Technology Review: Image Enhancement, Feature Extraction and Template Protection of a Fingerprint Authentication System

Md. Rajibul Islam, Md. Shohel Sayeed and Andrews Samraj
Faculty of Information Science and Technology, Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia

Abstract: Nowadays, biometric technologies are turning into the basis of a widespread array of vastly secure recognition and authentication solution for an individual. Biometric recognition is the automated detection of a human being that is based on behavioral or physiological characteristics. The need for highly secure detection and personal verification technologies is becoming apparent, as the level of security breaches and transaction fraud increases. The core intention of this paper is to review the widespread research that has been done on the image enhancement, feature extraction as well as template protection of the fingerprint authentication system over the previous few decades. Especially, it discusses the techniques of enhancement, extraction and protection that have been implemented in order to solve the problem. To conclude, it illustrates experimental outcomes from the modern fingerprint authentication schemes that have been experienced with the FVC2004 Database.

Key words: Biometrics, image enhancement, feature extraction, template protection, fingerprint authentication

INTRODUCTION

Individual data privacy and confidential financial transactions can be offered by biometric-based solutions. The demand for biometrics can be found in commercial applications such as financial transactions, law enforcement agencies, retail sales, health and social services are already promoting these technologies. Data protection, network, workstation and domain access, single sign-on, application logon, transaction security and Web security as well as remote access to resources are incorporated by biometric-based authentication applications. It is very essential nowadays to trust in these electronic transactions for the healthy growth of the global economy. Biometrics are set to saturate nearly all aspects of our daily lives and the economy, whether utilized alone or integrated with other technologies such as smart cards, digital signatures and encryption keys.

This section presents the background of the fingerprint identification and verification systems and the numerous techniques that were utilized in fingerprint authentication systems. Seow et al. (2002) investigated the suitability of the fingerprint-scanned image to be verified via inverse Fast Fourier Transform after a thinning process and their technique applied directly onto a gray-scaled fingerprint image without pre-processing. Wang et al. (2002) developed a fingerprint classification algorithm that was based on directional fields to reduce time for fingerprint classification. Bella et al. (2003) developed the security of Smartcard simulating MCC (Match On Card) using TOC (Template On Card). A novel protocol was projected to address the problem of user authentication to smartcards using devices that were inexpensive. Moon et al. (2003) described the implementation of the USB Token System for fingerprint verification. Florian et al. (2004) portrayed a protocol to solve the problem of comparing fingerprints without actually exchanging them. Sanchez-Reillo et al. (2004) illustrated the architectures for Biometric Match-on-Token which would be more secure and reduced users’ potential rejection. Mohamed Mostafa (2005) explained a novel algorithm, which was much faster and reliable for fingerprint identification system. The new algorithm was named as a novel binary line-pattern algorithm for embedded fingerprint authentication system. The algorithm proposed by Mohamed Mostafa (2005) had reached a higher identification precision for the poor quality fingerprint with less memory and complexity compared with conventional methods. Another fingerprint authentication was investigated and described by Patrick et al. (2005). They presented a platform based design approach for this application, based on a ladder of Virtual Machines (VM). Farid and Moskowitz (2005) presented a fingerprint authentication based on
composite signature watermarking. Digital watermarking is a technology to bury information in digital media. They extended the digital watermarking technique Phasemark™, originally developed solely for image verification, to biometrics to assist in forensic analysis. Emiko et al. (2006) developed a new fingerprint sensor that had a novel sensing principle in order to solve some problems such as the fact that captured fingerprint images are easily affected by the condition of the finger surface and the manner of finger pressing due to the sensing principle and it can degrade authentication performance. Arun et al. (2006) presented fingerprint warping using ridge curve correspondences to improve matching performance.

FINGERPRINT IMAGE ENHANCEMENT

Biometrics proposes an effective approach to recognize subjects because it is concerned with the unique, reliable and stable personal physiological features.

Corrupted and occluded regions can be improved by the contextual information from the contiguous neighborhood because of the regularity and continuity properties of the fingerprint image. Hong et al. (1998) tagged such regions as ‘recoverable’ regions. The filters themselves may be classified in the Fourier or spatial domain. A computerized enhancement algorithm’s effectiveness depends on the scope to which contextual information is exploited. Islam et al. (2007a, 2008a) developed a fingerprint image enhancement technique using gamma manipulation and gamma correction with a few conventional enhancement techniques to support in gaining better feature information from low resolution and poor quality fingerprints. Bader et al. (1995) portrayed an enhancement filter. Regions in real images are rarely harmonized in gray level and are sharp along their borders because of blur and noise. An enhancement filter that reduces these effects will yield an improved segmentation result which is known as preprocessing the image. A parallel median algorithm was illustrated by Bader and Jain (1996). Westman et al. (1990) have proposed a general-purpose procedure for image segmentation which mingles iterative image enhancement through a Symmetric Neighborhood Filter (SNF) with an iterative and Hierarchical Connected Component (HCC) analysis. There is still a need for successful methodology to clean the valleys between the ridge contours. Wu et al. (2004) tested that noisy valley pixels and the pixels in the interrupted ridge flow gap were impulse noises. For that reason, they illustrated a new approach to fingerprint image enhancement which was based on integration of Anisotropic Filter and Directional Median Filter (DMF). Gonzalez and Woods (2002) and Shapiro and Stockman (2000), median filter is carried out as swapping a pixel with the median value of the preferred neighborhood. Essentially, the ridges and valleys in a fingerprint image interchange in a reasonably steady frequency and remain in a local constant direction (Ratha et al., 1995). Visibly, the Gabor filter considers the frequency and orientation of the images concurrently (Hong et al., 1998).

The Directional Filter Bank (Bamberger, 1990; Bamberger and Smith, 1992) is composed of a synthesis bank and an analysis bank (analysis filter bank). However it has the inconvenience of frequency scrambling when a low frequency area is misplaced in the subband images resulting in distortions in the decomposed directional subband images (Bamberger, 1990; Bamberger and Smith, 1992). Nevertheless, the DFB used in their study removes frequency scrambling during back-sampling and resampling matrices (Park, 1999). Sherlock et al. (1994) performed contextual filtering absolutely in the Fourier Domain. Sherlock et al. (1994) illustrated that the filter’s angular bandwidth was taken as a part wise linear function of the distance from the singular points such as core and delta. As a substitute, Ravishankar (1994) developed the angular coherence measure. This was stronger to errors in the orientation estimation and omitted the estimation of the singular point location. Watson et al. (1994) proposed one more approach for performing improvement in the Fourier domain and this was derived from root filtering technique (Jain, 1989). Here the image was separated into overlapping blocks. During attenuating the weak components that approach had the effect of increasing the dominant spectral components. This very closely resembled matched filtering (Jain, 1989). Further dissimilarities of Fourier domain enhancement algorithm may be located in Maio et al. (2004).

The fingerprint enhancement block has the task of enhancing the fingerprint on each impression of each user by the code which loosely follows the approach presented by Kovacevski (2000). Just before feature extraction a thinning process needs to be performed as indicated in Zhang and Suen (1984). In this process two tests are run one after the other until none of them discover pixels that need to be removed. However, this method does not meet the requirements imposed to a thinning algorithm because it still leaves a few spurious structures that do not permit a single point inside a line to have only two neighbors, a ridge-end only one and a bifurcation three. The minutiae extraction process defined in Acero and Baja (1984), used matrices of 3×3 pixels to search for typical minutiae, that is, ridge end and ridge bifurcations. The gamut mapping may reduce the effect of the image processing algorithm (Dijk and Verbeek, 2006). An enhanced fingerprint matching approach was applied using TSVM
(Jia and Cai, 2005) to evaluate the performances after image enhancement of the fingerprint authentication system.

**FEATURE EXTRACTION OF FINGERPRINT**

Various kinds of biometrics and various types of sensors too are available in the market which is being used for personal identification (Kang et al., 2003). It is very important to acquire good quality images but in practice a significant percentage of acquired images are of poor quality due to some environmental factors or user’s body condition (Jain et al., 1999). Robust fingerprint minutiae extraction systems impose computational requirements that are difficult to fulfill for a processing system (Hong et al., 1998). Therefore, various approaches were proposed for several years to increase the performances of the feature extraction algorithms.

Ratha et al. (1995) proposed an adaptive flow orientation supporting segmentation or binarization algorithm. There the orientation field was computed to find the ridge directions at each point in the image. Maltoni et al. (2003) offered a feature extraction algorithm that works straightforwardly on gray scale images. Most of the techniques working with gray level images are based on ridge following. The difference between the approaches of Ratha et al. (1995) and Maltoni et al. (2003) is that, Ratha et al. (1995) approach is a point wise operation and Maltoni and Maio et al. (2003) approach is based on ridge detection wherever each ridge is successively traced along its complete length. Through this approach, the neighboring maxima cannot be consistently located in poor quality images and as a result, false positives are still established.

Islam et al. (2007b, 2008b) presented a new feature extraction approach by using projection incorporated subspace method with principal component analysis and region merging technique to obtain the entire minutiae information in improving the matching performance of the fingerprint authentication system. Jianxin et al. (2001) have described about Projection Incorporated Subspace in their study. The reason that the projection incorporated subspace method is used in this study that it requires fewer eigenvectors. Using less eigenvectors means that less computational power and processing time is needed. PCA is a useful statistical technique that has found application in fields such as fingerprint recognition and image compression and is a common technique for finding patterns in data of high dimension (Andrews et al., 2004). A region merging technique was studied which is the most natural method to overcome the over-segmentation of watersheds transformation by Yu (2004). An alternative solution to the problem is to treat it as a set of potentially inconsistent constraints (Ming Jiang, 2006).

**TEMPLATE PROTECTION OF FINGERPRINT**

Through the common exploitation of biometric identification systems, establishing the legitimacy of biometric data itself has appeared as a significant research issue. The security/integrity issue of biometric data becomes tremendously critical (Anil and Umut, 2003), due to the fact that biometric data is not secret and is not replaceable and merged with the existence of numerous types of attacks that are potential in a biometric system. There has been a lot of research done on mixing dissimilar biometrics for a variety of reasons (Kumar and Zhang, 2006).

Therefore in order to defend biometric information, various sorts of techniques were proposed earlier. Nandakumar et al. (2007) presented a vault hardening scheme consisting of three major steps. Firstly, a random conversion function based on the user password was utilized to the biometric template. Then the fuzzy vault framework protected the transformed template. Lastly, a key derived from the password encrypted the vault. While the fuzzy vault scheme has demonstrated security properties (Juels and Sudan, 2002; Dodis et al., 2004), it has several limitations such as (1) If similar biometric data is reprocessed for making different vaults with different polynomials and random chaff points, the protection of the vault can be compromised (Boult et al., 2007; Scheirer and Boult, 2007). (2) It is achievable for an attacker to develop the non-uniform character of biometric features and expand attacks derived from a statistical study of points in the vault. (3) It is feasible for a challenger to alternate a few points in the vault with his own biometric features, while the number of chaff points in the vault is much bigger than the number of genuine points (Boult et al., 2007; Scheirer and Boult, 2007). (4) The unique template of a valid user is exposed temporarily while it is being authenticated, which may be collected by an attacker.

Qiming et al. (2006) proposed a secure sketch scheme. They discussed how to obtain a reliable cryptographic key from noisy data, for example biometric templates, through the help of several additional information entitled a sketch. Costanzo (2007), has demonstrated the exploitation of biometrics to generate cipher keys, though these approaches characteristically necessitate that an individual accumulate a template of their biometric in either a remote or local database which can be evaluated to future biometric samples. His approach reduces the demand for template storage and exhibits how a cryptographic key can be created during the exercise of biometric feature and parametric aggregation along with convinced mathematical permutation and combination (Costanzo, 2007). Regrettably, even key generation approaches so far
illustrated by Clancy et al. and Linnartz et al. in the literature (Clancy et al., 2003; Linnartz and Tuyls, 2003) involve presigned trial representations, rigorous calculations and more complex systems than their key release equivalents. Sheshab et al. (2005) proposed a hierarchical key generation and distribution scheme that deals with energy, power limitations and sensor network computational. Cavoukian and Stoianov (2007) discussed privacy-enhanced uses of biometrics with meticulous focus on the security and privacy benefits of Biometric Encryption (BE) more than the supplementary uses of biometrics. Scheiner and Boult (2007) proposed a security analysis approach of foremost Privacy Enhanced Technologies (PETs) for biometrics as well as Biometric Fuzzy Vaults (BFV) and Biometric Encryption (BE). Watermarking is one of the modern techniques widely used in protecting templates of fingerprint images. For watermarking, the fingerprint image is used as the base or the cover image and the palmprint features are used as the watermark (Yeung and Pankanti, 2000; Yeung and Mintzer, 1998). Two common methods for cracking a user passkey are dictionary attacks and social engineering techniques (Nandakumar et al., 2007).

Islam et al. (2007c, 2008c) demonstrated a new template protection technique using synthesis of two biometric together by watermarking with fixed digit encryption methods to defend the template information from the attackers on the entire fingerprint authentication system. Hans Georg Schaathun (Schaathun, 2006), presented some attacks in watermarking layer. A real watermarking scheme cannot be anticipated to be infallible. The attacks are: (1) Non-collusive watermarking attack (2) Collusive watermarking attack (3) Cropping a segment. The security of the information transformed is considered by Islam et al. (2008d) against hill-climbing attack (Ross et al., 2007), replay attack (Jain et al., 2005), collusion attack. Hill-climbing attack (Jain et al., 2005) makes use of a replied matching score in order to make a fake. The adversary throws the transformed features to the authentication server for matching. Because the system of Islam et al. (2008d) uses the fixed digit to seek the corresponding data, it is difficult for the adversary to improve the fake from the replied matching score. Therefore, the probability of the adversary’s success on the proposed authentication scheme becomes less than conventional biometric authentication.

OUTCOMES OF SOME MODERN EXPERIMENTS

The outcomes below are shown for different techniques performed on the same database, that is, FVC2004 and because of very few researchers are implemented their techniques using these databases, a few comparative studies are shown in the tables below. Performance evaluations of various techniques are difficult because almost all researchers are obtaining fingerprint data using different sensors with having different type of quality, size and resolutions. Hence, for a review report it’s hard to compare the performances’ outcome of different techniques without performing any experiments. However, a few comparative analyses are shown in this section in order to draw a concept about the modern experiments’ outcome.

Table 1 shows the Equal Error Rates (EER) of different algorithms using the full FVC2004 database (all four datasets) as for the comparative study. The Equal Error Rate marks a system’s operating point at which it incorrectly recognizes genuine users and imposters with equal probability. Different EERs in each database were compared with that of other algorithms of image enhancement, at first the enhancement algorithm by Hartwig et al. (2008) and two more algorithms in FVC2004 light category and at last the enhancement technique by Islam (2009). Among them P103 is the algorithm in FVC2004 which on average obtained the 5th place ranked by EER and P097 ranked 6th in FVC2004 (FVC2004, 2004). All the rows represent Equal Error Rates in case of all impressions being initially enhanced by the method of Hartwig et al. (2008) in the first row, P049 and P009 algorithms in the second and third row respectively and by the approach of Islam (2009) in the last row of Table 1.

From Table 1, the conclusion is reached that it is not self evident that what is perceived as an enhancement actually improves the recognition performance. By contrast, there is a significant risk that it actually can deteriorate the identification performance, especially when the images are of poor quality.

Table 2 shows the percentage of false minutiae detected by different feature extraction algorithms using FVC2004 (FVC2004, 2004) databases. The average results of FA (false minutiae) are compared with that of other

<table>
<thead>
<tr>
<th>Enhancement method</th>
<th>DB1 (%)</th>
<th>DB2 (%)</th>
<th>DB3 (%)</th>
<th>DB4 (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hartwig et al. (2008)</td>
<td>12.00</td>
<td>8.20</td>
<td>5.00</td>
<td>7.00</td>
</tr>
<tr>
<td>P103 (Ranked 5th)</td>
<td>4.18</td>
<td>4.99</td>
<td>5.38</td>
<td>2.78</td>
</tr>
<tr>
<td>P097 (Ranked 9th)</td>
<td>6.10</td>
<td>4.79</td>
<td>5.13</td>
<td>3.43</td>
</tr>
<tr>
<td>Islam (2009)</td>
<td>1.52</td>
<td>2.64</td>
<td>3.74</td>
<td>2.81</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: Comparative analysis in terms of False Minutiae (FA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Methods</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Method A (Mait and Maiton, 1997)</td>
</tr>
<tr>
<td>Method E (Mait and Maiton, 1997)</td>
</tr>
<tr>
<td>Shi and Govindaraju (2006)</td>
</tr>
<tr>
<td>Islam (2009)</td>
</tr>
</tbody>
</table>
algorithms of feature extraction, one is the chaincode
based feature extraction algorithm by Shi and Govindaraju
(2006) and two more methods reported in Maio and
Maltoni (1997) and lastly, synthesis biometric based
feature extraction by Islam (2009). According to Shi and
Govindaraju (2006) the false minutiae are detected mostly
due to binarization of the difficult local area where a ridge
is broken by noise or low image contrast. In contrast the
approach presented by Islam (2009), has the ability to
solve ridge broken problems through region merging
algorithm technique that is used to remove imperfect reconstruction
problems after synthesis. The 1st and 2nd row includes
results of the two Methods A and E reported in Maio and
Maltoni (1997) for comparison where false minutiae are
determined due to the irregularity of the binary traces
produced by the binarization process. The evaluation
shows the supremacy of the proposed technique in terms of
efficiency and robustness.

Table 3 presents the comparative risk analyses of
several template security approaches. In Table 3 the tick
(\(\checkmark\)) indicates that the template protection approach has
the possible risk of that particular attack and the cross (\(\times\))
indicates that the approach has the capability to protect
the template from that particular attack.

The security of the information transformed is
considered by Islam (2009) against hill-climbing attack
(Ross et al., 2007), replay attack (Jain et al., 2005),
collision attack is now considered. Hill-climbing attack
(Jain et al., 2005) makes use of a replied matching score
in order to make a fake. While the application server sends
the matching score to client or adversary, the adversary transforms embedded feature data selected
from database that the adversary constructs. The adversary
throws the transformed features to the authentication server for matching.

**CONCLUSION**

Because of the fingerprint images acquired by a
variety of sensors were different kinds of quality
such as low resolution and sometimes of very poor
quality images, hence numerous approaches were used.

To estimate the performance of several approaches
different researchers have used different methods for the
experiments. Global features matching, local features
matching, graph based matching are utilized and the
performances are evaluated by the False Acceptance Rate
(FAR), False Rejection Rate (FRR) and Equal Error Rate
(EER). And the outcome of the matching performance of
the authentication varies on the use of different
enhancement technique along with the quality of images
which are gained by using different types of sensors.
Hence, comparing the performance of various techniques
may be possible in terms of the values of FAR, FRR, EER
and the database as well as the matching technique
should be same. It can be performed two types of
evaluation of the image enhancement technique. Those are qualitative and/or qualitative
comparison. Therefore, performance evaluation for the
image enhancement, feature extraction and template
protection technique depends on the quality of the
fingerprint image as well as the types of sensors/scanners
by which fingerprint images are being taken, performance
of matching techniques depending on the different feature
information (delta, core, minutiae) of the fingerprint, that
is, which matching technique is providing better
performances on which feature of fingerprint image.

**REFERENCES**

Single trial source separation of VEP signals using
selective principal components. Proceedings of the
2nd International Conference on Advances in
Medical Signal and Information Processing, Sept. 5-8,


Arcelli, C. and G. S.D. Baja, 1984. A width independent fast
Intell., 7: 463-474.

warping using ridge curve correspandences. IEEE


