IJCSN International Journal of Computer Science and Network, May 2014
ISSN (Online) : 2277-5420
www.IJCSN.org

Technical Challenges for Biometric Science

[1] Dilip Tamboli, [2] Sandeep B Patil, [3] Dr. G.R.Sinha

[1] P.G. Scholar, Department of Electronics & Telecommunication Engg. SSGI Bhilai, C.G.India

[2] Associate Prof., Department of Electronics & Telecommunication Engg. SSGI Bhilai, C.G.India

[3] Associate Director & Prof., Department of Electronics & Telecommunication Engg. SSGI Bhilai, C.G.India

Abstract- The Biometric is the study of physiological or behavioral characteristics used for the identification of a person. These characteristics of a person include the features like fingerprint, face; hand geometry, voice and iris are known as biometrics. Typical physiological features measured include individual's fingerprints, retina, face, iris and hand. Typical behavioral features that can be measured include voice patterns, handwriting and keystroke dynamics. Basically we can use physiological characteristics than behavioral because behavioral characteristics are changed with age and environment whereas physiological characteristics never changed during whole life. In previous papers the overall matching algorithm were based on the clearly fingerprint images which was not applicable for dusty images, oily images characteristics. When these characteristics are forensics altered dusty images, oily images are challenged.

We have all heard about criminals who have altered their fingerprints so as not to be identified by law enforcement because of poor image quality and after long period dust covers the original fingerprint images. This paper focuses on an algorithm for latent fingerprint matching. The aim is to develop an algorithm for latent fingerprint matching using descriptor based Hough transform which is specially for dusty images used in law enforcement lab. Proposed algorithm achieves better accuracy and lower error rate while using the dusty fingerprint image as a biometric data.

Keywords- *biometric,fingerprint,physiological,behavioral, hough transform, law enforcement, latent.*

1. Introduction

The word " Biometrics" comes from the Greek language and is derived from the words "Bio" means life and " Metric" means to be measure, So biometrics is a field of science and technology used to be measure life characteristics. Biometric system uses physical (like fingerprint and retina) and behavioral (like voice and handwriting) parameters for person identification. Biometric data are unique for each individual person, even two identical twins. Basically we can use physical parameters than behavioral because behavioral parameters are changed with age and environment whereas physical parameters never changed during whole life.[1] Biometric technologies offer two means to determine an individual's identity: verification and identification. Verification confirms or denies a person's claimed identity by asking, "Is this person whom he/she claims to be?" Identification, also known as recognition, attempts to establish a person's identity by asking, "Who is the person?" Verification is a one-to-one comparison of the biometric sample with the reference template on file. A reference template is the enrolled and encoded biometric sample of record for a user. Identification makes a one-to-many comparison to determine a user's identity. It checks a biometric sample against all the reference templates on file. If any of the templates on file match the biometric sample, there is a good probability the individual has been identified.[2]
Many different types of unique physiological or behavioral characteristics exist for humans. Some of the more traditional uses of these biometric methods for identification or verification include: [2]

- Fingerprint recognition—Fingerprint recognition systems rely on the biometric device's ability to distinguish the unique impressions of ridges and valleys made by an individual's finger.
- Hand geometry—Hand geometry solutions take more than 90 dimensional measurements to record an accurate spatial representation of an individual's hand.
- Retina scanning—Retinal scanning involves an electronic scan of the retina, the innermost layer of the wall of the eyeball.
- Iris scanning—Iris scanning uses a camera mounted between three and 10 feet away from the person to take a high-definition photograph of the individual's eyes. It then analyzes 266 different points of data from the trabecular meshwork of the iris.
- Facial recognition—Facial recognition attempts to identify a subject based on facial

characteristics such as eye socket position, space between cheekbones, etc.

- Signature dynamics—Dynamic signature verification not only compares the signature itself, but also marks changes in speed, pressure and timing that occur during signing.
- Keystroke dynamics—Keystroke dynamics technology measures dwell time (the length of time a person holds down each key) as well as flight time (the time it takes to move between keys). Taken over the course of several login sessions, these two metrics produce a measurement of rhythm unique to each user.
- Voice recognition—Voice recognition biometrics digitize a profile of a person's speech into a template voiceprint and stores it as a table of binary numbers. During authentication, the spoken passphrase is compared to the previously stored template.

  Fingerprint-based identification is the most popular biometric technique used in automatic personal identification Law enforcement agencies uses it routinely for criminal identification. Now, it is also being used in several other applications such as access control for high security installations, credit card usage verification, and employee identification. The main reason for the popularity of fingerprints as a form of identification is that the fingerprint of a person is unique and remains invariant through age. [3]

A fingerprint is characterized by ridges and valleys. The ridges and valleys alternate, flowing locally in a constant direction. A closer analysis of the fingerprint reveals that the ridges (or the valleys) exhibit anomalies of various kinds, such as ridge bifurcations, ridge endings, short ridges, and ridge crossovers. Eighteen different types of fingerprint features have been enumerated in. Collectively, these features are called *minutiae*. For automatic feature extraction and matching, the set of fingerprint features is restricted to two types of minutiae: ridge endings and ridge bifurcations.[4]

We do not make any distinction between these two feature types since data acquisition conditions such as inking, finger pressure, and lighting can easily change one type of feature into another. More complex fingerprint features can be expressed as a combination of these two basic features. [4] For example, an enclosure can be considered as a collection of two bifurcations, and a short ridge can be considered as a collection of a pair of ridge endings.[4]

Biometrics is becoming an essential component of personal identification solutions, since biometric identifiers cannot be shared or misplaced, and they represent any individual's identity. Biometric recognition refers to the use of iris, fingerprint, face, palm and speech characteristics, called biometric identifiers. Fingerprint matching is a significant part of this process. It is an extremely difficult problem, due to variations in different impressions of the same finger. The problems stem from the fact that fingerprints of different users appear to be similar, whereas different finger impressions of the same user look different. [5]

Biometric recognition can be described as automated methods to accurately recognize individuals based on distinguishing physiological and/or behavioral traits. It is a subset of the broader field of the science of human identification. Technologies used in biometrics include recognition of fingerprints, faces, vein patterns, irises, voices and keystroke patterns (See Figure 1). In the subfield of telebiometrics, these recognition methods are applied to telecommunications. [6] In a non-automated way and on a smaller scale, parts of the human body and aspects of human behavior have been used ever since the dawn of mankind as a means of interpersonal recognition and authentication. For example, face recognition has been used for a long time in (non-automated) security and access applications, e.g., as a method to verify that the owner of a passport and the person showing the passport are the same, by comparing the person's face and the passport photo. [6]

The Digital Revolution added ICT as a means to fulfill recognition and authentication processes, often through PCs and computerized telecommunication devices, such as cash dispensers. Users authenticate themselves to the machine by entering a secret knowledge-based authenticator, such as a PIN or passphrase, or by the possession of a token, like a bank card or key, and sometimes authentication requires a combination of knowledge and possession. [6]

The 1960s also saw the first automated biometric recognition applications. However, the biometric industry did not take off at that time, due to high cost, low recognition accuracy and the lack of standards and testing benchmarks with which the different approaches could be compared and quality ensured. To further the use of biometric systems, issues of security and privacy will need to be carefully addressed, as well as the high levels of expectation in accuracy, reliability, performance, adaptability, and cost of biometric technologies for a wide variety of applications. [6]

(1) Fingerprint (2) Iris

(3) DNA (4) Keystroke pattern

Figure (1): Overview of some biometrics

2. The Design of Biometric System

It is divided into hardware and software.

The basic block diagram of a biometric system works in the following two modes. In verification mode the system Performs a one-to-one comparison of a captured biometric With a specific template stored in a biometric database in order to verify the individual is the person they claim to be. [7] In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. [7]

2.1 Matlab Software

An improved algorithm used in fingerprint matching, highly recommended for high-performance applications, biometric system improved database.

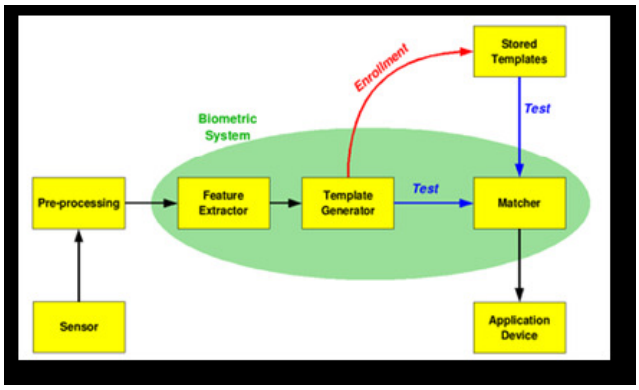


Figure (2): Biometric System Diagram

2.2 Sensors

Block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics we want to consider.

2.3. Pre-processor

Performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. Removing some noise), to use some kind of normalization, etc.

2.4. Feature Extractor

We have to extract the features we need. This step is really important we have to choose which features to extract and how. Moreover we have to do it with certain efficiency.

2.5. Template Generator

We can have a vector of numbers or an image with particular properties: all those data are used to create a template. A template is a synthesis of all the characteristics we could extract from the source, it has to be as short as possible (to improve efficiency) but we can't discard too many details, thus losing discrimination ability. Then the behavior of the system changes according to what was requested.

2.6. Matcher

It matches the image with the previously stored memory.

2.7. Stored Templates

The obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hammering distance).

2.8. Application Device

The decision that the matcher has taken is sent as output, so that it can be used for any purpose .it can allow a purchase or the entrance in a restricted area. [7]

3. Preprocessing

3.1 Histogram Equalization

It is a graphical representation of the intensity distribution of an image. It quantifies the number of pixels. It is a method that improves the contrast in an image in order to stretch out the intensity range. It is also used for increase the global contrast of an image.

Figure (3): Fingerprint after Histogram Equalization

3.2 Fast Fourier Transform

It is also used for image enhancement. Divide the image into block 32*32 pixels and perform FFT. It improves the appearance of the ridges, filling up small holes in ridges and bifurcation.

3.3 Binarization

Binarization is the process of alter a gray scale image to a black and white image (or binary image). In MATLAB, a value of one represents that the pixel is white and value of zero represents that the pixel is black. This modification of gray scale image to binary image is executed by using threshold process to the image. When a threshold process is applied to an image, each pixel values are analyzed to the input threshold. Those pixel values which are smaller than the threshold value is place to zero and those pixel value which are greater than the threshold value is place to one. At the end of this process each pixel values within the image are either zero or one, and the image has been modifying to binary form. After this conversion the ridges in the fingerprint are highlighted with black color while valleys are highlighted with white color. Binarization can be done in MATLAB using inbuilt function "im2bw". Example, b=im2bw („Input Image"); [1]

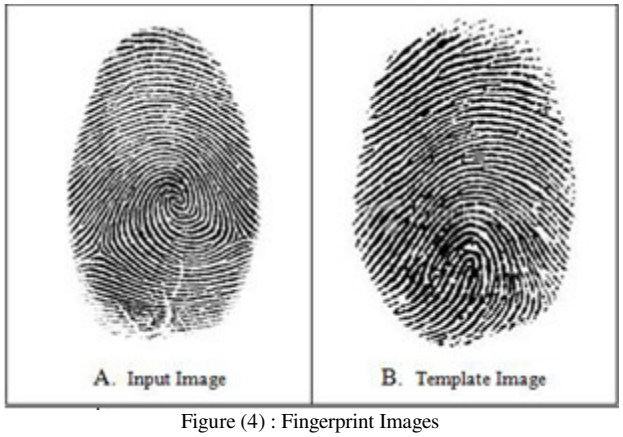


Figure (4) : Fingerprint Images

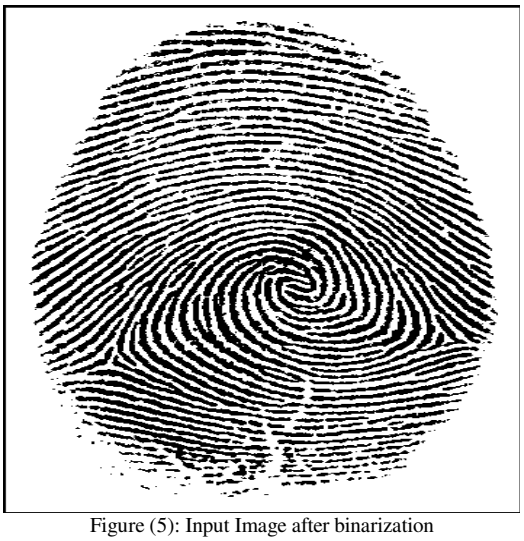


Figure (5): Input Image after binarization

3.4 Thinning

After binarization, next leading pre-processing technique used for matching process is thinning. Image thinning is the process of decrease the thickness of all ridges lines

into single pixel width. Thinning process does not convert the original x, y location and angle of direction of the minutiae points of the image, which assure the true calculation of minutiae points. It is also known as Block Filtering. Ridges thinning are used to destruct the extra pixel of ridges till the ridges are just one pixel broad .This is done using MATLAB‟s inbuilt morphological thinning function named as “bimorph”. Example, bimorph (“Binary image”, “thin‟, Info); Bimorph shows morphological operations on binary image. [1]

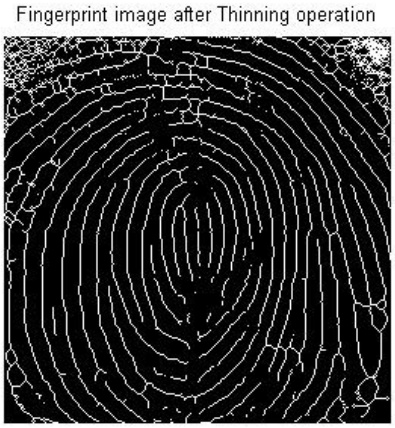
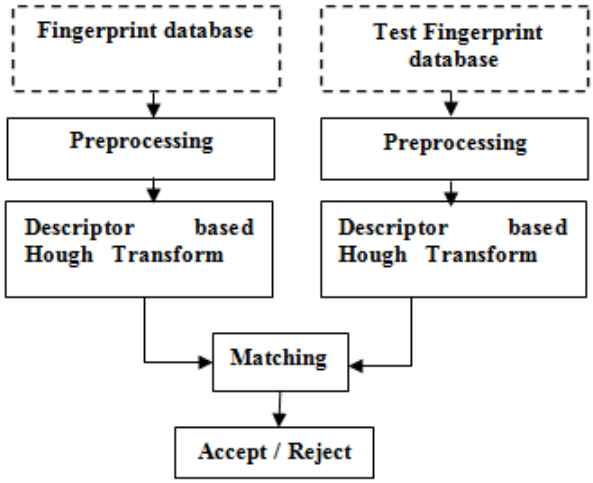


Figure (6) : Input Image after Thinning

4. Methodology

4.1 Flow Chart



4.2 Block Diagram

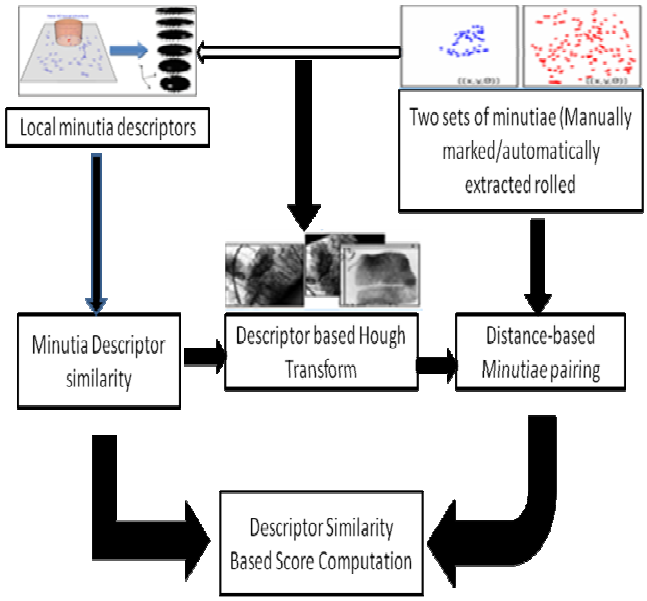


Figure (7): Latent Fingerprint Matching Approach

The Hough transform is frequently used to locate possibly occluded straight edges or lines in machine vision. Each detected edge pixel in a binary image votes for a potential edge upon which it might lie. The Hough transform is potentially suitable for video-rate applications such as motion detection but the computational burden is high, motivating hardware implementations. The underlying principle of the Hough transform is that there are an infinite number of potential lines that pass through any point, each at a different orientation. The purpose of the transform is to determine which of these theoretical lines pass through most features in an image – that is, which lines fit most closely to the data in the image. [8]

The input to a Hough transform is usually a raw image to which an edge detection operator is usually applied. Thus this way we guarantee that the set of points to be transformed are likely to be an “edge” in the image. The transform itself is quantized into an arbitrary number of bins, each representing an approximate definition of a possible line. Each feature in the edge detected image is said to vote for a set of bins corresponding to the lines that pass through it. By simple incrementing the value stored in each bin for every feature lying on that line, an array is built up which shows which lines fit most closely to the data in the image. By finding the bins with the highest value, the most likely lines can be extracted. The

simplest form of extracting those peaks is to apply some form of threshold operator which compares against some constant. But this threshold operator is not unique and different techniques can be applied yielding better results in different circumstances. [9]

Input to matcher: Manually marked minutiae in latents and automatically extracted minutiae in rolled prints.

Alignment: Each possible minutiae pair votes for a set of alignment parameters (translation and rotation); vote is proportional to the similarity between their local minutiae neighborhood of these peaks; one highest peak per fine parameter space is chosen as a candidate alignment.

Minutiae pairing: a minutiae pair (from aligned latent and rolled print) is considered a matched pair if the Euclidean distance and direction difference between the two are less than some prespecified threshold (one-to-one minutiae matching).

Score Computation: global matching score for each candidate alignment is the sum of the similarities of all matched pairs divided by the number of minutiae in the latent; final score between a latent and rolled print is the maximum score among the candidate alignment.

5. Conclusions

The presented fingerprint matching algorithm designed for matching latents to rolled/plain fingerprints which is based on a descriptor-based Hough Transform alignment. A comparison between the alignment performance of the proposed algorithm and the well-known Generalized Hough Transform shows the superior performance of the proposed method. The reported matching results for two different latent fingerprint databases with a large background database of around 32K rolled prints was reported. The comparison is made with three different state-of-the-art fingerprint matchers. The additional automatically extracted features will include improving the matching performance without an increase in manual labor. Thus the proposed matcher is more accurate than the two commercial matchers, they are significantly faster for dusty images.

References

[1] Bhargava Neeraj, Bhargava Ritu,Mathuria Manish and Cotia Minaxi, “Fingerprint Matching Using Ridge End and Bifurcation Points”, ICRTITCS,2012,PP.12-15

[2] Source://en.wikipedia.org/An overview of the Technology.

[3] Federal Bureau of Investigation, U.S.Government Printing Office, Washington, D.C.,”The Science of Fingerprints: Classification and Users”, 1984.

[4] Ratha Nalini K, Jain Anil K and Rover Dianej, “An FPGA Based Point Pattern Matching Processor With Application to Fingerprint Matching” IEEE, Vol.3, No.95, 1995, PP. 394-401.

[5] Baig Sabia, Ishtiaq Ummer, Kanwal Ayesha and Ishtiaq Usman, “Electronic Voting Machine System Using Fingerprint Matching with Gabor Filter”, Proceeding of International Bhurban Conference Applied Sciences & Technology Islamabad Pakistan,2011,10-13,PP.130-135.

[6] “Biometrics & Standards” ITU-T Technology Watch report, 2009.

[7] Habib Amber, Ateeq Ijlal Shahrukh and Hameed Kamran, “Biometric Security System Based on Fingerprint Recognition” IJSET, Vol.2, No.9, 2013, PP.892-894.

[8] Alessandra A. Paulino, Jianjiang Feng and Anil K.Jain, “Latent fingerprint matching using descriptor-based Hough transform”,IEEE Transaction On information forensics and security, 8(1),2013, 31-45.

[9] A Alessandra A. Paulino, Jianjiang Feng and Anil K.Jain, “Latent fingerprint matching using descriptor-based Hough transform” in Proc.Int.Joint Conf.Biometrics,2013 1-7.

[10] B. Miller.”Vital Signs Of Identify”, IEEE Spectrum, vol.34, 1994, pp.22-30.

[11] S. H. Lee, S. Y. Yi, and E. S. Kim, “, Fingerprint identification by use of a volume holographic optical, correlator”, Proc. SPIE **3715**, 1999, 321–325.

[12] T. J. Grycewicz, “Techniques to improve binary joint transform correlator performance for fingerprint, recognition”, Opt. Eng. 1999, **38**(1), 114–119.

[13] Y. Yan, G. Huang, W. Feng, G. Jin, and M. Wu, “Multichannel wavelet correlators for fingerprint identification, by the use of associative storage in a photorefractive material”, Proc. SPIE **3458**, 1998, 259–266.

[14] Zhiguo Yang, Yashuo Li, Yilong Yin, Xuzhou Li,, “A Template Selection Method Based on Quality for Fingerprint Matching”, 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),2012, IJECCT, 7(10), 1382-1385.