ISSN : 2231-0711

A Survey on Approaches to Improve Quality of Fingerprint Image and Template Security

JANANI.B
Research scholar
PSGR krishnammal college for women
Coimbatore

DR. N. RADHA
Assistant professor
PSGR Krishnammal College for women
Coimbatore

Abstract-A biometric is a distinct biological trait that can be used to recognize a person. Fingerprints have been used for over a century and are the most widely used for user identification. Fingerprint identification is commonly employed in Forensic science to support criminal investigations and in biometric systems such as civilian and commercial identification devices.Fingerprint is the pattern of ridges and valley on the inner surface of a finger or a thumb. The low quality fingerprint imagesused for feature extraction and matching will not produce efficient results. To deal with this various methods for enhancing low-quality fingerprints images are discussed. In addition to enhancement, the storage of fingerprint template is also an important issue. Because when the hacker steels the template from the database, it can be misused. To avoid this problem, various template security techniques are surveyed.In this paper various image quality enhancement techniques and template security techniques are reviewed in the literature.

INTRODUCTION

Biometric systems automatically determine or verify a person's identity based on his anatomical and behavioral characteristics such as fingerprint, palmprint, vein pattern, finger knuckles, face, Iris, voice and gait. Biometric trait, called the feature set is unique for each and every person. The feature set obtained during enrolment is stored in the system database as a template.

One of the momentous issues in biometric systems is protecting the template of a user which is usually stored in a database or a smart card. Stolen biometric templates can be used to compromise the security of the system in the following two ways: (i) The stolen template can be replayed to the matcher to gain unauthorized access, and (ii) A physical spoof can be created from the template to gain unauthorized access to the system. An attacker can furtively acquire the biometric information of a genuine user. Hence, spoof attacks are possible even when the attacker does not have access to the biometric template. However, the attacker needs to be in the physical nearness of the person he is attempting to impersonate in order to stealthily acquire his biometric trait. On the other hand, even a remote attacker can create a physical spoof if he gets access to the biometric template information. Unlike passwords, when biometric templates are compromised, it is not possible for a genuine user to revoke his biometric identifiers and switch to another set of uncompromised identifiers. Due to this irretrievable nature of biometric data, an attack against the stored templates constitutes a major security and privacy peril in a biometric system. Since a biometric trait is an everlasting link between a person and his identity, it can be easily prone to abuse in such a way that a person's right to privacy and secrecy is compromised. Hence, strategies to protect biometric template and to ensure an individual's privacy are urgently needed.

Human experts routinely use the context information of fingerprint images, such as ridge continuity and regularity to help in identifying them. This means that the underlying morphogenetic process that produced the ridges does not allow for irregular breaks in the ridges except at ridge endings. Because of the regularity and continuity properties of the fingerprint image, occluded and corrupted regions can be recovered using the contextual information from the surrounding area. Such regions are regarded as "recoverable" regions. The efficiency of an automated enhancement algorithm depends on the extent to which they utilize the contextual information. The following literature describes several enhancement methods for fingerprint images.

LITERATURE SURVEY

FINGERPRINT ENHANCEMENT

Novel Adaptive Approach

Tahmasebi and Kasaei [1] presented a novel Adaptive Approach for fingerprint enhancement filter design. To improve the efficiency of the enhancement process, the designed filter adapts itself to the characteristics of input images. Moreover, the filter parameters are automatically calculated with no need of any predetermined parameters. Different filter masks are adapted for different image scales to improve the efficiency of the enhancement process. The algorithm is fast and the required computational load is negligible.

Chain code image representation

Zhixin Shi and VenuGovindaraju[2] presented a novel use of chain code image representation in fingerprint image enhancement and minutiae extraction. The chaincode representation allows efficient image quality enhancement and detection of fine minutiae feature points. For image enchantment binarization algorithm is used binarized after a quick averaging to generate its chaincode representation. The direction field is estimated from a set of selected chaincodes. The original gray-scale image is then enhanced by a filtering algorithm. The minutiae are detected using a sophisticated ridge contour following procedure.

Short Time Fourier Transform (STFT) Analysis

Sharat et.al [3] presented new approach for fingerprint enhancement based on Short Time Fourier Transform(STFT) Analysis.The algorithm simultaneously estimates all the intrinsic properties of the fingerprints such as the foreground region mask, local ridge orientation and local frequency orientation. Furthermore these propose a probabilistic approach of robustly estimating these parameters. The enhancement utilizes the full contextual information (orientation, frequency, angular coherence) for enhancement.

Low-Quality fingerprint enhancement

Ju Cheng Yang et al [4] presented a novel algorithm for low-quality fingerprint enhancement in spatial domain. This method enhances ridges with a mixture of local normalization and ridge compensation filter in which this filter uses orientation of ridges. This method efficiently enhances the contrast among valleys and ridges of low-quality fingerprint images. In addition it restores the important ridge structures by improving the pixels on ridges and weakens the non-ridge pixels during ridge orientation.

TEMPLATE SECURITY

Alignment-Free Cancelable Fingerprint Templates

Chulhan Lee et.al [5] presented a method for generating cancelable fingerprint templates that do not necessitate alignment and a method for making changing functions. Cancellable templates of fingerprints are generated by extracting translation and rotation invariant value for each minutia. Then movement for the translation and orientation of each minutia are calculated by using two changing functions.Each minutia is rotated and moved by the transformed total of movement by means of the orientation of a minutia as the reference direction. Once an ideal invariant value is extracted, the same minutia yields the same invariant values even if fingerprint images are changed. During that situation, the method does not corrupt performance because the geometric relationships between the original fingerprint templates are sealed in the transformed fingerprint templates.

Reliable fuzzy vault System

YounJoo Lee et. al [6] presented reliable fuzzy vault system that was based on iris data. One drawback of conventional fuzzy vault systems was that they did not have good performance because of intra variations of input biometric data. To reduce the intra variations of input iris images,pattern-clustering technique and local shift-matching method are used. Multiple iris features are extracted from multiple local iris patches to produce an unordered set. The result achieved improved the performance without requiring pre alignment and retained high security levels in terms of private keys and iris templates.

Bit-String Cancelable fingerprint templates

Chulhan Lee and JaihieKim [7] presented new technique for template security based on cancellable biomertic fingerprint. It transforms original biometric templates in a bit-string. The alignments are not necessary for transformation. One drawback the performance was ideal when each user had a different PIN and the two templates from the same fingerprint were not matched when the corresponding PINs were different.

Symmetric Hash Functions for Fingerprint minutia

Tulyakov et. al [8] proposed a hash-based transformation method. For each minutia, the N nearest neighbour minutiae was found and M (MoN) hashed minutiae were generated using symmetric hash functions. The hashed minutiae were then stored in a database and compared to the query hashed minutiae. Unlike common hash functions, these hash functions showed good biometric properties .In the hash space, these researchers discovered the geometric relationship between the query and the enrolled fingerprint. However, they did not describe how the newly hashed minutiae could be generated when stored minutiae were compromised.

S.NO	AUTHOR	TECHNIQUES	MERITS	DE-MERITS
1.	A. M. Tahmasebi and S. Kasaei-2002	Novel Adaptive Approach	Performs fast and less computational load	Improvements in the quality of directional image affect the performance of enhancement process
2	Zhixin Shi &Venu Govindaraju-2006	Chain code image representation	Better enhancement of fingerprint is achieved	Better processing for the binarization is needed. Added minutiae and exchanged minutiae due to attached noise
3	Sharat S. Chikkerur, Alexander N. Cartwright and Venu Govindaraju-2007	Short Time Fourier Transform (STFT) Analysis	Enhancement utilizes the full contextual information, Requires reduced space requirements,	Robust orientation smoothening is not done for fingerprint enhancement
4	J. C. Yang, D. S. Park, and R. Hitchcock-2008	low-quality fingerprints image enhancement	Better enhancement is achieved for low-quality images	Improved accuracy is not obtained
5	Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh, Sangyoun Lee, and Jaihie Kim-2007	Alignment-Free Cancelable Fingerprint Templates	Controls the performance and changeability of the changing function	Occurrence of errors while obtaining invariant values. Degrades the performance because false accept rate increases from the disclosed PIN.
6	YounJoo Lee, Kang Ryoung Park, Sung Joo Lee, KwanghyukBae, and Jaihie Kim- 2008	Reliable fuzzy vault System	Doesn't require pre alignment, Retains high security levels of template	Lacks in performance because of occlusion problem, Storage space is occupied for a more than one encryption method
7	Chulhan Lee and JaihieKim	Cancelable biometric fingerprint	Doesn't require alignment, it retains bit-string	Occurrence of error due to alignment are reduces the time of performance.
8	Tulyakov et. al	Hash function	Performed by generating nearest neighbour minutia.	Doesn't shows significant performance for low-quality images

CONCLUSION

The present work surveyed various methods for enhancing low-quality fingerprints and generating secured biometric templates. Methods for enhancing low-quality fingerprint such as Novel Adaptive Approach, Chain code image representation, Short Time Fourier Transform (STFT) Analysis and a novel approach for enhancing fingerprint in spatial domain. The methods for achieving secured biometric templates are done by Alignment-Free Cancellable Fingerprint Templates, Reliable fuzzy vault System, cancellable biometric and hash function for Template Security approach. Future work is to improve the quality of the fingerprint and store the templates in secure format using one way hash function, through cancellable Bio Hashing. Comprise table is generated for surveyed methods which shows merits and performs better in one scenario and limitation occurs in various aspects.

REFERENCE

[1] A. M. Tahmasebi and S. Kasaei, “A novel adaptive approach to fingerprint enhancement filter design,” Signal Processing, Image Communication., vol. 17, no. 10, pp. 849–855, 2002.

[2] Z. Shi and V. Govindaraju, “A chaincode based scheme for fingerprint feature extraction,” Pattern Recognition., vol. 27, no. 5, pp. 462–468, 2006.

[3] S. Chikkerur, A. N. Cartwright, and V. Govindaraju, “Fingerprint enhancement using STFT analysis,” Pattern Recognition., vol. 40, no. 1, pp. 198–211, 2007.

[4] J. C. Yang, D. S. Park, and R. Hitchcock, “Effective enhancement of low-quality fingerprints with local ridge compensation,” IEICE Electron. Exp., vol. 5, no. 23, pp. 1002–1009, 2008.

[5] C. Lee, J. Y. Choi, K. A. Toh, S. Lee, and J. Kim, “Alignment-free cancelable fingerprint templates based on local minutiae information,” IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 37, no. 4, pp. 980–992, Aug. 2007.

[6] YounJoo Lee, Kang Ryoung Park, Sung Joo Lee, KwanghyukBae, and Jaihie Kim,”A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System”,IEEE transactions on systems, man, and cybernetics: cybernetics, vol. 38, no. 5, october 2008

[7] Chulhan Lee and JaihieKim , “Cancelable fingerprint templates using minutiae-based bit-strings” Journal of Network and Computer Applications 33 pp.236–246, 2010.

[8] Tulyakov S, Chavan VS, Govindaraju V. Symmetric hash functions for fingerprint minutiae. In: International workshop on pattern recognition for crime prevention, security and surveillance, Bath, UK, 2005.

[9] Gonzalez, woods, and Eddins, “Digital image processing “,Prentice hall,2004.

[10] X. Jiang and W. Yau, “Fingerprint minutiae matching based on the local anf global structure”, in Proc. 15th Int. Conf. Pattern Recong., 2000, vol. 2, pp. 1042-1045.

[11] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, “BioHashing: Two factor authentication featuring fingerprint data and tokenised random number”, pattern Recognition, vol. 37, no. 11, pp.2245-2255, nov.2004.

[12] A. B. J. Teoh, D. C. L. Ngo, “Cancellable biometric featuring with tokenized random number”, Pattern Recognition. Lett., vol.26, no. 10.pp. 1454-1460, jul.2005.

[13] A. Teoh, Y. Kuan, S Lee. Cancellable biometrics and annotations on BioHash. Pattern recognition,2007.

[14] J. C. Yang, D. S. Park, and R. Hitcock, “Effective enhancement of low-quality fingerprint with local ridge compensation”, IEICE Electron. Exp., vol. 5, no.23, pp. 1002-1009,2008.