a necessity for the client to be physically present during validation, it serves as a restriction against the possibility of clients emerging with fake refutation claims at a later stage [3]. Biometrics throws open advantage over the conventional safety measures about Non repudiation, Accuracy, Screening and Security process.

Biometric systems find out or verify a person's individuality based on his anatomical and behavioral features such as fingerprint, face, eye, speech and gait and these traits cannot be easily lost or forgotten or shared or forged. A biometric scheme delivers automatic recognition of a person depending on some particular unique feature held by the person [5].

The merit of a biometric technique is assessed by means of its inbuiltcapability in recognition, which is estimated using the bogus refutation and fake acceptance rates [6]. Biometric identification methods make use of a single feature for identification are regularly affected by several practical problems like noisy sensor data, non-universality or lack of uniqueness of the biometric trait, unacceptable error rates, and spoof attacks problems [8]. Since the fact, that accuracy of single biometric system is easily affected by the dependability of the sensor used for identification [9].

To overcome the dependability of sensor problem multimodal biometric systems, are estimated to be more dependable because of presence of several, independent fragments of evidence. These methods are able to encounter the accurate performance provisionstariff by numerous applications. They address the problem of non-universality, since multiple traits safeguard adequate population coverage. Multimodal biometric systems overwhelm many of these limitations by combining the proofs obtained from various bases. Multimodal biometrics has produced better accuracy and population coverage, while decreasing susceptibility to spoofing.

Normally, the fingerprint surface is made up of ridges and valleys that serve as a friction surface when we are fascinating the objects. The fingerprint images can be represented by both global as well as local features. The inclusive features include singular points such as core and delta, the ridge orientation and ridge spacing. Minutiae are local features marked by ridge discontinuities. Commonly, fingerprint recognition [10 has the following advantages over other biometrics: (1) universality - the population that has legible fingerprints exceeds the population that possesses the passports; (2) high distinctiveness - even identical twins who share the same DNA have different fingerprints.

The remaining paper is organized as follows; chapter II gives the detail about fingerprint analysis and chapter III tells about methodologies used for fingerprint verification. Chapter IV displays the experiments carried out for verifying fingerprint and its results finally chapter V describes the conclusion and future enhancement of this research work.

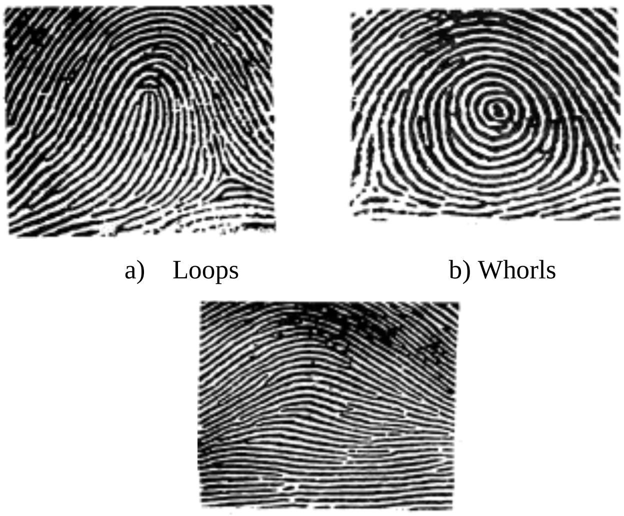
II. FINGER PRINT ANALYSIS

Fingerprints have been systematically studied for a number of years in our society. The characteristics of fingerprints were studied as early in 1600s. In the year of1684, the English plant morphologist, named Nehemiah Grew, published the first scientific research paper which reporting his systematic study on the ridge, furrow, and pore structures. In the year of 1788, author Mayer was given the detailed explanation of the anatomical formations of fingerprints. Purkinji proposed the first fingerprint classification, which classified into nine categories on 1823. Sir Francis Galton introduced the minutiae features for fingerprint matching in late

19th century. Fingerprint identification or fingerprint verification refers to the automated method of authenticating a match between two human fingerprints.

Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints more recently becoming automated (i.e. a biometric) due to development in computing capabilities. Fingerprint recognition is trendy because of the inbuilt ease in acquisition, the various sources available for collection, and their established use and collections by law enforcement and immigration purpose [11].

Fingerprints are unique patterns, made by friction raised and recessed, which appear on the pads of the fingers and thumbs. The palms, toes and feet are also unique patterns; however, these are used less often for identification.The fingerprint pattern, such as the print left when an inked finger is pressed onto paper, is that of the friction ridges on that particular finger. Friction ridge patterns are grouped into three different categories (Fig1) such as loops, whorls, and arches, each with unique variations depending on the shape and relationship of the ridges among it.



a) Loops b) Whorls

c) Arches

Fig1. Fingerprint types

Loops - that recurred back on themselves to form a loop shape. Loops are divided into radial loops and ulnar loops. The loops account for approximately 60 percent of pattern types.

Whorls - form circular or spiral patterns, like tiny whirlpools. There are four groups of whorls: plain, central pocket loop, double loop and accidental loop. Whorls make up about 35 percent of pattern types.

Arches - create a wave-like pattern and include plain arches and tented arches over it. Tented arches rise to a sharper point than plain arches. Arches make up about five percent of all pattern types.

The two fundamentalproperty of fingerprint identification are uniqueness and persistence. There is no two people have ever been found to have the same fingerprints—including identical twins. In addition to that no single person has ever been found to have the same fingerprint on multiple fingers.

Persistence also called as permanence, the principle of person's fingerprints is remains unchanged throughout their lifetime. As new skin cells form, they remain tiled in the existing friction ridge and furrow pattern as same. In reality, the research conducted on many people andverifies this persistency by recording the same fingerprints over decades and observing that the features remain the same [12]. Even attempts to remove or damage one's fingerprints will be frustrated when the new skin grows, unless the damage is extremely deep, in which case, the new bargain caused by the damage will now persist and is also unique in pattern.For example, an analyst comparing a crime scene fingerprint to a fingerprint on file to gather known prints with the same general pattern type, then using a loop, compare the fingerprints side-by-side to identify specific information within the minutiae feature that match. In case of enough details correlated, the fingerprints are determined to be from the same person.According to Forensic Science, there are three types of fingerprints.

Patent prints: are easy to locate since they are visible to the stripped eye. Patent prints occur when someone has a substance on their fingers such as grease, paint, blood, or ink that leaves a visible print on a surface.

Plastic prints: are less common than patent prints since they occur when someone touches an object such as wax, butter, or soap and leaves a three-dimensional impression of the finger on the object.

Latent prints: Is the most common type of print and take the most effort to locate. Since they are invisible to eye. Latent prints occur when someone touches any permeable or nonporous surface. The natural oils and residue on fingers leave a deposit on surfaces which mirror the ridges and furrows that are present on the individual's finger.

III. METHODOLOGY

Methodologies used for fingerprint identification is explained blow;

a) Binarization

Binarization is the process of changing a pixel image to a binary image. In the old days binarization was important for sending faxes to other place butits still important for things like digitalizing text or segmentation.

The input fingerprint image is as a gray-scale image[range 0 – 255]. Binarization is the process oftransforming the Gray-scale image into the binary image[0,1]. The gray-scale transformations do not depend onthe position of the pixel in the image. Because of the pixel representation median value is 0 this value is used as threshold value in binarization process. Finally the simple algorithm of this process is:

- Get the size of the image
- Check for all pixel value representation. If the value is greater than or equal to ’0’, change the value to ’1’, else change to ’0’.

A transformation Tof the original brightness P from scale [P_0, P_k] intobrightness q from a new scale [q_0,q_k] is given byq =T (P1).The straight line denotes the negativetransformation; the dashed line is linear function ‘b’enhances the image contrast between brightness value P1,P2 (Fig2). The function ‘c’ is called brightness threshold andresults in a black-and-white image (Binarized image).

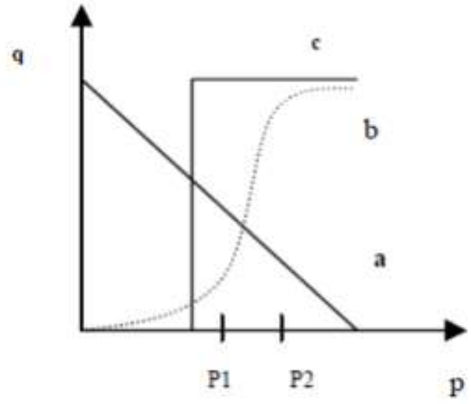


Fig2. Binarized image transformation

b) Thinning

Asuccessful and exact thinning algorithm directly affects the fingerprint feature extraction, matching accuracy and results. The best known thinning algorithms fall into the following two categories: Iterative and Non-iterative. Iterative algorithms delete pixels on the boundary of a pattern repeatedly until only the unit pixel-width thinned image remains. Non-iterative distance transformation algorithms are not suitable for general applications since they are not robust, especially for patterns with highly variable stroke directions and thicknesses. Thinning, based on iterative boundary removal, can be divided into sequential and parallel algorithms. Thinning is mostly done on the binarized image of the fingerprint. The mostly discussed and described thinning algorithms are based on parallel thinning, as they are fast and efficient. Algorithms are described by Zhang-Suen [13], Guo-Hall [14], Abdulla et al [15], R. W. Hall [16]. In this work Zhang-Suen algorithm is used for thinning fingerprint

Zhang-Suen’s Algorithm

The Zhang-Suen’s algorithm works by using a 3×3sized block. It is an iterative algorithm and it removes all the shape points of the image except those that belong to the skeleton of the image [14].

The algorithm is described below:

```
1. While points are deleted, do
2. For all p(i, j) pixels, do
3.          If (a) $2 \leq B(P1) \leq 6$
               (b)   $A(P1)=1$
               (c) One of the following statements is true:
                        1.  $P2 \cdot P4 \cdot P6 = 0$ in odd iteration,
                        2. $P2 \cdot P4 \cdot P8 = 0$ in even iteration,
               (d) One of the following statements is true:
                        1. $P4 \cdot P6 \cdot P8 = 0$in odd iteration,
                        2. $P2 \cdot P6 \cdot P8 = 0$ in even iteration, then
4. Delete the pixel of p(i, j)
```

whereA (P1) is the number of 0 to 1 conversion in the clockwise direction from P9 , B (P1) is the number of non-zero neighbors of : $B(P1)= P2 + P3 +\Lambda+ P9$.P1 is not deleted, if any of the above conditions is not met. The algorithm is fast, but fails to maintain such patterns that have been reduced to 2 × 2 squaresand they are completely removed.

c) Minutiae Extraction

The approach in [17] is similar to the approach taken in the study and reported in this work. The method proved suitable enough for handling matching problems due to image ridge orientation and size variations. The proposed algorithm for the computation of the pattern matching scores for fingerprint images relies on the distances between the image core and the minutiae points. The formulation of the algorithm was motivated by the fact that the relative distance to the core point from each minutia point does not change irrespective of the image directional flow. The core point being the point of maximum turning is the point at which the gradient is zero. The core points A and B shown in Figure 5 are the points of maximum turning of the ridge structures in the two images. They are also the points where the directional fields experience total orientation changes [18].

The processor for minutiae extraction

a. Obtain the core point

b. Obtain the x and y coordinates for all the true bifurcations and ridge endings in the thinned image. The Crossing Number (CN) value for a candidate ridge ending and bifurcation is obtained according to the formula:

For a candidate bifurcation point:

Examine the 3 x 3 neighbourhood of the bifurcation point in a clockwise direction. Forthe three pixels that are connected with the bifurcation point, label them with the value of1.

Label with 1 the three ridge pixels that are connected to these three connected pixels.

Count in a clockwise direction, the number of transitions from 0 to 1 ($T01$) along theborder of image M. If $T01 = 3$, then the candidate minutiae point is validated as a truebifurcation

For a candidate ridge ending point:

- Label with a value of 1 all the pixels in *M*, which are in the 3 x 3 neighborhood of theridge ending point.
- Count in a clockwise direction, the number of 0 to 1 transitions (*T*01) along the border ofimage *M*. If *T*01 = 1, then the candidate minutiae point is validated as a true ridge ending.

c. The distance, λi between the ith minutiae point Pi(ai,bi) and the image core point M(ρ, σ) isobtained from:

$$\lambda_i = ((a_i - \rho)^2 + (b_i - \sigma)^2)^{0.5}$$

d. The degree of closeness12is obtained for matching image K with image L by using the formula:

$$E_c = \sum_{i=1}^{s} (|G(i) - H(i)|) * \{G(i)\}^{-1}$$

Where s is the smaller of the respective number of feature points in the two images, G(i) and H(i)represent the distance between the ith minutiae point and the core point in K and L respectively.

e.The correlation coefficient value, S between K and L, is then computed as the pattern matching score by using the formula:

$$S = (1 - E_c) * 10^{-2}$$

From this formula, the closeness value will be 12 = 0 for exact or same images and, consequently, the correlation will be S = 1.

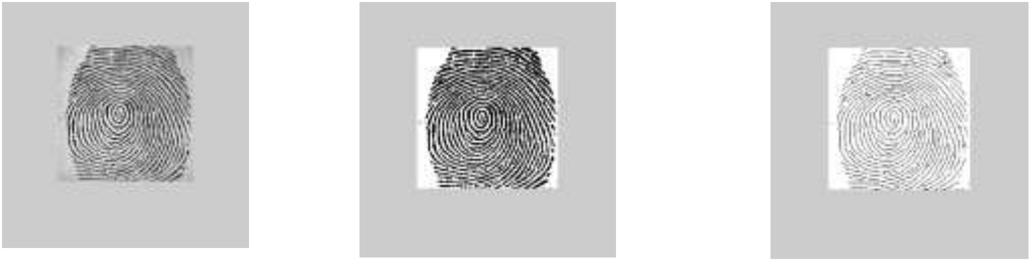
IV. EXPERIMENT AND RESULT

a. Data collection

Database used for experiment is DB4 FVC2004. Several fingerprint images in this database are low quality. Size of each fingerprint images is 288x384 pixels, and its resolution is 500 dpi.

b. Read image and processing

The input image is read using imread comment in matlab platform. After the read operation, ridges in the fingerprint are highlighted with black color while furrow are white by using binarization process. Next step is thinning the given image. Ridge thining is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. The following figure(Fig3) shows the operation of above mentioned.

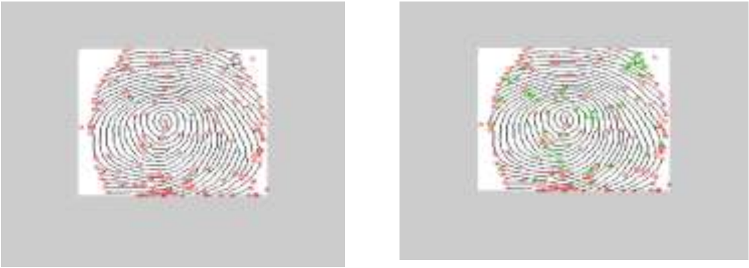


a) original image b) After binarization c) After thinning

Fig3. Original and processed image

c. Minutiae extraction

Most algorithms are using minutiae, the specific points like ridges ending, bifurcation. Only the position and direction of these features are stored in the signature for further comparison. Next process is to filter the thinned ridge map by the filter "minutie". Minutie compute the number of one-value of each 3x3 window: 1) if the central is 1 and has only 1 one-value neighbor, then the central pixel is a termination. 2) if the central is 1 and has 3 one-value neighbor, then the central pixel is a bifurcation. 3) if the central is 1 and has 2 one-value neighbor, then the central pixel is a usual pixel. The blow figure (Fig4) demonstrates the termination and bifurcation ponts.

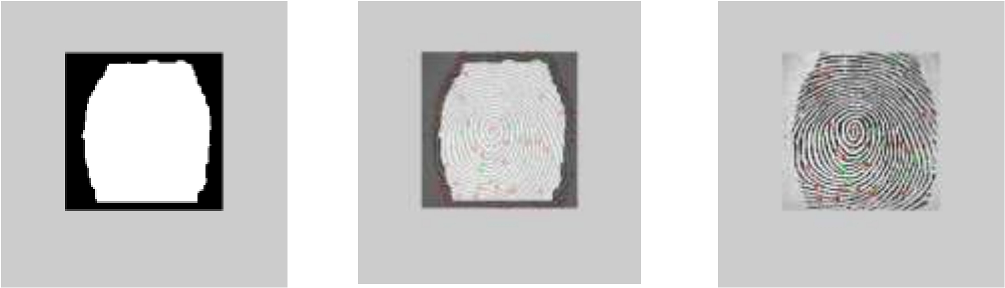


a) Termination extraction b) Bifurcation extraction

Fig4. Minutiae extraction

d. ROI extraction and Suppress extrema minutiae

Another step is to determine a ROI. For that, we consider the binary image, and apply a closing on this image and erosion operation for define suppress minutiae external to this ROI. The figures (Fig5) give the ROI and suppressextrema.

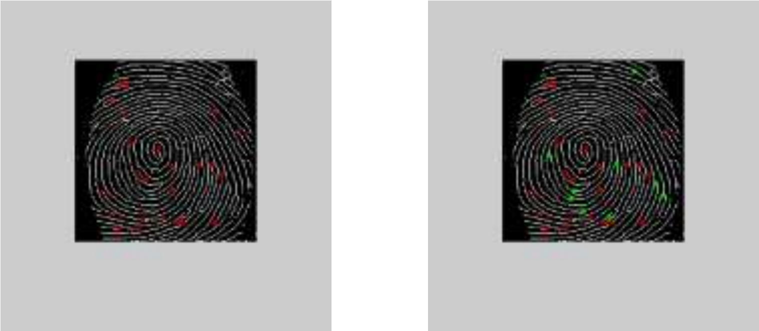


a) Background subtraction b) ROI extraction c) Suppress extrema minutiae

Fig5. ROI and suppress extrema extraction

e. Orientation

To determine the different minutiae points we have to find the orientation of each one. First process is to find the orientation of the termination. For finding that, analyze the position of the pixel on the boundary of a 5 x 5 bounding box of the termination. And compare this position to the Table variable. The Table variable gives the angle in radian. For each bifurcation it has three lines. So operate the same process than in termination case three times. The following figure (Fig6) illustrates the orientation points.



a) Termination Orientation　　b) Bifurcation Orientation

Fig6. Orientation points

f. Validation/ minutiae matching with Euclidian distance

This step validates the minutiae points and calculates the Euclidian distance for matching. Given two set of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not. If the fingerprint is matched based on the minutiae points and distance is 0. If not match then it will show the nearest match and the distance value is >0. The following figures (Fig7 and Fig8) demonstrate the match and non-match fingerprint.

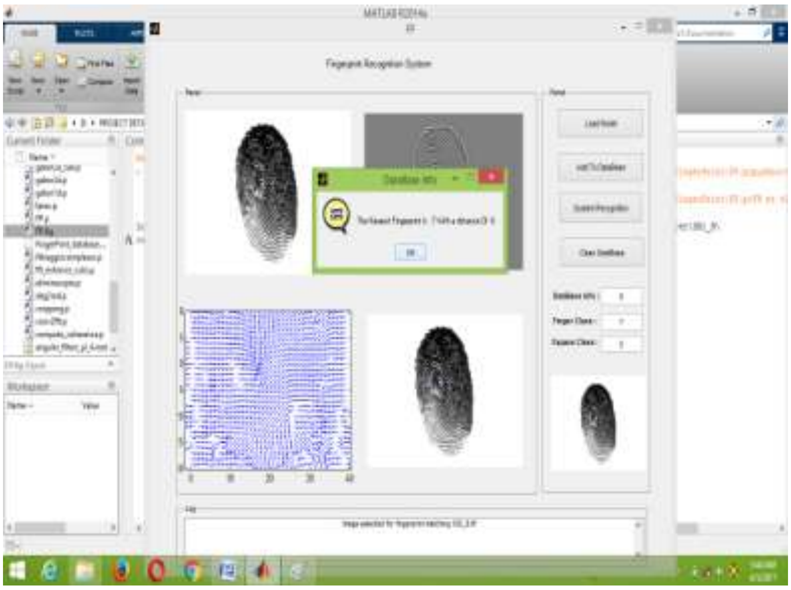


Fig7. Matched fingerprint

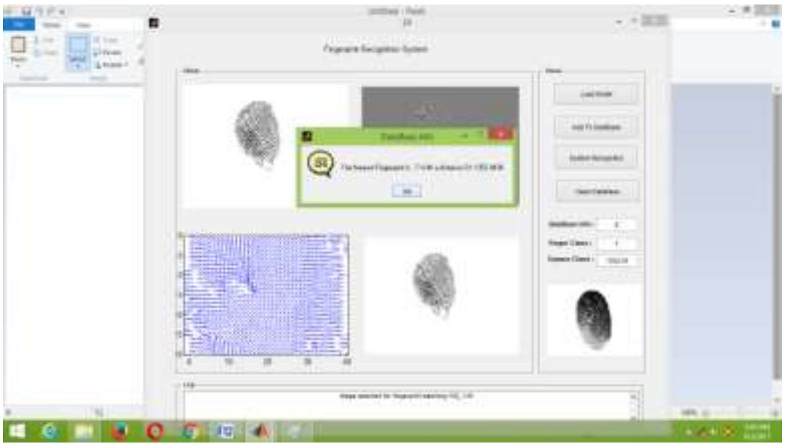


Fig8. Non-match fingerprint

V. CONCLUSION

Performance evaluation is important for all pattern recognition applications and particularly so for biometrics, which is receiving widespread international attention for citizen identity verification and identification in large-scale applications. The algorithm used the relative distances between the minutiae and the core points. This algorithm hinged on the premise that irrespective of image orientation, the minutiae points maintain constant distances with the core point for a given image size. And the validation and matching is done based on the minutiae points and Euclidian distance value. Future research direction aims at the optimization of the proposed algorithm for further reduction in the false match rate values and the computation times.

REFERENCE

[1] D. V. Hiep, T. Q. Duc, and N. T. H. Lan, “A Multibiometric Encryption Key Algorithm Using Fuzzy Vault to Protect Private Key in BioPKI Based Security System”, Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), pp. 1-6, Nov. 2010.

[2] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins", In Proceedings of the Symposium on Usable Privacy and Security ACM Press, pp. 77–88, 2005.

[3] K. D. Mitnick, W. L. Simon, and S.Wozniak, “The Art of Deception: Controlling the Human Element of Security”, John Wiley & Sons, 2002.

[4] D. V. Klien, “A Survey of, and Improvements to Unix Password Security”, In Proceedings of the Second USENIX Workshop on Security, pp. 5-14, 1990.

[5] S. Kadry and K. Smaili, "A Design and Implementation of a Wireless IRIS Recognition Attendance Management System", Information Technology and Control, Vol. 36, No. 3, pp. 323-329, 2007.

[6] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, “Integrating Faces, Finger- prints and Soft Biometric Traits for User Recognition”, In Proceedings of ECCV International Workshop on Biometric Authentication (BioAW), The Art of Deception: Controlling the Human Element of Security Vol. 3087, pp.259-269, 2004.

[7] S. K. Mohanty and P. K. Pattnaik, "Authentication Based on Texture Analysis and SVM Classification", International Journal of Instrumentation, Control and Automation (IJICA), Vol. 1, No. 1, pp. 61-66, 2011.

[8] Z. Yaghoubi, K. Faez, M. Eliasi and A. Eliasi, "Multimodal biometric recognition inspired by visual cortex and Support vector machine classifier", International Conference onMultimedia Computing and Information Technology (MCIT), pp. 93-96, 2010.

[9] C. H. Chen and C. Chu, "Fusion of Face and Iris Feature for Multimodal Biometrics", Lecture Notes in Computer Science, Vol. 3832, pp. 571-580, 2005.

[10] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview", in Proc. of 12th European Signal Processing Conference (EUSIPCO), pp. 1221-1224, September 2004.

[11] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, pp. 250-255, March 2005.

[12] S. Gupta, V. Doshi, A. Jain and S. Iyer, "Iris Recognition System using Biometric Template Matching Technology", International Journal ofComputer Applications, Vol. 1, No. 2, pp. 21-30, 2010.

[13] T. Zhang and C. Suen, "A fast parallel algorithm for thinning digital patterns," Communicationsof the ACM, vol. 27, pp. 236–239, 1984.

[14] Z. Guo and R. Hall, "Parallel thinning with two-subiterationalgorithms,"Communications of the ACM, vol. 32, pp. 359–373, 1989.

[15] W. Abdulla, A. Saleh, and A. Morad, "A preprocessing algorithm for hand-written characterrecognition," Pattern Recognition Letters 7, pp. 13–18, 1988.

[16] R. Hall, "Fast parallel thinning algorithms: Parallel speed and connectivity preservation,"Communications of the ACM, vol. 32, pp. 124–129, 1989.

[17] Giuseppe P.E and Albert N. (2003): Fingerprint Matching Using Minutiae Triangulation. Available online at http://idisk.mac.com/geppy.parziale/Public/Papers/delaunay.pdf. Accessed 23/01/2012

[18] Perez-Diaz A. J. and Arronte-Lopez I. C. (2010): Fingerprint Matching and Non-Matching Analysis for Different Tolerance Rotation Degrees in Commercial Matching Algorithms, Journal of Applied Research and Technology, Vol. 8 No. 2, page 186-199