JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

MINUTIA BASED FINGERPRINT AUTHENTICATION

Sachin Harne [1], Mr K. J. Satao [2], Imroze Khan [3]

[1] Department of Computer Science and Engineering, RCET, Bhilai, INDIA

[2] Department of Computer Science and Engineering, RCET, Bhilai, INDIA

[3] Department of Electrical & Instrumentation Engineering, NIT, Raipur, INDIA
sachin.harne2027@gmail.com, kjsatao@rediffmail.com, imroze786@gmail.com

Abstract

Biometric authentication is an excellent way to security now days. Now it has been proven that each and every individual has its own biometric feature such as *Fingerprint, Iris, Footsteps, Face and Voice* which is different from other. These can be used to identify individual. Using biometric not only guarantees identification but it guarantees fast identification. Now day's technologies are exploring the features of biometric authentication for rapid and fast identification of individuals. Top it companies such as Nokia, Samsung, Motorola are using these features in mobile technology to securely authenticate right person. Again companies such as IBM, HP and HCL are using these technologies to provide fast and secure login to the devices.

In this paper I have explored one of the biometric authentication schemes which are most popular, "MINUTIA BASED FINGER PRINT AUTHENTICATION". Thumb impression of each person has different minutiae structures. These minutiae can be extracted from the fingerprint image and processed to get digital data based on minutiae and their orientation. These data are stored in database to obtain a list of known persons. These data can be used to identify person by using different fingerprint matching schemes. In this paper I have used Euclidian distance technique to match to fingerprint data.

Keywords: Biometric, Minutiae, Euclidian distance.

1. Introduction

With the advent of technology in almost all spheres of life in the 21st century, there is an increasing need for us to be able to authenticate the person who is using the services. As more and more of these services are automated without any human agent in between, we need to ensure that the person who is using the service is the

ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

right person. Thus, the bonus of now verifying the authenticity of the person again falls on machines. We need technology to verify the user before he can access any service or protected information. This is where the science of Biometrics comes in.

2. Previous Work

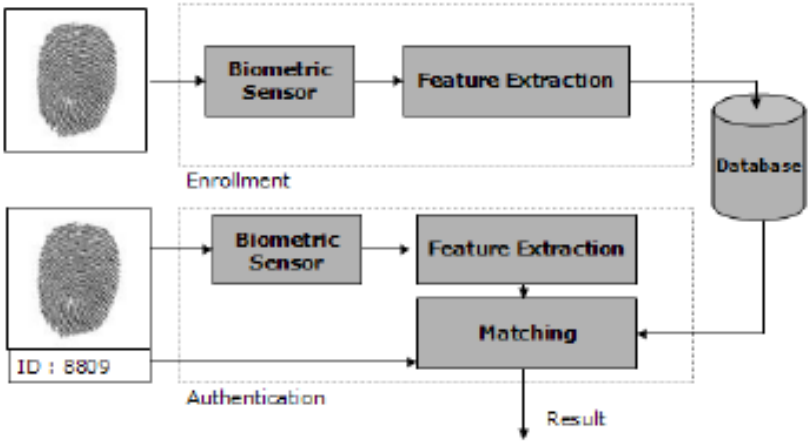
Many automatic fingerprint matching approaches have been proposed. Among the various Fingerprint representation methods, the minutiae-based fingerprint representation and matching are widely used by both machine and human experts. Minutiae representation has several advantages compared to other fingerprint representations in terms of the template size and its discriminability. In our work, we will focus on minutiae-based systems. Minutiae-based fingerprint matching involves search for the correspondence between two lists of points in high-dimensional (usually in three-dimensional or higher) space. Minutiae matching is usually addressed as a point pattern matching problem and many approaches can be applied. However, the relaxation methods, algebraic and operational research solutions, tree-pruning approaches, and energy-minimization methods impose unrealistic requirements, such as equal number of feature points and every point has to have a match. They are also inefficient. Hough transform-based methods convert the matching problem to the problem of locating peaks in the discrete Hough space and the underlying transform parameters of participating fingerprint is recovered. Methods that depend on the pre-alignment increases the matching efficiency and accuracy. Other approaches that avoid alignment and match local features have been also proposed. However, there has been no research that explicitly address the issues of partial fingerprint matching. The study on the security strength of a fingerprint recognition system compared to a password system has been conducted recently. They make assumptions that the two participating fingerprints have the same number of feature points and have a fixed image size. The security strength of a fingerprint system diminishes when the size of fingerprint decreases. However, the relation between fingerprint size and the system security strength and how to maintain the security level of a partial fingerprint recognition has not been addressed.

3. Present Work

The fingerprint matching system proposed here is a simple technique based on minutiae matching, and it works as good as other techniques which rely totally on minutiae features for fingerprint matching. Our algorithm basically consists of the following stages:

ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

1. Fingerprint image preprocessing and minutiae extraction: We use standard image processing techniques to extract minutiae features from the fingerprint.
2. Image alignment using Euclidean Distance as the similarity measure
3. Saving processed image in database.
4. Matching % generation with other fingerprints in database.



4. Minutiae-Based Fingerprint Recognition

Our research uses the minutiae-based fingerprint representation to design the systems due
to the advantages of wide accessibility and stability. Minutiae-based fingerprint representation and matching are widely used by both machine and human experts. Minutiae representation has several advantages compared to other fingerprint representations. Minutiae have been (historically) used as key features in fingerprint recognition tasks. Its configuration is highly distinctive and several theoretical models use it to provide an approximation of the individuality of fingerprints. Minutiae-based systems are more accurate than correlation based systems and the template size of minutiae-based fingerprint representation is small. Forensic experts use this representation which has now become part of several standards for exchange of information between different systems across the world.

4.1 Fingerprint Image Enhancement

Fingerprint image quality is an important factor in the performance of minutiae extraction and matching algorithms. A *good* quality fingerprint image (Figure 2.5(a)) has high contrast between ridges and valleys. A *poor* quality fingerprint image (Figure 2.5(b) and (c)) is low in contrast, noisy, broken, or smudgy, causing spurious and missing minutiae. Poor quality can be due to cuts, creases, or bruises

ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

on the surface of finger tip, excessively wet or dry skin condition, uncooperative attitude of subjects, damaged and unclean scanner devices, low quality fingers (elderly people, manual worker), and other factors. The goal of an enhancement algorithm is to improve the clarity (contrast) of the ridge structures in a fingerprint. General-purpose image enhancement techniques are not very useful due to the non-stationary nature of a fingerprint image. However, techniques such as

(a) (b) (c)

(a) A good quality fingerprint image; (b) a poor quality fingerprint caused by extremely dry skin; (c) a noisy fingerprint image.

gray-level smoothing, contrast stretching, histogram equalization, and Wiener filtering can be used as preprocessing steps before a sophisticated fingerprint enhancement algorithm is applied. Techniques that use single filter convolutions on the entire image are not suitable. Usually, a fingerprint image is divided into sub regions and then a filter whose parameters are pre-tuned according to the region's characteristics is applied. Each local region of a fingerprint can be seen as a surface wave of a particular wave (ridge) orientation (perpendicular to flow direction) and frequency. Several types of contextual filters in both spatial and frequency domains have been proposed in the literature. The purpose of the filters is to fill small gaps (low-pass effect) in the direction of a ridge and to increase the discrimination (band-pass effect) between ridges and valleys in the direction orthogonal to the ridge . O'Gorman and Nikerson were the first to propose the use of contextual filtering. By assuming that the ridge frequency remains constant across an entire fingerprint image, 16 bell-shaped filters are pre-computed. The filter whose direction best fits the sub region's orientation is selected and then convolved on every point of the sub region. proposed a fingerprint enhancement based on Gabor filters. Gabor filters have both frequency-selective and orientation-selective properties which capture the periodic and non-stationary nature of a fingerprint image. For a given frequency f and orientation θ, the symmetric two-dimensional Gabor filter has the following form :

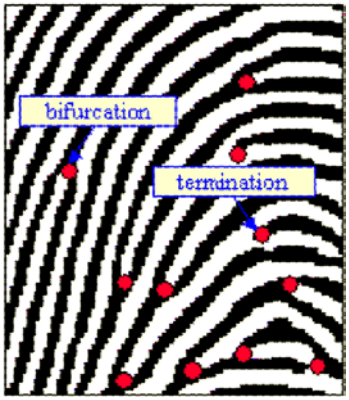
$G(x,y) = \exp\{-⅓\}$

ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

where, $x_\theta = (x \sin(\theta) + y \cos(\theta))$, $y_\theta = (-x \cos(\theta) + y \sin(\theta))$, and σx and σy are the standard deviations of the Gaussian envelope along the x- and y-axes, respectively. The values of f and θ can be estimated from the target sub regions. However, the selection of σx and σy is not straight forward. Smaller values of σx and σy reduce spurious ridges and valleys and remove noise. On the other hand, larger σx and σy values make the filters robust to noise and are likely to create spurious ridges and valleys.

4.3 Minutiae Extraction

Many methods have been proposed to extract minutiae features from fingerprint images. We can do processing in gray scale or we can binarize the image and then process



Two main types of minutiae: Bifurcation and Ridge Ending.

This tool given a fingerprint image in .tiff, .jpg, .bmp format will extract all the minutiae points in the fingerprint, and write its x-coordinate, y-coordinate and the corresponding ridge orientation in a .fp file. The tool also provides a Graphical user interface where we can visualize the minutiae extracted along with the ridge angle, overlayed on the actual fingerprint image. Though, one issue with this tool is that the authors haven't released the source code for it, hence we have to manually open each fingerprint image using the tool, and save the .fp file. Though this is a tiresome process, once .fp files of all the fingerprints in the database are obtained we can use them easily. The reliability of minutia features plays a key role in automatic fingerprint recognition. Generally, the minutiae representation of a fingerprint consists of simply a list of minutia points associated with their spatial coordinates and orientation. Some methods also include the types and quality of minutiae in the representation. Minutiae extraction algorithms are of two types:

(i) binarization-based extraction and
(ii) gray-scale based extraction.

JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

In this project we have used binarization-based extraction. Most of the proposed minutiae extraction methods are binarization-based approaches. They require conversion of the gray-scale fingerprint image (8 bits per pixel, 256 gray levels) into a binary form (2 bits per pixel, black and white). Various binarization techniques have been presented in the image processing literature [96, 88]. One intuitive approach is to use a global threshold t and assign each pixel a value according to the following equation:

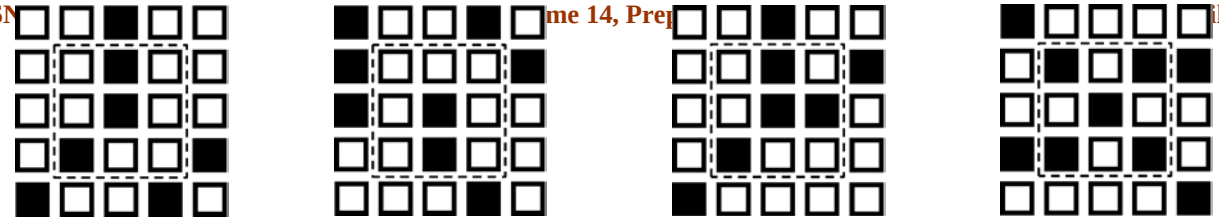
$$I_b(x,y) = \begin{cases} 1 & \text{if } I(x,y) > t \\ 0 & \text{if } I(x,y) \leq t \end{cases}$$

where I(x, y) is the intensity value of the pixel at (x, y) in a gray-scale image. Otsu's method describes a technique to obtain the global threshold t from a statistical viewpoint. The contrast variation in a fingerprint image makes it impossible to find an optimal global threshold. Adaptive techniques are preferred in general but they fail on poor quality images.

Several methods have been proposed to utilize the flow texture of a fingerprint image in binarization tasks. Stock and Swonger observed that the average local intensity of a ridge line along its flow direction is highest and used it in binarization. Ratha, Chen and Jain use a 16×16 window centered and oriented along the local ridge direction on each pixel. Ridge lines are recognized as peaks of the gray-level profile of pixel intensities projected on the central segment of the window. Usually, the binarization-based minutiae extraction methods apply a thinning algorithm after the binarization step to obtain the *skeletons* of fingerprint ridges. Once a binary skeleton of a fingerprint is obtained, minutiae extraction becomes a trivial task. Let us assume that the foreground and background pixel values of a fingerprint skeleton are 1 and 0, respectively.

Minutia can be detected by examining the 8-neighborhood of a ridge skeleton pixel at (x, y) and classified as:

- a ridge ending if $\Sigma i,j=-1 \cdots 1\ I(x + i, y + j) = 2$;
- an intermediate ridge point if $\Sigma i,j=-1 \cdots 1\ I(x + i, y + j) = 3$;
- a ridge bifurcation if $\Sigma i,j =-1 \cdots 1\ I(x + i, y + j) = 4$;
- or a crossover minutia.



(a) an intra-ridge pixel; (b) a ridge ending; (c) a bifurcation; (d) a crossover

4.3 Ridge Count

For using fingerprints as a biometric feature, we extract different type of features from fingerprint like what is the type of fingerprint (arch, loop, whorl etc) or what are the discontinuities in ridge of fingerprint. These discontinuities in ridges of fingerprints are called minutiae. The major Minutiae features of fingerprint ridges are: ridge ending and bifurcation. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges.

Fingerprint with minutiae detected along with ridge angle at that point.

4.4 Minutiae Based Matching

Matching is the most important part of an automatic fingerprint recognition system. It compares two (feature) templates (I and R) that are extracted from the query and reference fingerprints and returns a binary decision (matched/non-matched) or a similarity score ($S(I,R)$) to indicate how similar the two participating fingerprints are.

Minutiae-based fingerprint matching involves search for the correspondence between two lists of points in high-dimensional (usually in three-dimensional or higher) space. A triplet is the most common representation of a minutia, where (x, y) is the location and is the orientation of the minutia. Therefore, the templates are represented as:

$I = \{m1, m2, \cdots, ma\}$, ,i = 1 · · · a

$R = \{m1, m2, \cdots, m'b\}$, , j = 1 · · · b,

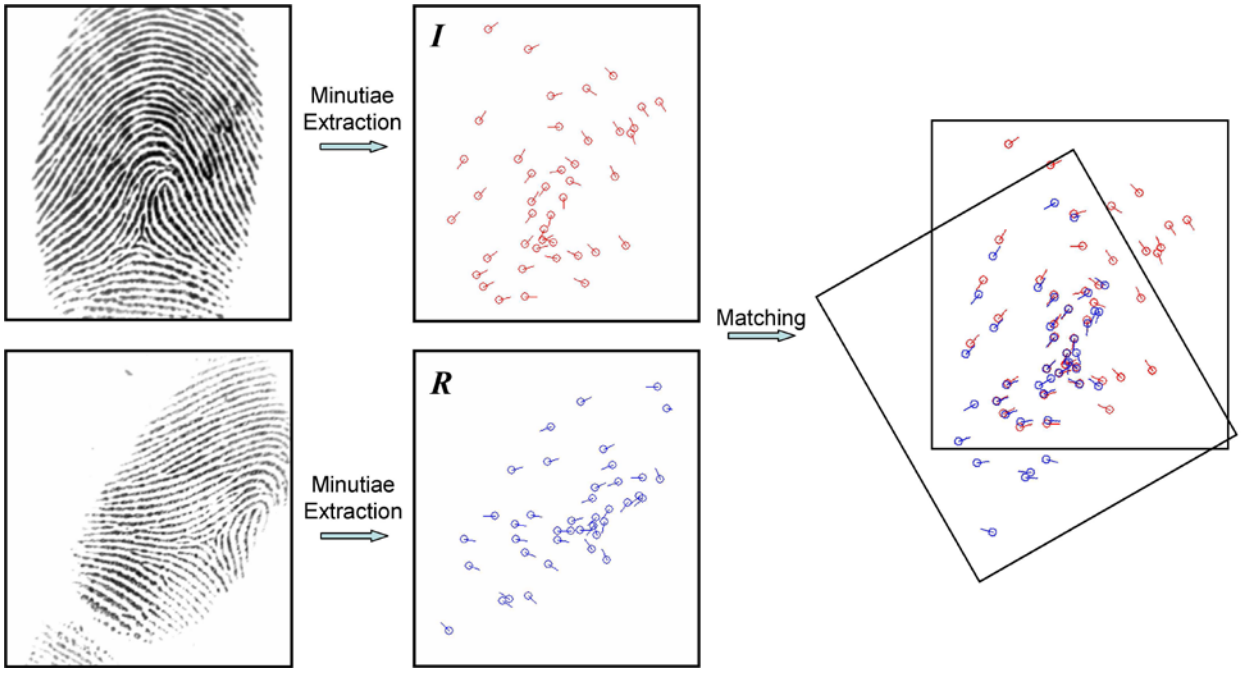
JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

where a and b are the number of minutiae in ***I*** and ***R***, respectively. A minutia m′ j in ***R*** matches the minutia mi in ***I***, if they are *sufficiently close* in terms of spatial distance and orientation difference. Given two tolerance distances r0 and 0, minutia mi matches minutia m′j

if and only if:

$\text{sqrt}(xi - x'j)^2 + (yi - y_j')^2 \leq r0$
and
$\min(|\theta i - \theta' j|, 360 - |\theta i - \theta' j|) < 0.$

Usually, minutia mi in ***I*** relates to the minutia m′j in ***R*** through some geometric transformation



The transformation parameters of T(·) are not known in advance. One must recover the transformation function T(·) that maps the point set from ***I*** to ***IT***. The underlying assumptions
of the geometric transformation (such as rigid transformation, affine transformation, complex non-linear transformation, etc.) are important to the design of a matching algorithm.

5. Result Analysis

5.1 Histogram Equalization

JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

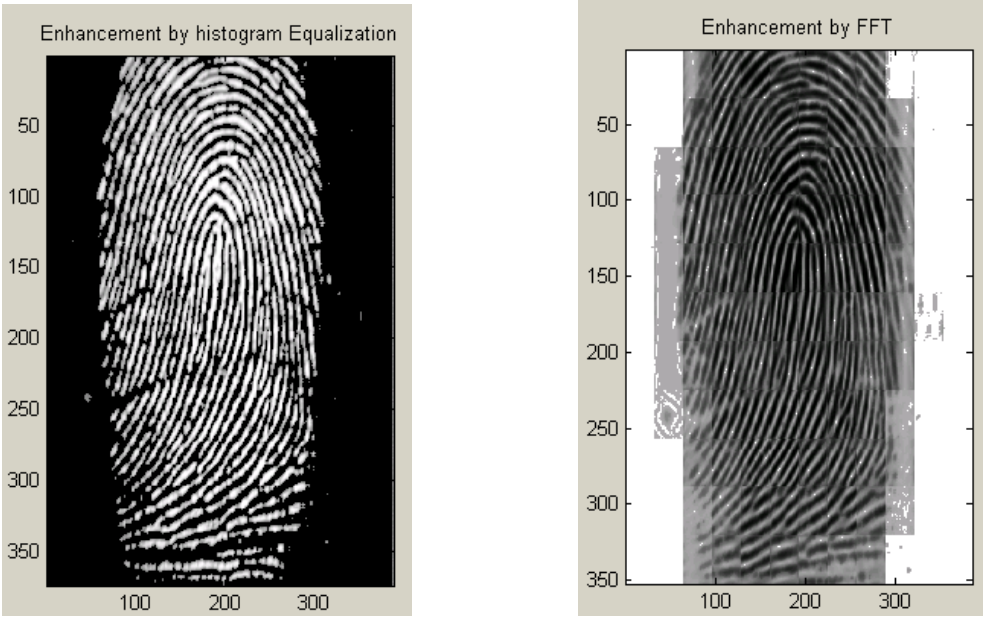
Histogram equalization assigns the intensity values of pixels in the input image such that the output image contains a uniform distribution of intensities. In other words the image is histogram equalized to correct brightness, contrast and equalize the different intensities level of the image. In histogram equalization the new intensity values are calculated by using the formula

$$O_i\, i = \left[\sum_{j=0}^{i} N_j\right] \times \frac{I_m}{N} \qquad (1)$$

O_i = New intensity value of i^{th} pixel

I_m = Maximum intensity level

N = Number of pixels



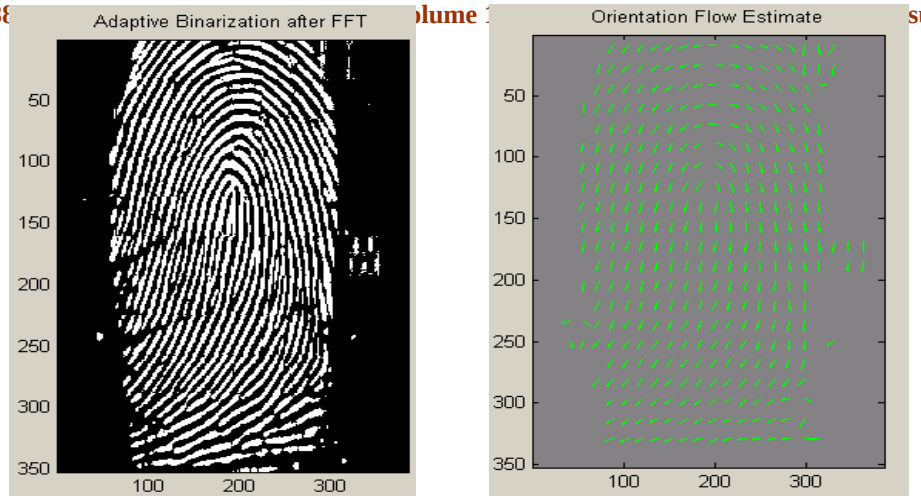
(a) (b)

3.1 (a)Histogram Equalized of a typical face image (b) Enhancement by fft

5.2 Binarization of image

Each pixel has a corresponding multi-bit gray-level value, and convert it into a binary image, in which each pixel has a binary value, either black (foreground) or white (background). Binarization is used particularly in simplifying document mages

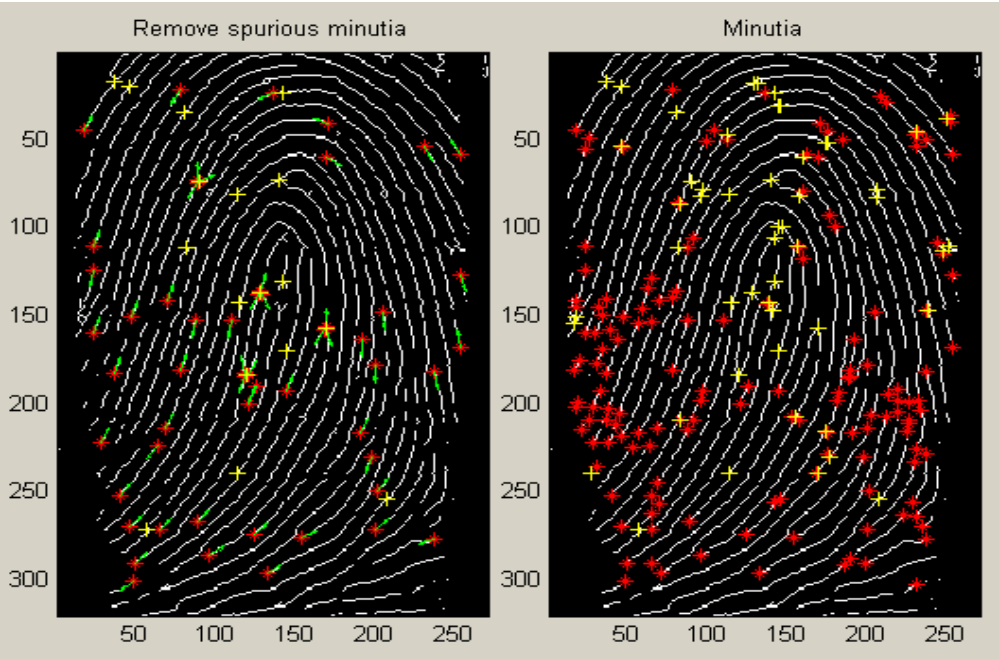
JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-88 lume 1 submitted 18 April 2011



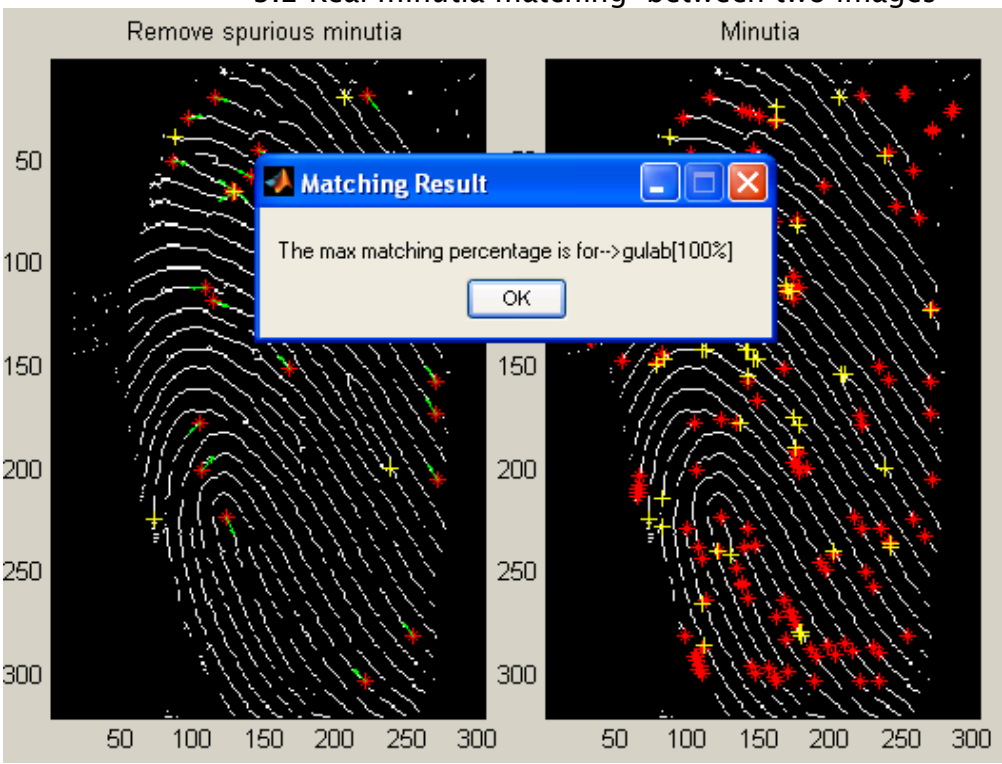
(C)

3.2(C) Adaptive Binarization after fft (D)Orientation flow estimate

JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-88 d 18 April 2011



3.2 Real minutia matching between two images



3.3 Max matching percentage

JCSE The Journal of Corrosion Science and Engineering
ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

6. Conclusion

The goal of this thesis is to study the security impact of partial fingerprints on automatic fingerprint recognition systems and to develop an automatic system that can overcome the challenges presented by partial fingerprint matching. The contributions of our research are as follows:

- The security strength of a partial fingerprint matching algorithm was measured in terms of *bit-strength* and compared with password-based authentication systems. It had been shown that the *bit-strength* of a system that matches a partial fingerprint against a full fingerprint decreases along with the reduction in size of partial fingerprints. To maintain the security level of a partial fingerprint recognition system, features that contain more information must be considered.
- We use localized secondary features for partial fingerprint matching. The limited foreground area offered by a partial fingerprint has a high chance of missing global singular points, such as core and delta points, which are essential for any pre-alignment based matching algorithm. Secondary features rely only on relative information between minutiae and handle fingerprint distortion more effectively.

ISSN 1466-8858 Volume 14, Preprint 15 submitted 18 April 2011

References

[1] A.S. Abutaleb and M. Kamel. A genetic algorithm for the estimation of ridges in fingerprints. *IEEE Transactions on Image Processing*, 8(8):1134–1138, 1999.

[2] Canada Border Services Agency. CANPASS: streamlines customs clearance for frequent travellers. http://www.cbsa-asfc.gc.ca/travel/canpass/menu-e.html, 2004.

[3] Anil Jain , Lin Hong , Ruud Bolle,On-Line Fingerprint Veri_cation, IEEE Transactions on Pattern Analysis and Machine Intelligence, v.19 n.4, p.302–314, April 1997.

[4] Lin Hong, Yifei Wan, Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777–789

[5] J. Yang, L. Liu, T. Jiang, and Y. Fan. A modified Gabor filter design method for fingerprint image enhancement. *Pattern Recognition Letter*, 24:1805–1817, August 2003.

[6] Seung-Hoon Chae, Jong Ku Kim, Sung Jin Lim, Sung Bum Pan, Daesung Moon and Yongwha Chung, “Ridge-based Fingerprint Verification for Enhanced Security, "*International conference on consumer electronics*, pp. 1–2, 2009.

[7] Jaspreeth Kour and Neeta Awasthy, “Non Minutiae based Fingerprint Matching,” *International Association of Computer Science and Information Technology –IEEE Spring Conference*, pp. 199 – 203, 2009

[8] Chengming Wen, Tiande Guo and Shuguang Wang, “Fingerprint Feature-point Matching Based on Motion Coherence,” *Second International Conference on Future Information technology and Management Engineering*, pp. 226–229, 2009.

[9] B. Bhanu, X. Tan, A triplet-based approach for indexing of fingerprint database for identification, in: Proceedings of the Third International Conference on Audio and Video-based Biometric Person Authentication (AVBPA), Halmstad, Sweden, 2001, pp. 205–210.