# A Prototype Biometric Security Authentication System Based Upon Fingerprint Recognition

Wei Xiang[†], Bhavin Desai[†], Paul Wen[†], Yafeng Wang[‡], and Tianshu Peng[§]

[†]Faculty of Engineering and Surveying, University of Southern Queensland,
Toowoomba, QLD 4350, Australia, {xiangwei, pwen}@usq.edu.au
[‡]Beijing University of Posts and Telecommunications, Beijing 1000876, China
[§]Computing Centre of Gansu Provincial Department of Science & Technology
Lanzhou, Gansu Province 730030, China

**Abstract.** In this paper, we have proposed a prototype biometrics authentication system based upon fingerprint recognition. The major functional blocks of the proposed authentication system are presented in details. A simple but effective algorithm is proposed to detect and remove false minutia, which is able to considerably improve the system performance. The performance of the developed system is demonstrated to have a high level of accuracy through experimentation.

## 1 Introduction

Over the past decades, there is an ever-growing need to authenticate and identify individuals automatically. The process of determining the truthfulness of the claimed identity is termed authentication [1]. The currently prevalent technology of using a PIN or password for authentication is inadequate because they are disclosable, transferable and difficult to remember. Biometric-based methods are emerging as a robust and reliable means of security authentication.

Biometrics are automated methods of authenticating an individual's identity based upon a physiological or behavioral characteristic [2]. Among the characteristics measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voiceprint. With rapid progress in application areas such as enterprise-wide network security infrastructures, government IDs, secure electronic banking and investing, and health and social services, the need for highly secure identification and personal verification technologies is becoming apparent. Biometrics link events to particular individuals. As a result, utilising biometrics for personal authentication is convenient and considerably more accurate than current methods. Users have nothing to carry or remember. In contrast, a passwords or PIN may be difficult to remember or illegally used by someone other than the authorised user. When designing an automated system to handle large population identification, however, accuracy and reliability of authentication are significant challenges.

In this paper, we will discuss the development a prototype biometric security authentication system based upon fingerprint recognition. The reminder of the paper will be organised as follows. Section 2 provides an overview of biometrics security authentication systems and Section 3 details the fingerprint recognition technique. A prototype biometrics authentication system is proposed and its major functional blocks are discussed in detail in Section 4. Experimental results regarding the performance of the system are presented in Section 5, whereas conclusions are drawn in Section 6.

## 2 Biometric Security Authentication Systems

Biometric authentication uses a person's physiological aspects such as fingerprints, face, retina etc. These characteristics are unique for every individual. They remain unique for the lifetime and can provide secure means of authentication. Biometric security authentication systems possess unique benefits compared to traditional authentication systems, e.g., increased security, increased convenience, and better fraud detection, etc.

Biometrics consist of several distinct methods for authentication which uses different physical or behavioral aspects of humans such as fingerprint, face, iris, retina, hand geometry etc. Each method has its own advantages and drawbacks which decides its suitability for certain applications. In particular, fingerprint identification has received considerable attention over the last decades. It is a common misconception that fingerprint recognition is a solved problem. Despite significant research over past decades, fingerprint technology is nowhere near to the theoretical upper bound of the performance [3]. As a result, we consider the development of a prototype biometrics security authentication system based upon fingerprint recognition in this paper.

Accuracy is the most critical issue for any security authentication system. Various performance metrics may be used to evaluate the accuracy of biometrics systems. Among them, false acceptance rate (FAR) and false rejection rate (FRR) are the two most popular performance metrics. FAR in biometrics is the probability that a user's template will be incorrectly judged to be a match for a different user's template, whereas FRR is the probability that system declares no match between input pattern and database information incorrectly. In this paper, we will adopt both FAR and FRR to report on the performance of the developed biometrics security authentication system.

## 3 Fingerprint Recognition

Among all these biometric methods, fingerprint recognition is the most widely used and practical technology. It is the most mature biometric method which is used as a legitimate proof by the court of law all over the world. First of all, fingerprints are fully formed at about seven months of fetus development. Furthermore, fingerprint is proven to be unique for everyone even for identical twins, and remains unchanged throughout a person's life.

Fingerprints are classified initially according to global level features such as delta and core to reduce the size of matching possibilities. Though the global level features are important in classification and indexing, they are not distinctive enough for accurate matching. Local ridges of fingerprint form special characteristics, which are commonly known as minutia details. The major minutia features of fingerprint ridges include ridge bifurcation, ridge termination, and short ridge. Ridge bifurcations are points at which a single ridge split into two ridges, whereas ridge termination is the point at which a ridge terminates. Short ridges are ridges which are significantly shorter than the average length of ridges in the fingerprint. Minutiae patterns are very important in the analysis of fingerprints since they are the most distinct features of fingerprint.

Performance of the matching algorithm in fingerprint recognition largely depends on the quality of the acquired fingerprint image. In practice, a significant amount of captured fingerprint images are of poor quality [4]. Therefore, preprocessing is often applied to fingerprint images in order to enhance fingerprint features, thereby increasing the robustness of the feature extraction process. There are many preprocessing methods to improve the quality of fingerprint images, e.g., histogram equalisation, image binarisation, ridge thinning, etc.

Salient and unique features of fingerprint images need to be extracted for the purpose of fingerprint recognition. Feature extraction is a task of extracting singular points in a thinned ridge map. The minutia extraction algorithm is of prime importance in fingerprint recognition applications. Minutia extraction is the process of locating minutia details in the thinned fingerprint image map. Ridges in the map are one pixel wide and either black or white. To extract these features ridge pixels with three neighboring pixels (bifurcation) and with only one neighboring pixel (termination) are identified. Due to the effect of noise, a large amount of spurious minutia may be detected through the minutia detection process. Postprocessing techniques can be applied to identify genuine minutia and remove spurious ones.

Minutia matching algorithms compare minutia features extracted from input fingerprint images. Their objective is to determine whether or not the prints were originated from the same finger. In typical minutia matching algorithms, a threshold value is set. A decision is made based upon whether the matching score is greater or less than the predetermined threshold.

## 4 Prototype Fingerprint Authentication System

In this section, we introduce a prototype biometrics authentication system based upon fingerprint recognition. Matlab is used to implement a graphical user interface (GUI) and underlying image enhancing, minutia extraction, and matching algorithms. The Matlab GUI is interfaced with a Microsoft fingerprint scanner for capturing realtime fingerprint images.

### 4.1 Preprocessing

Preprocessing is applied to scanned fingerprint images in order to enhance image quality, and thereby aid in the subsequent minutia extraction and matching processes. Histogram equalisation, Fourier transform, and image binarisation are three preprocessing techniques that are applied in the proposed system.

Scanned images often have a limited range of colours or lack contrast. Histogram equalisation is an image processing technique for adjusting dynamic range and contrast of images [5]. An image histogram is a graphical representation of the tonal distribution of the occurrences of each intensity value in the image. Mathematically, the histogram of a digital image with $L$ possible intensity levels in the range of $[0, G]$ is defined as

$$p(r_k) = \frac{n_k}{N}, \tag{1}$$

where $r_k$ is the $k$th intensity level in $[0, G]$, $n_k$ is the number of pixels in the image whose intensity levels are $r_k$, and $N$ is the total number of pixels.

Histogram equalisation allows for areas of lower local contrast to gain a higher contrast without affecting the global contrast. This is achieved through spreading out the most frequent intensity values. The new intensity value $s_k$ of the equalised image corresponding to the input value of $r_k$ is given by

$$s_k = \mathit{\Gamma}(r_k) = \sum_{j=1}^{k} p(r_j). \tag{2}$$

To reduce the computational complexity of the subsequent minutia extraction and matching algorithms, image binarisation is adopted. The primary objective of the process is to differentiate object pixels from background pixels. A threshold value is chosen to binarise the image. Pixels are binarised to 1's or 0's depending upon whether they are greater or less than the predetermined threshold. In this paper, we choose the mean of the image as the threshold value.

### 4.2 Minutia Extraction

In the fingerprint image only ridges and valleys contain minutia and other features. Segmentation is the process of extracting foreground (containing ridges) from the background. If minutia extraction algorithm is applied to background regions, it results in extraction of noisy and spurious minutia. Hence it is important to specify the boundary region for ridge-valley portion and apply extraction to that region only.

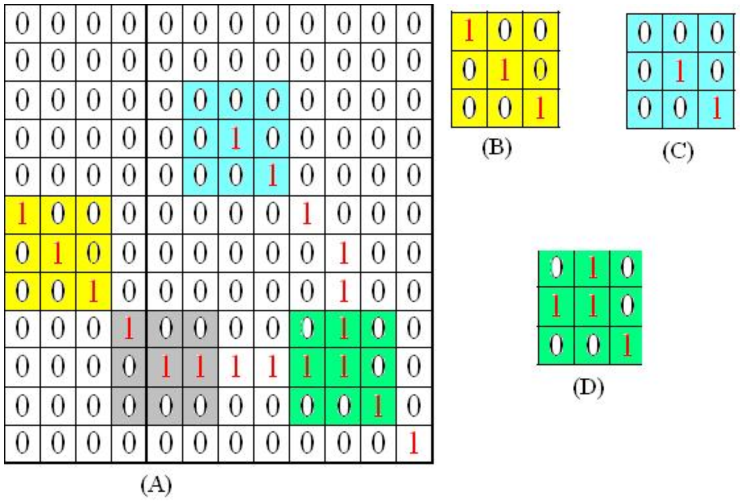
The prototype system adopts the method of variance thresholding [6] for the purpose of segmentation. According to the algorithm, the image is divided into $16 \times 16$ pixel blocks. The variance $V(k)$ of block $k$ can be determined through the following equation

$$V(k) = \frac{1}{W^2} \sum_{i=0}^{W} \sum_{j=0}^{W} (I(i,j) - M(k))^2, \tag{3}$$

where $I(i,j)$ is the intensity value of pixel at $(i,j)$, $M(k)$ is the mean intensity of block $k$, and $W$ is a constant of 16. The variance computed by (3) is compared against a threshold value, which is set to 0.05 in our system. If the variance of the block is less than the threshold, the block will be determined as background and thus discarded.

After segmentation ridge thinning is performed so as to make all ridges exactly one pixel wide being represented by binary 1's. This removes extra points on the ridges without removing small objects, and thus makes the following operation of minutia extraction much easier and reduces the possibility of false minutia detection.

Fig. 1 graphically illustrates the process of the minutia extraction algorithm. As shown in the figure, ridges are represented by binary 1's, whereas background (valley) is represented by 0's. The image is divided into 3 × 3 blocks as shown in Fig. 1(A). The middle pixel of each block is extracted and all other pixels which have a value of one are counted. In Fig. 1(B), there are exactly two 1's in the block except for the center pixel. This indicates that this block contains a normal ridge. In Fig. 1(C), there is only one 1 in addition to the middle pixel. This represents *minutia termination*. In Fig. 1(D), there are three 1's except for the centre pixel. This denotes *minutia bifurcation*. The locations of all genuine ridges identified through the above process are stored in a matrix for later reference.



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

(A)

| | | |
|---|---|---|
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

(B)

| | | |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

(C)

| | | |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 0 |
| 0 | 0 | 1 |

(D)

**Fig. 1.** Illustration of minutia extraction. (A) part of image with 3 × 3 blocks marked; (B) normal 3 × 3 pixel block; (C) ridge termination; (D) bifurcation.

Scanned fingerprint images usually contain a considerable amount of noise. This will cause significant performance deterioration for the authentication system. We only consider ridge bifurcations and ridge terminations as genuine minutia. All other features such as island, spur, spikes, and holes need to be identified and marked as false minutia.

We propose a simple but effective algorithm to detect and remove false minutia. The algorithm identifies and treats all very closely located minutia as false minutia, e.g., termination - bifurcation, bifurcation - bifurcation, and termination - termination. The rational behind this method is that if two detected minutia are located very closely to each other, it is highly likely that both of them are situated on the same ridge or neither of them is genuine minutia. The effectiveness of this false minutia removal algorithm will be demonstrated in Section 5 through experimental results.

### 4.3 Minutia Matching

Minutia matching is the process of determining whether a template image from the database and a query fingerprint image are from the same finger. More precisely, assume $m$ and $n$ are the number of minutia in the template $T$ and query fingerprint $Q$. Denote by $x$,$y$, and $\theta$ the $x$ coordinate, $y$ coordinate and orientation of minutia. $T$ and $Q$ can be represented by $T = ((x_1^T, y_1^T, \theta_1^T), \cdots, (x_m^T, y_m^T, \theta_m^T))$ and $Q = ((x_1^Q, y_1^Q, \theta_1^Q), \cdots, (x_n^Q, y_n^Q, \theta_n^Q))$. The task of minutia matching is to yield a matching score, and determine whether $T$ and $Q$ are from the same finger.

Minutia matching involves two stages, i.e., the alignment stage and matching stage [6]. The first stage aligns all minutia in the query image $Q$ according to the coordinates of minutia in the template image $T$ through a series of translation and rotation. However, it is almost impossible to match all parameters, i.e., $x, y, \theta$, even after alignment due to deformations and noise. To overcome this problem a bounding box of fixed length is defined around the aligned minutia. If the corresponding template minutia is within that box range and direction discrepancy between them is very small, they are considered as a matching pair.

If the number of matching pairs are denoted by $M_{TQ}$, the matching score $S$ can be determined by

$$S = \frac{100 M_{TQ}}{M_T M_Q}, \tag{4}$$

where $M_T$ and $M_Q$ are the number of minutia in the template and query image, respectively. The matching score $S$ is compared to a threshold value to determine whether or not the two fingerprint images are matched.

## 5 Performance Evaluation

In this section, we report on the performance evaluation results of the developed prototype biometrics authentication system. FAR and FRR mentioned in Section 2 will be used as the primary performance metrics.

As discussed in Section 4.1, the system implements the histogram equalisation technique to improve the quality of the scanned fingerprint. Fig. 2(A) and (B) illustrate the original captured fingerprint image and its histogram. Apparently, the histogram suggests that the image is dominated mostly by bright pixels, whose contrast can be considerably enhanced through histogram equalisation. Fig. 2(C) and (D) demonstrate the equalised image and the corresponding histogram. Clearly, the ridges appear darker and clearer than in the original image after histogram equalisation.

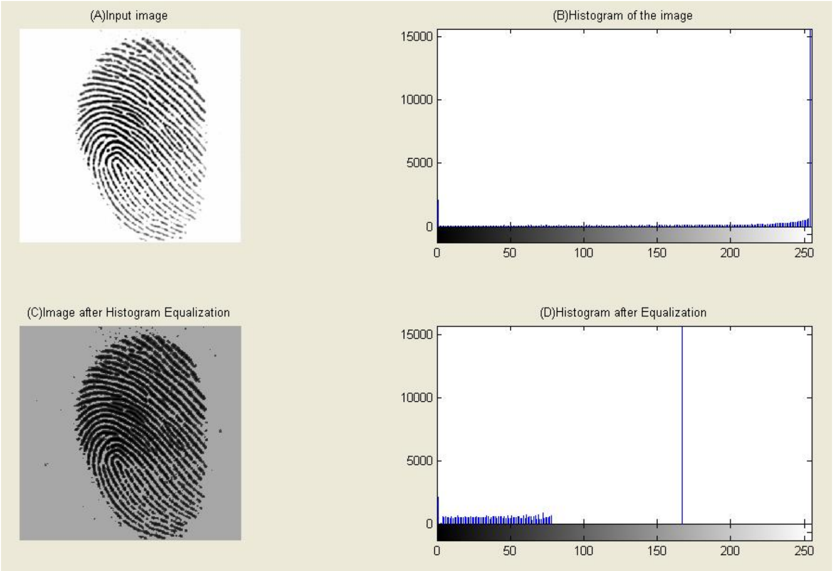


**Fig. 2.** Histogram equalisation result.

Fig. 3 demonstrates the result of initial minutia extraction. More specifically, Fig. 3(A) depicts the minutia features of the fingerprint after image binarisation and ridge thinning as discussed in Section 4. As a comparison, Fig. 3(B) shows the result of minutia extraction, where bifurcations are marked with the yellow + sign and terminations are marked with the red $*$ sign.

Fig. 4 illustrates the result after applying the simple false minutia detection and removal algorithm as introduced in Section 4.2. Comparing Fig. 4(A) to Fig. 4(B), it can be clearly seen that most false minutia is removed after applying the proposed algorithm.

Finally, we present the result on FAR and FRR using fingerprint images from the FVC2000 fingerprint database [7]. Seven image sets are used. Each set image contains eight different images for the same fingerprint. To measure FAR, the first image of each set is matched against any image from all other image sets. Similarly, to measure FRR, the first image of each set is compared against all other images from the same set. The results are listed in Table 1. Note that the threshold for the matching score in (4) is set to 25 in all experiments. Table 1 clearly demonstrates the high accuracy of the developed fingerprint recognition system.

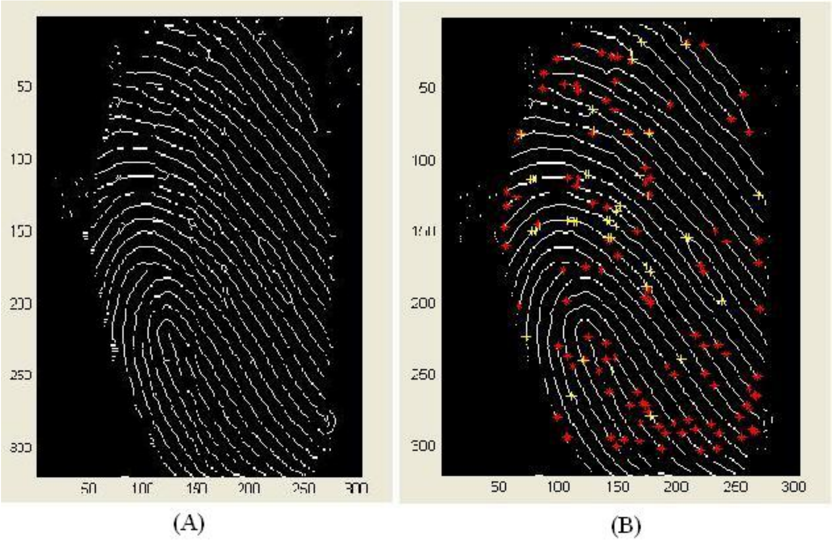


**Fig. 3.** Minutia extraction result. (A) binarised and thinned input image; (B) marked minutia.

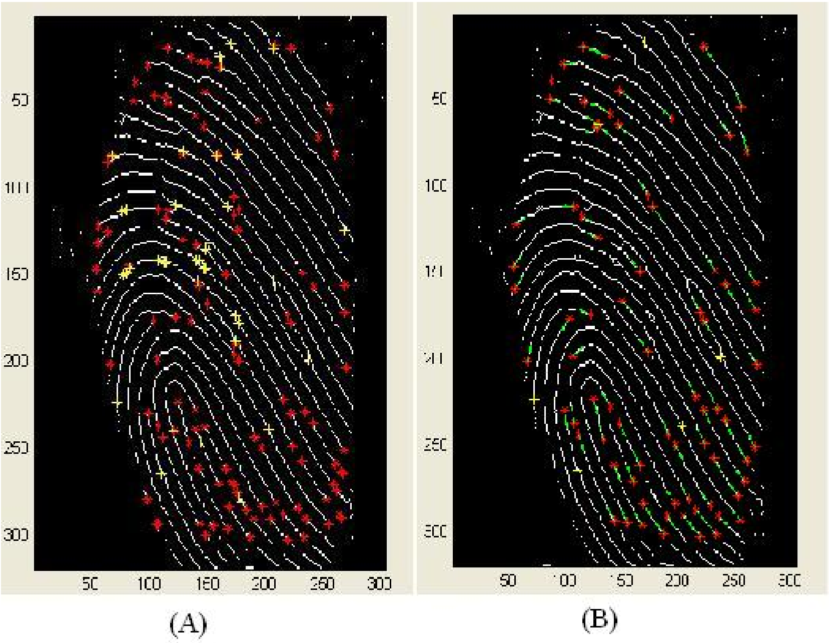


**Fig. 4.** False minutia detection and removal result. (A) fingerprint image with all minutia detected; (B) fingerprint image with false minutia removed.

**Table 1.** FAR and FRR performance evaluation results.

| Fingerprint set | FRR (%) | FAR (%) |
|---|---|---|
| Set 1 | 9.2 | 8.7 |
| Set 2 | 7.6 | 5.2 |
| Set 3 | 9.8 | 8.6 |
| Set 4 | 9.9 | 8.9 |
| Set 5 | 6.7 | 5.0 |
| Set 6 | 9.8 | 9.1 |
| Set 7 | 6.5 | 7.2 |

## 6 Conclusions

In this paper, we have proposed a prototype biometrics authentication system based upon fingerprint recognition. An overview of biometrics authentication systems is presented, which introduces a variety of biometrics techniques. More specifically, this paper provides a detailed understanding the fingerprint recognition technique.

The major functional blocks of the proposed authentication system are presented in details. A simple but effective algorithm is proposed to detect and remove false minutia, which is able to considerably improve the system performance. The performance of the developed system is demonstrated to have a high level of accuracy through experimentation.

## References

1. Jain, A. K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20 (2004)
2. Nanavati, S., Thieme, M., Nanavati, N.: Biometrics: Identity Verification in a Networked World, John Wiley & Sons, New York (2002)
3. Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S.: Handbook of Fingerprint Recognition, Springer, New York (2005)
4. Zhang, D. D.: Biometric Solutions: For Authentication in an E-World, Springer, Berlin (2002)
5. Gonzalez, R. C., Woods, R. E.: Digital Image Processing, 3rd edition, Prentice Hall, Upper Saddle River, NJ (2008)
6. Hong, L.: Automatic Personal Identification Using Fingerprints, Ph.D. Thesis, Michigan State University (1998)
7. FVC2000: Fingerprint Verification Compitition, `http://bias.csr.unibo.it/fvc2000/download.asp`