ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 3 (Jul. - Sept. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Performance Evaluation of Biometric System for The Pattern Recognitiosion

[I]Neha, [II]Er. Kapil Arora
[I]M.Tech(Student), [II]Assistant Professor
[I,II]Dept. of ECE, RPIIT College, Karnal, Haryana, India

Abstract
Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. The work is done to develop a complete system for fingerprint verification through extracting and matching minutiae. To achieve good minutiae extraction in fingerprints with varying quality, preprocessing in form of image enhancement and binarization is first applied on fingerprints before they are evaluated. Many methods have been combined to build a minutia extractor and a minutia matcher. Minutia-marking with false minutiae removal methods are used in the work. The proposed work is based on elastic matching algorithm for minutia matching. This algorithm is capable of finding the correspondences between input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. We have proposed an improved framework for extracting high accuracy minutiae set, by integrating a robust point-based unsupervised segmentation algorithm, topological pattern adaptive finger print enhancement algorithm with singularity preservation, a thinning-free minutiae detection algorithm. The proposed work is performed on the software MATLAB 7.1 and the designs layout is performed on the Graphical user interface (GUI). The proposed work shows the results matching with different fingers of different persons.

Keywords
FFT, finger, Minutia, binarization etc

I. Introduction

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society, in which questions related to identity of an individual such as "Is this the person who he or she claims to be?", "Has this applicant been here before?", "Should this individual be given access to our system?" "Does this employee have authorization to perform this transaction?" etc are asked millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, etc. With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming more critical.[7]

A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user, and not anyone else. Examples of these systems include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of an impostor. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. The major advantages of this traditional personal identification are that

(i) They are very simple
(ii) They can be easily integrated into different systems with a low cost.

However these approaches are not based on any inherent attributes of an individual to make a personal identification thus having number of disadvantages like tokens may be lost, stolen, forgotten, or misplaced; PIN may be forgotten or guessed by impostors. Security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor; further, simple passwords are easy to guess (by an impostor) and difficult Passwords may be hard to recall (by a legitimate user).Therefore they are unable to satisfy the security requirements of our electronically interconnected information society. The emergence of biometrics has addressed the problems that plague traditional verification.

1. Biometric

In the world of computer security, biometrics refers to authentication techniques that rely on measurable physiological and individual characteristics that can be automatically verified. In other words, we all have unique personal attributes that can be used for distinctive identification purposes, including a fingerprint, the pattern of a retina, and voice characteristics. Strong or two-factor authentication—identifying oneself by two of the three methods of something you know (for example, a password), have (for example, a swipe card), or is (for example, a fingerprint)—is becoming more of a genuine standard in secure computing environments [9]. Some personal computers today can include a fingerprint scanner where you place your index finger to provide authentication. The computer analyzes your fingerprint to determine who you are and, based on your identity followed by a pass code or pass phrase, allows you different levels of access. Access levels can include the ability to open sensitive files, to use credit card information to make electronic purchases, and so on.

2. Biometrics Authentication Techniques

A biometric authentication is essentially a pattern-recognition that makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. An important issue is designing a practical approach to determine how an individual is identified. An authentication can be divided into two modules:

a.) Enrolment module
b.) Identification or Verification module

3. How Biometric Technologies Work

The enrolment module is responsible for enrolling individuals into the biometric system. During the enrolment phase, the biometric characteristic of an individual is first scanned by a biometric reader

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

to produce a raw digital representation of the characteristic. In order to facilitate matching, the raw digital representation is usually further processed by feature extractor to generate a compact but expensive representation, called a template. Depending on the application, the template may be stored in the central database. Depending on the application, biometrics can be used in one of two modes: verification or identification. Verification—also called authentication—is used to verify a person's identity—that is, to Authenticate that individuals are who they say they are. Identification is used to establish a person's identity—that is, to determine who a person is. Although biometric technologies measure different characteristics in substantially different ways, all biometric systems start with an enrolment stage followed by a matching stage that can use either verification or identification.

4. Biometric system

Among all biometric traits, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits anomalies in local regions of the fingertip, and it is the position and orientation of these anomalies that are used to represent and match fingerprints.

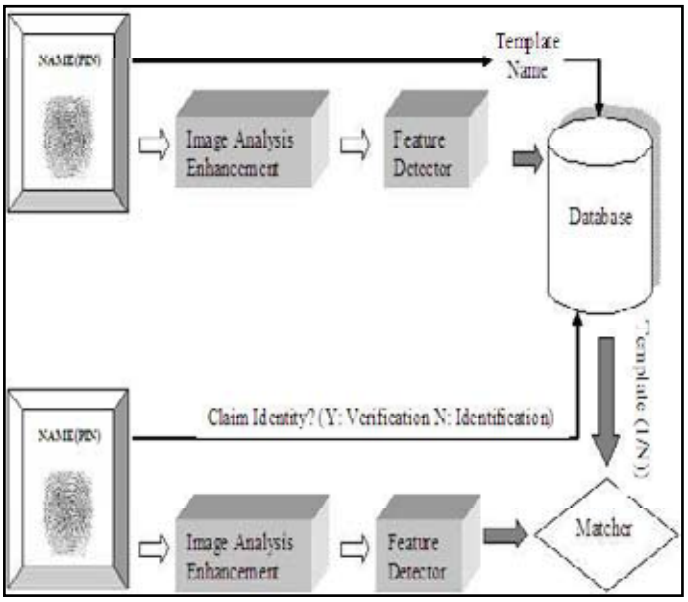


Fig. 1.1: biometric system[3]

Although not scientifically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual. Even identical twins having similar DNA, are believed to have different fingerprints. Traditionally, fingerprint patterns have been extracted by creating an inked impression of the fingertip on paper. The electronic era has ushered in a range of compact sensors that provide digital images of these patterns. These sensors can be easily incorporated into existing computer peripherals like the mouse or the keyboard, thereby making this mode of identification a very attractive proposition. This has led to the increased use of automatic fingerprint-based authentication systems in both civilian and law enforcement applications.

II. Literature Survey

Lin Hong performed a work, "Automatic Personal Identification Using Fingerprints". In his work the author used finger print for the identification. The author used in his work the phenomenon of minutia for the matching of ridges of different fingers print and obtained a satisfactory solution for the matching of the finger print. The simulation results in his work shows the better performance with matching criteria meeting above the threshold. The author in his work proposed the concept of automation system which was highly suitable for the personal identification based on finger prints.

D. Maio and D. Maltoni performed a work, "Direct gray-scale minutiae detection in fingerprints". The authors in this work proposed the concept of binarization and the conversion of an image into gray form to obtain the minutiae patter a better for the finger print matching. The authors performed the work in different environments and the result obtained were compared with others and found the better results. The author considers direct matching of gray scale minutiae which also gives better results in terms of speed.

L.Wang, H. Suo, and M. Dai performed a work "Fingerprint image segmentation based on Gaussian-hermite moments". In this work the author proposed a Gaussian hermite method for the segmentation of the finger print recognition. The image segmentation segments the image into proper patter for the proper matching of the segmented parts of the image pattern which is utilized for the fingerprint recognition.

FVC2002, http://bias.csr.unibo.it/fvc2002/ the work laboratory competition was held for the finger print recognition for the identification using finger print. The various finger images in our work are used from the same. The images pattern obtained from this has a unique identity and these are neither dry nor wet. So the finger print images used in this can be suitable used for the automatic biometric system for the finger print recognition. Therefore, the tiff finger images are taken from these proceedings to be used in our work.

J. Rogowska and M. E. Brezinski performed a work, "Evaluation of the Adaptive Speckle Suppression Filter for Coronary Optical Coherence Tomography Imaging," in this work the authors proposed a suppression filter method for the coronary optical coherence tomography imaging. The work was performed introducing the speckle noise and then filtering the image. The authors proposed the optical coherence concept and used the coherence and discussed the time aspects to perform the same. The simulation results are analyzed and give better environment.

III. Objectives

For the security point of view the finger print recognition has prime importance in every field such as in defence, companies, commercial, non- commercial areas etc for the recognition of the right person. As the method of recognition or even marking of attendance in the companies, colleges, school manually lead to many difficulties such as time wastage or the cognitive effect. The same can be solved with the automatic finger print recognition system. In our work we have used the pattern of human finger for the correct matching. However, the work is not limited to the finger prints only, the same can be extended with the effects of palm, eyes or face recognition.

Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. The work is done 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 linearization is first applied on fingerprints before they are evaluated. Many

methods have been combined to build a minutia extractor and a minutia matcher. Minutia-marking with false minutiae removal methods are used in the work. The proposed work is based on elastic matching algorithm for minutia matching. This algorithm is capable of finding the correspondences between input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. We have proposed an improved framework for extracting high accuracy minutiae set, by integrating a robust point-based unsupervised segmentation algorithm, topological pattern adaptive finger print enhancement algorithm with singularity preservation, a thinning-free minutiae detection algorithm. The proposed work is performed on the software **MATLAB 7.1** and the designs layout is performed on the **Graphical user interface (GUI).** The proposed work shows the results matching with different fingers of different persons.

IV. Proposed Methodology

Fingerprint Enhancement by Fourier Transform (FFT)
We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (1)$$

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.
In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.
Get the enhanced block according to:

$$g(x,y) = F^{-1}\left\{F(u,v) \times |F(u,v)|^{k}\right\} \quad (2)$$

where F-1(F(u,v)) is done by:

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v) \times \exp\left\{j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (3)$$

for x = 0, 1, 2, ..., 31 and y = 0, 1, 2, ..., 31.
The k in formula (2) is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation**.**

V. Results

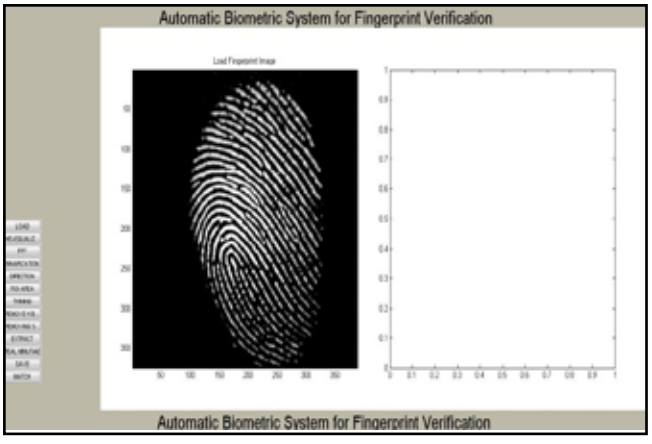


Fig. 1: loaded original image

Fig. 2: Histogram equalization

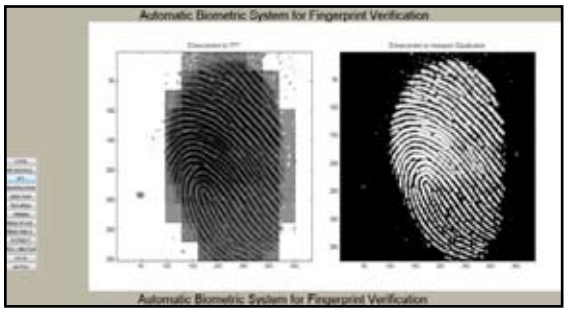


Fig. 3:After FFT enhancement

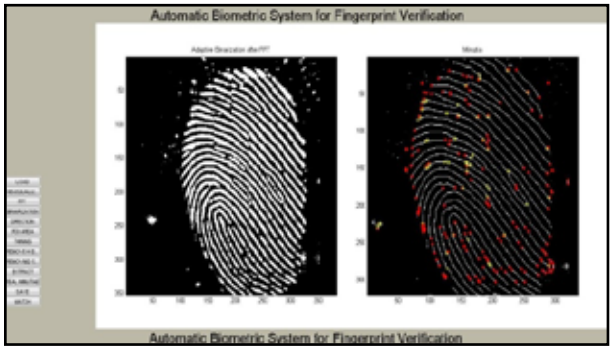


Fig. 4: Image after extract showing Minutia(right)

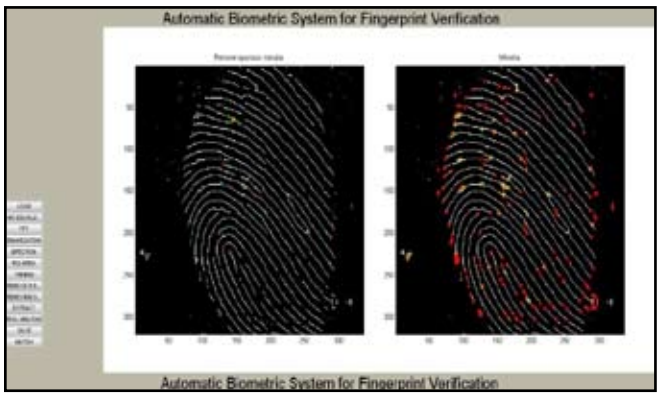
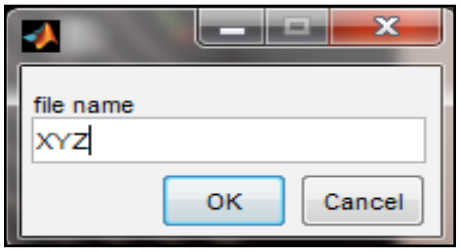
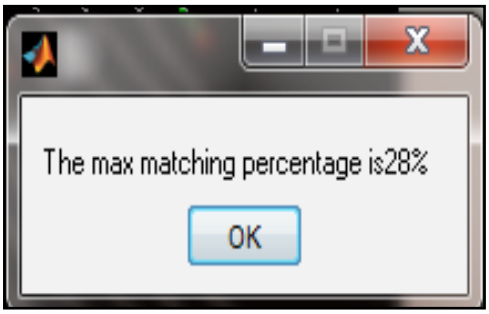
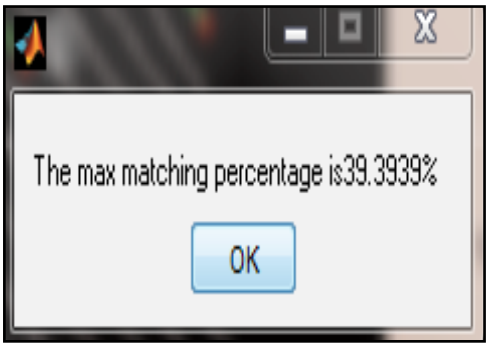


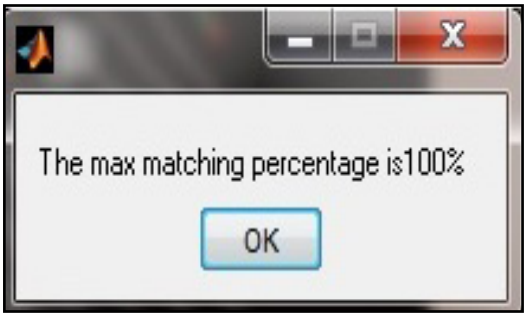
Fig. 5: Real Minutia marking (right) and False Minutia Removal (Left).



ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)







VI. Conclusion And Future Scope

The paper involves some novel changes like segmentation using Morphological operations, minutia marking with special considering the triple branch counting, minutia unification by decomposing a branch into three terminations, and matching in the unified x-y coordinate system after a two-step transformation are used in our project work which was not considered in the existing work.

Hence, the proposed automatic biometric system for the finger print verification gives the better performance with accuracy. The **MATLAB 7.1** environment on which the complete work is performed is highly compatible with the source code.

The same approach can be implemented using the neural network algorithm and ANFIS algorithm. There could be the improvement in the work for other types of images format and quality. The same work can be enhanced using the face recognition technique, speech recognition technique, iris matching technique etc

References

[1] *FVC2002.http://bias.csr.unibo.it/fvc2002/ 2010*

[2] *L.C. Jain, U. Halici, I. Hayashi, S.B. Lee and S. Tsutsui "Intelligent biometric techniques in fingerprint and face recognition" 1999, the CRC Press.*

[3] *M. J. Donahue and S. I. Rokhlin, "On the Use of Level Curves in Image Analysis, Image Understanding", VOL. 57, pp 652 - 655, 1992.*

[4] *A. Almansa and T. Lindeberg, "Fingerprint enhancement by shape adaptation of scale Space operators with automatic scale selection", IEEE Transactions on Image Processing, 9(12):2027–2042, 2000.*

[5] *F.Alonso-Fernandez, J. Fierrez-Aguilar, and J. Ortega-Garcia, "An enhance gabor filter-based segmentation algorithm for fingerprint recognition systems", In Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis(ISPA 2005), pages 239–244, 2005.*

[6] *S. A.M.Bazen, M. Van Otterlo and M. Poel. "A reinforcement learning agent for minutiae extraction from fingerprints", In Proc. BNAIC, pages pp.329–336, 2001.*

[7] *K. K. Hartwig Fronthaler and J. Bigun, "Local feature extraction in fingerprints by complex filtering", In Advances in Biometric Person Authentication, LNCS, volume 3781, pages pp.77–84, 2005.*

[8] *A. K. Jain, Y. Chen, and M. Demirkus, "A fingerprint recognition algorithm combining Phase-based image matching and feature-based matching", In Proc. of International Conference on Biometrics (ICB), pages 316–325, 2005.*

[9] *A. K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: Fingerprint matching using level 3 features" In Proc. of International Conference on Pattern Recognition (ICPR), volume 4, pp-477–480, 2006*

[10] *T.-Y.Jea. "Minutiae-Based Partical Fingerprint Recognition", PhD thesis, University at Buffalo, the State University of New York, 2005*

[11] *S. Klein, A. M. Bazen, and R. Veldhuis. "Fingerprint image segmentation based on hidden markov models", In 13th Annual workshop in Circuits, Systems and Signal Processing, in Proc. ProRISC 2009, 2009*

[12] *K. Mikolajczyk and C. Schmid, "Scale affine invariant interest point detectors" International Journal of Computer Vision, 60(1):pp.63–86, 2004.*

[13] *A. C. Pais Barreto Marques and A. C. Gay Thome "A neural network fingerprint Segmentation method", In Fifth International Conference on Hybrid Intelligent systems(HIS 05), page 6 pp., 2005*

[14] *G. Parziale and E. Diaz-Santana, "The surround imager: A multi-camera touchless device To acquire 3d rolled-equivalent fingerprints", In Proc. of IAPR Int.Conf. on Biometrics, LNCS, volume 3832, pages pp.244–250, 2006*

.