Journal of Applied Sciences 10 (14): 1397-1404, 2010
ISSN 1812-5654

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 MOC (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

Corresponding Author: Md. Rajibul Islam, Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia Tel: +60162489860

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 effectual 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 JaJa (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 re-sampling 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 Kovesi (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 Arcelli and Baja (1984), used matrices of 3×3 pixels to search for typical minutiae, that is, ridge endings 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 marging 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 prealigned trial representations, rigorous calculations and more complex systems than their key release equivalents. Shehab *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. Scheirer 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 1: EERs on the FVC2004 database, for different enhancement methods

	FVC2004 (%)			
Enhancement method	DB1	DB2	DB3	DB4
Hartwig *et al.* (2008)	12.00	8.20	5.00	7.00
P 103 (Ranked 5th)	4.18	4.99	5.38	2.78
P 097 (Ranked 6th)	6.10	4.79	5.13	3.43
Islam (2009)	1.52	2.64	3.74	2.81

Table 2: Comparative analysis in terms of False Minutiae (FA)

Methods	Percentage of FA
Method A (Maio and Maltoni, 1997)	8.52
Method E (Maio and Maltoni, 1997)	22.56
Shi and Govindaraju (2006)	38.67
Islam (2009)	0.31

Table 3: Comparative analyses based on numerous attacks: (v) indicates the risk of attacks and (×) denotes no risk of attacks

Attacks	Spoofing attack	Replay attack	Substitution	Tampering	Masquerade attack	Trojan horse attacks	Overriding Yes/No response	Privacy issue
Template Security Approaches								
Encryption (Soutar *et al*., 1999)	v	v	×	v	v	v	×	×
Non-invertible transform	×	×	×	×	×	×	v	v
Hardening/Salting (Teoh *et al*., 2006)	v	v	×	×	×	×	×	×
Key generation (Sun *et al*., 2007)	v	v	×	×	×	×	×	v
Secure sketch (Sutcu *et al*., 2007)	×	×	×	v	×	v	×	×
Hardened fuzzy vault (Nandakumar *et al*., 2007)	v	v	×	×	×	×	×	×
Islam (2009)	×	×	×	×	×	×	×	×

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 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 (v) indicates that the template protection approach has the possible risk of that particular attack and the cross (×) 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), collusion 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 various types 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 can 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 performance 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

Andrews, S., R. Palaniappan and V.S. Asirvadam, 2004. 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, Philadelphia, PA, USA., pp: 51-57.

Anil, K.J. and U. Umut, 2003. Hiding biometric data. IEEE Trans. Pattern Anal. Mach. Intell., 25: 1494-1498.

Arcelli, C. and G.S.D. Baja, 1984. A width independent fast thinning algorithm. IEEE Trans. Pattern Anal. Mach. Intell., 7: 463-474.

Arun, R., S.C. Dass and K.J. Anil, 2006. Fingerprint warping using ridge curve correspondences. IEEE Trans. Pattern Anal. Mach. Intell., 28: 19-30.

Bader, D.A., J. JaJa, D. Harwood and L.S. Davis, 1995. Parallel algorithms for image enhancement and segmentation by region growing with an experimental study. Tech. Rep., CS-TR-3449: 25-25.

Bader, D.A. and J. JaJa, 1996. Practical parallel algorithms for dynamic data redistribution, median finding and selection. Proceedings of the 10th International Parallel Processing Symposium, April 15-19, Departnement of Electronic Eng., Maryland University, College Park, MD, pp: 292-301.

Bamberger, R.H., 1990. The directional filter bank: A multirate filterbank for the directional decomposition of images. Ph.D. Thesis, Georgia Institute of Technology, Georgia.

Bamberger, R.H. and M.J.T. Smith, 1992. A filter bank for the directional decomposition of images: Theory and design. IEEE Trans. Signal Process., 40: 882-893.

Bella, G., S. Bistarelli and F. Martinelli, 2003. Biometrics to enhance smartcard security: Simulating MOC using TOC. Proceedings of the 11th International Workshop on Security Protocols, LNCS 3364, April 2003, Springer, Cambridge, UK., pp: 324-335.

Boult, T.E., W.J. Scheirer and R. Woodworth, 2007. Fingerprint revocable biotokens: Accuracy and security analysis. Proceedings of the CVPR, June 17-22, Minneapolis, MN, pp: 1-8.

Cavoukian, A. and A. Stoianov, 2007. Biometric encryption: A positive-sum technology that achieves strong. Technical Report, Information and Privacy Commissioner, Ontario, March 2007.

Clancy, T.C., N. Kiyavash and D.J. Lin, 2003. Secure smartcard-based fingerprint authentication. Proceedings of the ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications, March 2007, Berkley, California, pp: 45-52.

Costanzo, C.R., 2007. Active Biometric Cryptography (ABC): Key generation using feature and parametric aggregation. Proceedings of the 2nd International Conference on Internet Monitoring and Protection, July 1-5, San Jose, California, pp: 28-28.

Dijk, J. and P.W. Verbeek, 2006. Lightness filtering in color images with respect to the gamut. Proceedings of 3rd European Conference on Colour in Graphics, Imaging, and Vision, June 19-22, University of Leeds, UK., pp: 330-335.

Dodis, Y., L. Reyzin and A. Smith, 2004. Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data. Adv. Cryptol. EUROCRYPT, 3027: 523-540.

Emiko S., M. Takuji, N. Takahiro, S. Masahiro, S. Koji, M. Masahito and S. Koichi, 2006. Fingerprint authentication using optical characteristics in a finger. Proceedings of theSICE-ICASE International Joint Conference, Oct. 18-21, Bexco, Busan, Korea, pp: 1774-1777.

FVC2004, 2004. Fingerprint verification competition: Fingerprint database. http://bias.csr.unibo.it/fvc2004/Downloads/fvc2004cfp.pdf.

Farid, A. and I.S. Moskowitz, 2005. Composite signature based watermarking for fingerprint authentication. Proceedings of the 7th Workshop on Multimedia and Security, (WMS'05), New York, USA., pp: 137-142.

Florian, K., J.A. Mekhail, D. M'Raihi and J.R. Rice, 2004. Private fingerprint verification without local storage. Lecture Notes Computer Sci., 3072: 387-394.

Gonzalez, R.C. and R.E. Woods, 2002. Digital Image Processing. Pearson Education Inc., Upper Saddle River, NJ.

Hartwig, F., K. Klaus and B. Josef, 2008. Local features for enhancement and minutiae extraction in fingerprints. IEEE Trans. Image Process., 17: 354-363.

Hong, L., Y. Wan and A. Jain, 1998. Fingerprint image enhancement: Algorithm and performance evaluation, pattern analysis and machine intelligence. IEEE Trans. Pattern Anal. Mach. Intell., 20: 777-789.

Islam, M.R., M.S. Sayeed and A. Samraj, 2007a. Precise fingerprint enrolment through projection incorporated subspace based on Principal Component Analysis (PCA). Proceedings of the 2nd International Conference on Informatics, (ICI'07), Kuala Lumpur, Malaysia, T1, pp: 85-91.

Islam, M.R., M.S. Sayeed and A. Samraj, 2007b. Multimodality to improve security and privacy in fingerprint authentication system. Proceedings of International Conference on Intelligent and Advanced Systems, (ICIAS'07), Kuala Lumpur, Malaysia, pp: 753-757.

Islam, M.R., M.S. Sayeed and A. Samraj, 2007c. Webcam based fingerprint authentication for personal identification system. Int. J. Coll. Sci. India, 1: 19-29.

Islam, M.R., M.S. Sayeed and A. Samraj, 2008a. Biometric template protection using watermarking with hidden password encryption. Proceedings of the International Symposium on Information Technology 2008 (ITSIM), (ISIT'08), Kuala Lumpur, Malaysia, pp: 296-303.

Islam, M.R., M.S. Sayeed and A. Samraj, 2008b. Fingerprint authentication system using a low-priced webcam. Proceedings of the International Conference on Data Management, (ICDM'08), IMT Ghaziabad, India, pp: 689-697.

Islam, M.R., M.S. Sayeed and A. Samraj, 2008c. A secured fingerprint authentication system. J. Applied Sci., 8: 2939-2948.

Islam, M.R., M.S. Sayeed and A. Samraj, 2008d. Fingerprint synthesis toward construct enhanced authentication system using low resolution webcam. Proceedings of the International Conference on Data Managemen, (ICDM'08), IMT Ghaziabad, India, pp: 679-688.

Islam, M.R., 2009. Fingerprint identification and verification with secure technology. M.Sc. Thesis, Multimedia University, Malaysia.

Jain, A.K., 1989. Fundamentals of Digital Image Processing. Prentice Hall, Englewood Cliffs, NJ., USA., ISBN-10: 0133361659.

Jain, K., A. Ross and U. Uludag, 2005. Biometric template security: Challenges and solutions. Proceeding of 13th European Signal Processing Conference, Sept. 05, Turkey, pp: 1-4.

Jain, L.C., U. Halici, I. Hayashi, S.B. Lee and S. Tsutsui, 1999. Intelligent Biometric Techniques in Fingerprint and Face Recognition. The CRC Press, Boca Raton, Florida, USA.

Jia, J. and L. Cai, 2005. A TSVM-based minutiae matching approach for fingerprint verification. Lecture Notes Comput. Sci., 3781: 85-94.

Jianxin, W., C. Zhaoqian and Z. Zhihua, 2001. Projection incorporated subspace method for face recognition. Proc. 6th Int. Conf. Yong Comput. Sci., 2: 962-965.

Juels, A. and M. Sudan, 2002. A fuzzy vault scheme. Proceedings of the IEEE International Symposium on Information Theory, (IISIT'02), University of Lausanne, Switzerland, pp: 408-408.

Kang, H., B. Lee, H. Kim, D. Shin and J. Kim, 2003. A study on performance evaluation of fingerprint sensors. Proceedings of the 4th International Conference Audio- and Video-based Biometric Person Authentication, June 9–11, Guildford, UK, pp: 574-583.

Kovesi, P.D., 2000. MATLAB and octave functions for computer vision and image processing. Retrieved December 19, 2006, from http://www.csse.uwa.edu.au/~pk/Research/MatlabFns/index.html.

Kumar, A. and D. Zhang, 2006. Combining fingerprint, palmprint and hand-shape for user authentication. Proceedings Int. Conf. Pattern Recognition, 4: 549-552.

Linnartz, J. and P. Tuyls, 2003. New shielding functions to enhance privacy and prevent misuse of biometric templates. Proceedings of the 4th International Conference on Audio and Video Based Person Authentication, June 9-11, Guildford, United Kingdom, pp: 393-402.

Maio, D. and D. Maltoni, 1997. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. Mach. Intelligenc, 19: 27-40.

Maio, D., D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, 2004. FVC2004: Third fingerprint verification competition. Proceedings of the International Conference on Biometrics Authentication (ICBA), July 2004, Hong Kong, pp: 1-7.

Maltoni, D., D. Maio, A.K. Jain and S. Prabhakar, 2003. Handbook of Fingerprint Recognition. Springer, New York, pp: 348..

Ming Jiang, 2006. Digital image processing. http://iria.pku.edu.cn/~jiangm/courses/DIP/index.html.

Mohamed Mostafa, A.A., 2005. A novel line pattern algorithm for embedded fingerprint authentication system. ICGST Int. J. GVIP, 5: 29-35.

Moon, D., Y.H. Gill, S.B. Pan and Y. Chung, 2003. Implementation of the USB token system for fingerprint verification. Proc. SCIA LNCS, 2749: 998-1105.

Nandakumar, K., A. Nagar and A.K. Jain, 2007. Hardening fingerprint fuzzy vault using password. Adv. Biometrics, 4642: 927-937.

Park, S.I., 1999. New directional filter banks and their applications in image processing. Ph.D. Thesis, Georgia Institute of Technology, Atlanta, Georgia.

Patrick, S., H. David and V. Ingrid, 2005. Platform-based design for an embedded-fingerprint-authentication device. IEEE Trans. Comput. Aided Design Integrated Circuits Syst., 24: 1929-1936.

Qiming, Li, Y. Sutcu and D.M. Nasir, 2006. Secure sketch for biometric templates. Lecture Notes Comput. Sci., 4284: 99-113.

Ratha, N.K., S.Y. Chen and A.K. Jain, 1995. Adaptive flow orientation-based feature extraction in fingerprint image. Pattern Recognition, 28: 1657-1672.

Ravishankar, R.A., 1994. A Taxonomy of Texture Descriptions. Springer-Verlager, Heidelberg.

Ross, A., J. Shah and A. Jain, 2007. From template to image: Reconstructing fingerprints from minutiae points. IEEE Trans. Pattern Anal. Mach. Translation, 29: 544-560.

Sanchez-Reillo, R., J. Liu-Jimenez and L. Entera, 2004. Architectures for biometrics match-on-token solutions. Biometric Authentication, 3087: 195-204.

Schaathun, H.G., 2006. On watermarking/fingerprinting for copyright protection. Proceedings of 1st International Conference on Innovative Computing, Information and Control, Sept. 5-7, IEEE Computer Society, USA., pp: 50-53.

Scheirer, W.J. and T.E. Boult, 2007. Cracking fuzzy vaults and biometric encryption. Proceedings of the Biometrics Symposium, (BS'07), Baltimore, MD, pp: 1-6.

Seow, B.C., S.K. Yeoh, S.L. Lai and N.A. Abu, 2002. Image based fingerprint verification. Proceedings of the Student Conference on Research and Development Proceedings, (SCORD'02), Malaysia, pp: 58-61.

Shapiro, L.G. and G.C. Stockman, 2000. Computer Vision. Prentice Hall, Upper Saddle River, NJ.

Shehab, M., E. Bertino and A. Ghafoor, 2005. Efficient hierarchical key generation and key diffusion for sensor networks. Proceedings of the 2nd Annual IEEE Communications Society Conference on Sensor and AdHoc Communications and Networks, IEEE SECON, (ACSCSACN'05), School of Electrical and Computer Engineering, USA., pp: 76-84.

Sherlock, B.G., D.M. Monro and K. Millard, 1994. Fingerprint enhancement by directional Fourier filtering. IEEE Proc. Vis. Image Signal Process, 141: 87-94.

Shi, Z. and V. Govindaraju, 2006. A chaincode based scheme for fingerprint feature extraction. Pattern Recog. Lett., 27: 462-468.

Soutar, C., D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, 1999. Biometric Encryption. In: Bioscrypt Inc. ICSA Guide to Cryptography, Randall, K. (Eds.). Nichols, McGraw-Hill, New York.

Sun, S.W., C.S. Lu and P.C. Chang, 2007. Biometric template protection: A key-mixed template approach. Proceeding IEEE International Conference Consumer Electronics 2007, Jan. 10-14, Las Vegas, NV, pp: 1-2.

Sutcu, Y., Q. Li and N. Memon, 2007. Protecting biometric templates with sketch: Theory and practice. IEEE Trans. Inform. Forensics Security, 2: 503-512.

Teoh, A.B.J., A. Goh and D.C.L. Ngo, 2006. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans. PAMI, 28: 1892-1901.

Wang, S., W.W. Zhang and Y.S. Wang, 2002. Fingerprint classification by directional fields. Proceedings of the 4th IEEE International Conference on Multimodal Interfaces, Jan. 22, Pittsburgh, PA, USA., pp: 395-399.

Watson, C.I., G.T. Candela and P.J. Grother, 1994. Comparison of FFT fingerprint filtering methods for neural network classification. (Tech. Rep. No. NISTIR, 5493). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.6226.

Westman, T., D. Harwood, T. Laitinen and M. Pietikainen, 1990. Color segmentation by hierarchical connected components analysis with image enhancement by symmetric neighborhood filters. Proceedings of the 10th International Conference on Pattern Recognition, Jun. 16-21, Atlantic City, NJ, pp: 796-802.

Wu, C., Z. Shi and V. Govindaraju, 2004. Fingerprint image enhancement method using directional median filter. Proc. SPIE, 5404: 66-75.

Yeung, M. and F.C. Mintzer, 1998. Invisible watermarking for image verification. J. Elect. Imaging, 7: 578-591.

Yeung, M. and S. Pankanti, 2000. Verification watermarks on fingerprint recognition and retrieval. J. Elect. Imaging, 9: 468-476.

Yu, H.G., 2004. Morphological image segmentation for co-aligned multiple images using watersheds transformation. M.Sc. Thesis, Department of Electrical and Computer Engineering, The Florida State University.

Zhang, T.Y. and C.Y. Suen, 1984. A fast parallel algorithm for thinning digital patterns. Commun. ACM, 27: 236-239.