A Review on Secured Authentication Using Fingerprint Image Fusion

[1]Priyashree Firke, [2]Mr. Nilesh Gupta

[1]M.Tech Scholar, [2]Assistant Professor,
CSE Department
Chouksey Engineering College, Bilaspur, Chhattisgarh, India

***Abstract*: Human fingerprints are rich in details which is known as minutiae, which can be used as identification marks for fingerprint verification. The goal of this project is to develop a complete system for fingerprint verification through extracting and matching minutiae. To achieve good minutiae extraction in fingerprints with varying quality, pre-processing in form of image enhancement and binarization is first applied on fingerprints before they are evaluated. The approach of this project involves how the minutia points are extracted from the fingerprint images and after that between two fingerprints we are performing the fingerprint matching. Image enhancement, image segmentation, minutia extraction and minutia matching these stages are the main themes of our project. This project is coded in MATLAB.**

***Keywords*: Minuate Extraction, Fingerprint Verfication, Image Processing, matlab**

I INTRODUCTION

Basically Skin of human fingertips consists of ridges and valleys and they mixing together form the distinctive patterns. At the time of pregnancy these distinctive patterns are fully developed and are permanent throughout the whole lifespan.
Those patterns are called fingerprints. From different researches it has been observed that no two persons have the same fingerprints, so they are unique for each individual .because of the above mentioned characteristic, fingerprints are very popular for biometrics applications. Finger print matching is a very complex pattern recognition problem so Manual finger print matching is not only time taking but experts also takes long time for education and training.

Fingerprints have remarkable permanency and uniqueness throughout the time. From observations we conclude that the fingerprints offer more secure and reliable personal identification than passwords, id-cards or key can provide. Examples such as computers and mobile phones equipped with fingerprint sensing devices for fingerprint based password protection are being implemented to replace ordinary password protection methods.

Fingerprint

A finger prints are the most important part of human finger. It is experienced from the research that all have their different finger prints and these finger prints are permanent for whole life. So fingerprints have been used for the forensic application and identification for a long time.

Figure 1.1 Finger print image acquired by a Sensor

A fingerprint is the composition of many ridges and furrows. Finger prints can"t distinguished by their ridges and furrows. It can be distinguished by Minutia, which are some abnormal points on the ridges. Minutia is divided in to two parts such as: termination and bifurcation. Termination is also called ending and bifurcation is also called branch. Again minutia consists of ridges and furrows. valley is also referred as furrow

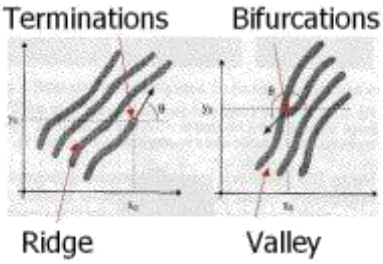

Figure 1.2 (DIAGRAM OF MINUTIA)

Finger Print Recognition

The fingerprint recognition problem can be grouped into two sub-domains such as:-

i) Fingerprint verification ii) fingerprint identification (Figure1.3).

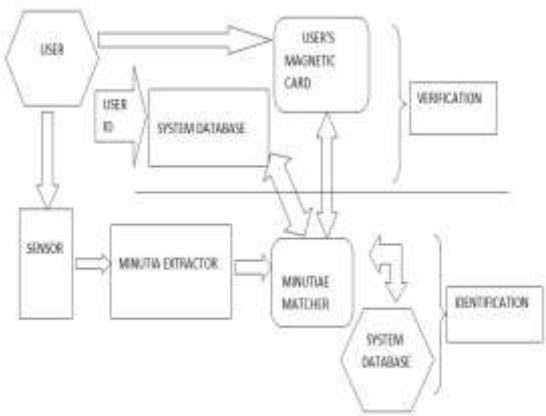

Figure 1.3 Fingerprint Verification and Identification

Fingerprint verification is the method where we compare a claimant fingerprint with an enrolee fingerprint, where our aim is to match both the fingerprints. This method is mainly used to verify a person's authenticity. For verification a person needs to his or her fingerprint in to the fingerprint verification system. Then it is representation is saved in some compress format with the person's identity and his or her name. Then it is applied to the fingerprint verification system so that the person's identity can be easily verified. Fingerprint verification is also called, one-to-one matching. Fingerprint identification is mainly used to specify any person's identity by his fingerprint. Identification has been used for criminal fingerprint matching. Here the system matches the fingerprint of unknown ownership against the other fingerprints present in the database to associate a crime with identity. This process is also called, one-to many matching. Identification is traditionally used for solve crime and catch thieves.

II LITERARURE SURVEY

Chu-Chiao Liao et.al (1) In this paper we present a new fingerprint matching method which combines different features, including minutiae and ridge features. The ridge features contain ridge count, ridge length, ridge curvature direction and ridge frequency. The proposed method achieves better performance than other methods. The average EER value of the proposed method is 0.82 whereas the average EER value of the conventional matching method is 8.12.

Anil K. Jain et.al(2) In 1899, Galton first captured ink-on-paper fingerprints of a single child from birth until the age of 4.5 years, manually compared the prints, and concluded that "the print of a child at the age of 2.5 years would serve to identify him ever after". Since then, ink-on-paper fingerprinting and manual comparison methods have been superseded by digital capture and automatic fingerprint comparison techniques, but only a few feasibility studies on child fingerprint recognition have been conducted.. Given rapidly growing requirements to recognize children for vaccination tracking, delivery of supplementary food, and national identification documents, our study demonstrates that fingerprint recognition of young children (6 months and older) is a viable solution based on available capture and recognition technology.

N.AQILI et.al (3) Matching is a key operation in the current fingerprint system. The objective of fingerprint matching is to achieve a high reliability in comparing two fingerprint details. The large variability in different impressions of the same finger makes reliable

matching fingerprint an extremely difficult problem. In this paper, a minutiae-based algorithm for fingerprint pattern recognition and matching is proposed, based on discrete to continuous approach, which is essentially a point pattern matching approach.

Mouad .M.H.Ali et.al (4) this article is an overview of a current research based on fingerprint recognition system. In this paper we highlighted on the previous studies of fingerprint recognition system. This paper is a brief review in the conceptual and structure of fingerprint recognition.
Muzhir Shaban Al-Ani- MIEEE et.al (5) many techniques are implemented to perform fingerprint recognition approach, and each technique based on specific criteria. The aim of this work is to find an efficient fingerprint recognition technique. This paper tries to offer a simple high performance approach to perform fingerprint recognition. This approach based on two main stages; the first one is the real data collection of human fingerprint samples and the second stage is concentrated on design and implementation of high performance fingerprint recognition approach.

Vladimir I. Ivanov (6) Swipe fingerprint scanners (sensors) can be distinguished based on their scanner pattern—a sufficiently unique, persistent, and unalterable intrinsic characteristic even to scanners of the same technology, manufacturer, and model. We propose a method to extract the scanner pattern from a single image acquired by a widely-used capacitive swipe fingerprint scanner and compare it with a similarly extracted pattern from another image acquired by the same or by another scanner.
Maciej Szymkowski (7) Fingerprints are one of the most popular biometrics traits. Feature extraction and vector creation are crucial in fingerprint-matching algorithms. For increasing the confidence of fingerprint recognition, different feature vector forms are considered in literature. In this paper, we introduce a complete (fully-implemented) algorithm for fingerprint recognition. The work describes image pre-processing based on our previous works and feature vector creation that bases on sectionalisation.

PROBLEM STATEMENT

The main objective of this thesis is to develop a robust algorithm for fingerprint recognition, which extracts especially the correct and exact minutiae points imperative in identifying a person. Very few researchers have conducted research on fingerprint ridges in order to prove a difference in gender. Though the 'fingerprints' are one of the widely used, most reliable, mature biometric technologies and are considered legitimate proof of evidence in courts of law all over the world, very few techniques have been addressed for gender identification. Some researchershave confirmed the use of fingerprint for gender identification which will be more useful in shortlisting the suspects. The gender and the age classification are the two most vital tools in the field of forensic anthropology or in the identification and verification system. When both these classifications are implemented together, the results will be considered as a great contribution to the society and it will reduce the number of suspects and spot the criminals effortlessly. To construct and execute an algorithm to identify the gender and the age group of a human fingerprint .

PROPOSED METHODOLOGY

4.1 System level design

Here a fingerprint recognition system contains a sensor, minutia extractor and minutia matcher [Figure 4.1 (a)].

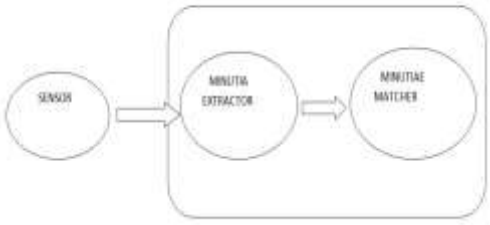

Figure 4.1 (a)

Optical and semi-conduct sensors are mainly used in fingerprint acquisition system. These sensors are of highly acceptable accuracy and high efficiency except for some cases like if the user‟s finger is too dirty or dry.To extract a minutia a three step approach is used such as:- i) pre processing stage ii) minutia extraction stage iii) post processing stage.

4.1.1 Pre-processing stage:-

Again pre-processing stage is divided in to three sub stages such as:- i) image enhancement ii) image binarization iii) image segmentation. For image enhancement we used two methods such as histogram equalization and Fourier transform. After enhancing the image we need to binaries the image for that we used the locally adaptive threshold method. For image segmentation we

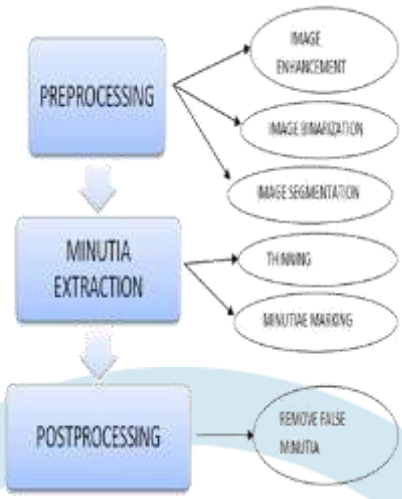

Figure 4.1 (b) [Minutia extractor]

preferred a three-step approach such as :- i) block direction estimation ii) segmentation by direction intensity iii) Region of Interest (ROI) extraction by Morphological operations

4.1.1 Pre-processing stage:-

Again pre-processing stage is divided in to three sub stages such as:- i) image enhancement ii) image binarization iii) image segmentation. For image enhancement we used two methods such as histogram equalization and Fourier transform. After enhancing the image we need to binaries the image for that we used the locally adaptive threshold method. For image segmentation we preferred a three-step approach such as :- i) block direction estimation ii) segmentation by direction intensity iii) Region of Interest (ROI) extraction by Morphological operations.

4.1.2 Minutia extraction

Minutia extraction stage is divided in to two sub stages such as:- i) fingerprint ridge thinning and ii) minutia marking We used iterative parallel thinning algorithm for minutia extraction stage. Ridge thinning is used to used to eliminate the redundant pixels of the ridge till the ridges are of one pixel wide.The minutia marking is quite simple task. Here crossing number (CN) concept is used.

4.1.3 Post processing stage

For the post processing stage, it has only one sub step that is removal of false minutia. Also a novel representation for bifurcations is proposed to unify terminations and bifurcation.

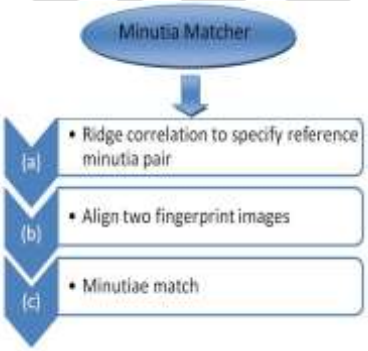

Figure 4.1 (c) Minutia matcher

EXPECTED RESULT

The above proposed methodology was really an effort to understand how the Fingerprint Recognition is used in many applications like biometric measurements, solving crime investigation and also in security systems. From minutiae extraction to minutiae matching all stages are included in this proposed method which generates a match score. Various standard techniques are used in the intermediate stages of processing.

REFERENCES

[1] 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.

[2] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancellable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.

[3] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–57, Dec. 2007.

[4] Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.

[5] Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.