An Efficient Approach for Fingerprint Recognition

Dr. R. Satya Prasad  
Associate Professor,  
Dept. of Computer Science & Engg.,  
Acharya Nagarjuna University  
Nagarjuna Nagar, Guntur, AP, India

Muzhir Shaban Al-Ani  
Anbar University,  
College of Computer Science,  
CS Department – Anbar - Iraq

Salwa Mohammed Nejres  
Acharya Nagarjuna University,  
Department of Computer Science & Engineering, India

Abstract – For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. Most biometric systems use everyday sensors, such as a digital camera, to obtain the observations of an individual’s biometric; other sensors would need to be analyzed. This paper aims to design an efficient approach for fingerprint recognition in which implemented via many steps; fingerprint image acquisition, fingerprint isolation, fingerprint enhancement, then feature extraction. Two fingerprint images for left and right thumbs are considered to be tested in the implemented system, which indicated adequate results.

Keywords – Fingerprint Enhancement, Fingerprint Recognition, Biometric Recognition, Biometric Technology and Features Extraction.

I. OBJECTIVES

This work is done during realizing the following objectives:
- Data Collection of fingerprint images for many persons.
- Classifying and cleaning the fingerprint images according to their characteristics.
- Construct the algorithm to recognize the fingerprint images.

II. INTRODUCTION

Biometrics can be used in environments where recognition of an individual is required. Applications vary and range from logical access to a personal computer, to physical access of a secure office or building. They can be used in a variety of collection environments as identification systems. Biometrics are also used for accountability applications, such as recording the biometric identities of individuals boarding an aircraft, signing for a piece of equipment, or recording the chain of evidence. Of course, biometrics perform more reliably in controlled environments, such as offices and laboratories, than in uncontrolled environments, such as outdoors [1].

A typical biometric system is comprised of five integrated components. A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system-level decision [2].

Biometrics systems follow four basic processes: collection, extraction, comparison, and decision. Collection involves using a sensor to capture the biometric traits and convert them to a digital format. Extraction takes the digital data and converts the distinctive features into a compact template. In the comparison step, the biometric system measures the likeness of the template to those in the database. Based on the likeness, the system decides whether or not the submitted biometric matches one of the templates in the database [3].

III. IMAGE ENHANCEMENT

An image represented with lack of contrast when there are no sharp differences between black and white. Brightness refers to the overall lightness or darkness of an image. Contrast is defined as the separation between the darkest and brightest areas of the image. Increase contrast means you increase the separation between dark and bright, making shadows darker and highlights brighter. Decrease contrast means you bring the shadows up and the highlights down to make them closer to one another. One of the important image enhancement methods is to compensate the contrast over the gray scale distribution. The fundamental of texture related applications as texture analysis seeks to derive a general, efficient and compact quantitative description of textures so that various mathematical operations can be used to alter, compare and transform textures. Most available texture analysis algorithms involve extracting texture features and deriving an image coding scheme for presenting selected features [4,5].

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. An image is a 2D function f(x,y), where x and y are spatial coordinates and the magnitude of f at any point is called the intensity of the image at that point. When x,y and the intensity are discrete quantities we call the y When x, y and the intensity are discrete quantities we call the image a digital image. The elements of a digital image are referred to as pixels. An image which has M rows and N columns is defined to be an image of size MxN. An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. In a (8-bit) grey scale image each picture element has an assigned intensity that ranges from 0 to 255. A gray scale image is what people normally call a black and white
image, but the name emphasizes that such an image will also include many shades of gray [6,7].

IV. FINGERPRINT RECOGNITION

A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Manual comparison of fingerprints for recognition has been in use for many years, and has become an automated biometric identification technique over the past two decades. Fingerprints have an uneven surface of ridges and valleys that form a unique pattern for each individual. For most applications, the primary interest is in the ridge patterns on the top joint of the finger. A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space and are the low, shallow portion of the friction ridge skin. Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path. The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching. Pattern matching simply compares two images to see how similar they are. Pattern matching is usually used in fingerprint systems to detect duplicates [8,9].

There are three main fingerprint patterns and classifications that are consistently observed in different people include arches, loops and whorls as shown in figure (1). Arches are usually observed on the mid of the finger tip, and have friction ridges, that are run in a parabola from one side of the pattern to another without turning back [10].
- Arches are found in about 5% of fingerprint patterns encountered. The ridges run from one side to the other of the pattern, making no backward turn.
- Loops occur in about 60-70% of fingerprint patterns encountered. These patterns have an oblong delta and core that is shaped like a loop. The core especially appears like a bean. Ulnar loops and radial loops are two different patterns of loops.
- Whorls are also common as the loops and occur in about 25-35% people. In a whorl, some of the ridges make a turn through at least one circuit. Any fingerprint pattern which contains 2 or more deltas will be a whorl pattern. There are four types of whorl patterns include, plain whorl, central pocket whorl, double loop whorl and accidental whorl.

V. RELATED WORKS

Many papers and articles are published related to fingerprint recognition subject, and we will try to consider some of these works:

Mary Lourde R. et al. (2010) implemented an approach of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy. Two competing algorithms were designed and compared against a common database using MATLAB simulations. The proposed approach contains of five stages involved in finger scan verification and identification: fingerprint, image acquisition, image processing, locating distinctive characteristics, template creation, and template matching. 50 (25 pairs) fingerprint images of quality better than the rest were selected out of the total sum and fed first as input into the minutiae based matcher, and then into the filter-bank based matcher [11].

Yilong Yin R. et al. (2010) proposed a hybrid fusion method of fingerprint identification is proposed to solve Double Low problem. Firstly, minutiae-based and ridge-
Based matching algorithms are used orderly, which are kinds of serial fusion strategy. Secondly, a rank-level fusion is used, which is a kind of parallel fusion strategy. The obtained results on FVC2002DB1 and FVC2002DB2 indicate that only 6.6% fingerprints are falsely rejected on the average under zero false accept rate with our method, while 14.8%, 9.4% fingerprints are falsely rejected under zero false accept rate with the serial fusion strategy and the parallel fusion strategy, respectively. Two individual methods are implemented: One is the minutiae-based matching algorithm and the other is the ridge-based matching algorithm. The serial fusion method of the minutiae-based matching algorithm and the ridge-based matching algorithm, and the other is the rank-level parallel fusion method of the two individual methods were implemented in this paper [12].

Yan Huang R. et al. (2011) implemented a practical privacy preserving fingerprint matching system that offered the promise of obtaining results dependent on private data without exposing that private data. The main drawback is that current protocols for privacy preserving computations are very expensive and impractical for real scale problems. In this work, the costs can be substantially reduced for a large class of biometric matching applications by developing efficient protocols for Euclidean distance, finding the closest match, and retrieving the associated record. This approach involves using the normal by products of a garbled circuit evaluation to enable very efficient oblivious information retrieval, and we believe this technique can be extended to other applications [13].

Arun Jain R. et al. (2012) proposed a framework for integrating the soft biometrics with finger hand geometry that improves the personal verification system. In the proposed system, first the soft biometric trait such as weight is matched. If weight is matched then on the second stage the dimensions of finger thumb are matched while scanning the fingerprint for verification. The minutiae points are calculated and matched only when the second stage is cleared. This technique improved that FAR (False Acceptance Ratio) and total response time of verification system. This paper presented a simple and effective method of hybrid biometric verification, hand finger geometry identification and fingerprint verification system. Although the soft biometric characteristics are not as permanent and reliable as the traditional biometric identifiers like fingerprint, they provided some information about the identity of the user that leads to higher accuracy in establishing the user identity [14].

Jossy P. George R. et al. (2012) proposed a transform domain fingerprint identification based on DTCWT. The original Fingerprint is cropped and resized to suitable dimension to apply DTCWT. The DTCWT is applied on Fingerprint to generate coefficient which form features. The performance analysis is discussed with different levels of DTCWT and also with different sizes of Fingerprint database. The Fingerprint is preprocessed to a suitable size that suit DTCWT. The Fingerprint features are obtained by applying DTCWT with different levels. The test image features are compared with Database images using Euclidean Distance. It is observed that the recognition rate is better in the case of DTCWT level 7 compared to lower levels with PIDB: PODB of 40:10. [15].

Vikram Singh R. et al. (2012) explained a survey on hybrid system for finger print. The final matching score is estimated using fusing matching scores of minutiae based and wavelet based method. By measuring False reject rate (FRR) and false accept rate (FAR) the performance of hybrid fingerprint identification method is calculated. This method is better than conventional minutiae method for real time verification. The hybrid method tries to formulate the best of on minutiae features and wavelet statistical features. Minutiae offer rich information for fingerprint matching algorithm. It requires additional information for matching. Wavelet shows important features for complex matching of images like texture oriented patterns. This method combines minutiae and statistical features. Features are directly extracted from gray scale fingerprint image. This hybrid method is suitable for authentication in real time with number of identities enrolled in them [16].

Muzhir Shaban Al-Abi (2013) studied the existing fingerprint recognition algorithms in order to improve the performance of the proposed fingerprint algorithm to develop as efficient novel system. The proposed fingerprint algorithm is concentrated on the improvement of the thinning process fingerprint enhancement and minutiae extraction based on optimal thinning. The output results indicate a significant improvement of the fingerprint recognition pattern. Various human fingerprints patterns are collected using traditional and electronic devices then these patterns are converted to digital forms to be processed via the designed algorithm marry modifications are introduced to the implemented algorithm to generate an optimal results. The implemented algorithm gives adequate results related to the other systems. This work is done applying several steps to achieve his goal: Collect several fingerprint images for same person, Construct a specific fingerprint database, Classify the fingerprint according to their characteristics and construct the algorithm to recognize the pattern [17].

Shweta Malhotra R. et al (2013) used Multimodal biometrics that allows fusing two or more characteristics into single identification. It leads to more secure and accurate data. In this paper, they have combined two characteristics: one physical and one behavioral and further a key is added to the template to make it more secure. The template is finally stored in database In this research paper, unimodal and multimodal biometrics are introduced. Various level of fusion in multimodal biometrics and classification of multibiometrics have also been included. Further, an approach is introduced which includes multimodal biometrics and also key binding which helps to keep the templates secure and uniquely identify a person. With these two concepts the approach is called hybrid and can be used to accurately identify an individual. There are many multimodal biometric choice of optimal fusion level and redundancies in the extracted
features are some challenges in designing multimodal biometric system that needs to be solved [18].

Atul Ganbawle R. et al (2014) proposed a hybrid fingerprint matching algorithm. The minutiae features are ridge ending, short ridge, and bifurcation etc. In this paper, we conclude that, the results are combined between the pattern and minutiae matching score. In minutiae algorithm, images are not well performed in the input images and database images. The hybrid proposed work is divided into two parts, preprocessing and post processing. In pre-processing, the original fingerprint image is converted into gray scale image and after that it is converted into binary image. In post processing, make the thinned image as a perfect single pixel width image with continuity in the ridge flow connectivity is performed. In this process gives the better and accurate results than previous methods. The proposed method provides more accurate and high reliability results than existing methods [19].

Z.K Adeyemo R. et al (2014) developed a hybrid attendance system using RFID and biometrics. Students environment was considered for the investigation. In this paper, a method to solve attendance problem through coordinated hardware and software design handshaking data communications among RFID tag, RFID reader and fingerprint scanner serially interfaced to the digital computer system was proposed. Biometric data and personal details are stored on the RFID tag to secure the tag and eliminate the dependency on the real time central server for authentication. Performance was evaluated in terms of read time with and without wallet, encoding, attendance, and enrollment feature using 50 trials. The system model which consists of the coordinated hardware and software design was also developed. The performance was evaluated in terms of read time with and without wallet; the work has provided a convenient and secure method of attendance compared to the traditional method of attendance system. By using database, the data was more organized. Using fingerprint data header structure provides high security and high speed performance [20].

VI. THE PROPOSED APPROACH

The proposed image processing of surface analysis approach based on increasing features and details of the specimen to become more visible. Many steps are done to implement the procedure of construct the hybrid composite material via molding steps. Then images are taken before and after drying the specimen with the certain oven during a specific time. The main steps of the image processing system to highlight the details of the specimen in order to be ready for decision are described in figure (2). These steps are:

- **Image Acquisision**: in image processing it can be defined as the action of retrieving an image from some source including converting the optical image into digital form using digital camera to be ready for processing.

- **Image Prepressing**: including preparing fingerprint, fingerprint isolation, fingerprint image resizing.

- **Color image into gray scale**: including converting image into gray scale image.

- **Fingerprint isolation**: including recognized fingerprint images and then isolated from the image.

- **Image Enhancement**: including filtering and enhance the contrast of each gray level.

- **Feature Extraction**: including extract the effective features of image to be ready for extracting their characteristics.

- **Decision Making**: including the comparison between data to reach the correct decision.

![Fig.2. image processing approach](image)

VI. RESULTS AND ANALYSIS

Various data of fingerprint images are collected (5 images of right thumb and 5 images of left thumb). These images are converted into digital forms to be ready for processing. The image intensity function \( f(x, y) \) may be characterized by two components: illumination \( i(x, y) \) and reflectance \( r(x, y) \) as well as noise \( n(x,y) \) in which:

\[
f(x, y) = i(x, y) * r(x, y) + n(x, y)
\]

Where \( 0 < i(x, y) < \infty \) and \( 0 < r(x, y) < 1 \)

Enhances the contrast of images by transforming the values in an intensity image, so that the histogram of the output image approximately matches a specified
histogram. The contrast, especially in homogeneous areas, can be limited to avoid amplifying any noise that might be present in the image.

The processed fingerprint images are of size 300*400 are isolated to be implemented. Figures 3 to 10 show the result of each step in the processing system for left and right thumbs and their corresponding histogram. In which we can denote that the adaptive enhancement with figure (7) & figure (8) and Canny edge detector figure (9) & figure (10) show powerful fingerprint identification. The obtained results show an acceptable recognition of the processed images.
Fig. 7. Adaptive left thumb image and histogram

Figure (8) Adaptive right thumb and histogram

Figure (9) Canny detector left thumb and histogram

Fig. 10. Canny detector right thumb and histogram
VII. CONCLUSION

In addition to common electronics/computer and hardware failures, common biometric issues include poor-quality biometric samples, user confusion, evasion or non-cooperation, noise, inadequate lighting, noisy sensor, or subject handicaps.

The number of fingerprints required is application dependent based on the implementation details. While a single fingerprint might prove sufficiently accurate for certain applications, two fingerprints (left and right thumbs) may be required for increased levels of accuracy.

The data are collected via traditional ink fingerprint then these data are converted into digital image via scanner. The implemented approach shows that the combination of adaptive enhancement with the canny edge detector gives an efficient recognition approach.

REFERENCES


AUTHOR'S PROFILE

Dr. R. Satya Prasad

received Ph.D. degree in Computer Science in the faculty of Engineering in 2007 from Acharya Nagarjuna University, Andhra Pradesh. He received gold medal from Acharya Nagarjuna University for his out standing performance in Masters Degree. He is currently working as Associate Professor and H.O.D. in the Department of Computer Science & Engineering, Acharya Nagarjuna University. His current research is focused on Software Engineering, Software reliability. He has published several papers in National & International Journals.

Muzhir Shaban Al-Ani


Salwa Mohammed Nejres

has received B.Sc. in Computer Science from University of Mustansiriya, Department of Computer Sciences, Iraq (2001-2002). She completed her M.Sc. in Computer Science Department at Al-Anbar University in the field of data mining (2009-2010). She is currently a Ph.D. student in computer Science Department of Acharya Nagarjuna University (ANU), Nagarjunanagar, India, ANU College of Engineering & Technology.