International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON FINGERPRINT PROTECTION TECHNIQUES

Austin J Gladston, Miss Ashitha S S.

Dept of Computer Science and Engineering
Lourdes Matha College Of Science And Technology
Kuttichal,Trivandrum

Abstract— *Fingerprint recognition systems are commonly used for authentication purposes. The traditional authentication techniques like passwords, tokens, smart cards are vulnerable to attacks. The fingerprints are biological features of a man which is unique. So protection of fingerprints for authentication purposes is important. The privacy of fingerprints can be protected by traditional methods like password, encryption and transformation techniques .Automated finger print matching techniques are used for verification purposes. Most of the matching techniques use minutiae features. The performance of the minutiae extraction depends on the quality of the image. Enhancement algorithms are used to improve the goodness index and verification accuracy of minutiae. Reconstruction of minutiae representation is used for finger print matching systems. The features of two fingerprints can be mixed to generate a new identity. The minutiae points or orientation features of two fingers can be combined together. Some techniques use gradient calculation method to find the reference point from the minutiae.*

Keywords:*Fingerprint,Minutiae,Fingerprint enhancement ,Privacy protection*

1.INTRODUCTION

Fingerprint Recognition Systems are considered as one of identification systems with confidence. Commonly used features are ridge orientation, ridge bifurcation,ridge contour,position etc.Feng and Jain [1] proposed a reconstruction algorithm to reconstruct plain and rolled fingerprints. Such systems are used in recognition systems where same finger is enrolled with different impression. In this method a fingerprint image is represented as a 2D amplitude and frequency modulated signal. The phase is calculated using the steps like orientation field reconstruction, estimation of gradient of continuous phase, continuous phase reconstruction, combination of spiral phase and the continuous phase. The local ridge orientation of each 8*8 block is calculated using nearest minutia in each of the eight sectors. The singular points in the finger print are handled using enhanced techniques to avoid shift of singularity. The reconstructed fingerprints are found to be almost same as original one.

The gradient of continuous phase at each block is obtained from the gradients of composite phase and spiral phase. To avoid discontinuity problems the initial orientation field is unwrapped. To unwrap fingerprints without singularity, depth-first,breadth-first or other techniques are used. A third order polynomial is commonly used to calculate the gradient. Then function is applied to gradient to obtain the explicit function of continuous phase. The reconstructed fingerprint are very smooth without any spurious minutiae.

In [2], the application of fuzzy vault for fingerprints is used. But a single finger never contains sufficient information for secure implementation's minutiae data of several finger prints are used to improve security. The stored minutiae are hidden as a set of chaff points. A polynomial is used to encode the biometric data.The query is changed as a set of attributes, which is compared with the stored fuzzy vault using Reed-Solomon decoding.

This fuzzy vault technique is error tolerant. To improve the correctness of the recovered

polynomial, a hash value of polynomial's coefficient is used. The minutiae of all fingers are stored as a feature vector in encoded form. To get optimized result a restriction is placed on the area of finger print. Only reliable fingerprints minutiae feature vectors are allowed to be inserted into the data base. The minimum Euclidean distance from genuine minutiae to the chaff points are considered during retrieval process. The pre-alignment algorithm scales down the fingerprint image and uses a threshold on pixel brightness to obtain the image displaying the shape of fingerprint. The cross matching of the vaults from several independent enrollments of a user remains as a serious threat to fuzzy vault.

Another approach for fingerprint protection is combining the features of two fingerprints[3].The minutiae features of one finger is combined with the orientation features of another finger to create a new identity. Reference detection helps to locate a reference point with maximum certainty value. The range of minutiae direction is from 0 to 360.A query minutiae determination and finger print matching score is used for image retrieval process. So attackers cannot recover the original minutiae template from combined minutiae fingerprints.

The performance of minutiae extraction information relies on quality of images [4].So image enhancement algorithms are used along with minutiae extraction modules. This helps to improve the clarity of ridges. Experimentally it is proven in this work that enhancement algorithms improve the goodness index. Most of the poor quality images may create significant number of spurious minutiae. Some of the significant minutiae may be ignored. The region of interest in fingerprint images can be divided as well defined regions, recoverable corrupted region and unrecoverable corrupted region.

The major steps of image enhancement algorithm used in [4] are normalization, local orientation, local frequency estimation, region mask estimation and filtering. The normalization helps to reduce variations in the grey level values along the ridges. A smoothed orientation field for each 16*16 block is estimated. The local ridge frequency estimation is an intrinsic property of image.For a fingerprint at a fixed resolution, the value of the frequency of ridges and furrows in a local neighborhood lies in a particular range [1/3,1/25].The fingerprints may be recoverable or unrecoverable regions. Assessment of shape based on amplitude, frequency and variance are used to classify the pixels into regions using squared error clustering algorithm. If the percentage of recovered regions is above a threshold, the input fingerprint image will be accepted. Gabor filters are used to remove noise from the inputted image. The goodness index (GI) is used to measure the quality of the extracted minutiae.

Handwritten signature images are used to secure private cryptographic keys. The first OSFV implementation uses a machine learning approach to select reliable feature representation [5]. Enhanced methods of this system are used to improve accuracy and security. The new method with key size adaptation achieves good performance. This system consists of two subsystems-enrollment and authentication. The enrollment phase is used to collect signature templates. The user representation matrix,UR consists of the vectors of feature information. This information is used for the authentication phase. The user representation matrix UR is encrypted by means of user password PW.Both FV and password are stored as a part of user bio-cryptography template(BCT).The user parameters FI and VI are used to lock the user cryptography key K by means of a single signature template T_S in a fuzzy vault FV.

The authentication subsystem uses the user query sample Q and the password PW.This helps to decode the fuzzy vault FV and restore the user cryptography key K.The password PW is used to decrypt the UR matrix.The vectors F1, V1 and Δ are used to decode the FV.

The OSFV based digital signature techniques are used for the automation of business processes.

The user signs the document, by hand. The handwritten signature image is used to unlock his private key. The unlocked key produces a digital signature by encrypting some message extracted from document. The encrypted message is considered as a digital signature and it is attached to the digital document. Any person with the user public key can verify the digital signature.

For performance improvement, the global features are represented once enough no:of enrolled samples becomes available. Multi-scale feature fusion method seems to be useful where different feature vectors are extracted based on different extraction scales. Fusing multiple feature types also increase the FV decoding accuracy. The margin between intra and interclasees of regions seems to differ when using different signature prototypes for FV encoding.

The accuracy of OSFV system relies on the quality of features used. Additional variants like adaptive matching, ensembling of fuzzy vaults, using additional passwords and cascading with traditional SV modules are used to improve accuracy.

Adaptive chaff generation and adaptive key size approaches are used to improve the security features. Several offline signature based FV implementation works are analyzed in this work. But the novel method to adapt cryptography key sizes for different users has shown good accuracy and security values. For forgery detection, better techniques with intelligence are needed.

Automatic fingerprint matching technique helps to automatically extract minutiae from images. The performance of the algorithm depends on the quality of images. Because of the variations in impression conditions, ridge configurations, skin condition and acquisition devices, the acquired fingers are of poor quality. This leads to the following problems like significant number of spurious minutiae may be created ,a large percent of genuine minutiae may be ignored and large errors in their localization may be introduced.

Fingerprint enhancement algorithms improve the clarity of ridge and furrow structures [6]. The steps used in enhancement techniques are normalization, local orientation estimation, local frequency estimation, region mask estimation and filtering. Incorporating the enhancement algorithms improves the verification accuracy of matching systems. Experimental results show that the enhancement algorithms improve both the goodness index and verification performance.

2.CONCLUSIONS

The success fingerprint combination and their extensive deployment all over the world have prompted some individuals to take extreme measures to evade identification by altering their fingerprints. The problem of fingerprint alteration or obfuscation is very different from that of fingerprint spoofing, where an individual uses a fake fingerprint in order to adopt the identity of another individual. While the problem of spoofing has received substantial attention in the literature, the problem of obfuscation has not been addressed in the biometric literature, in spite of numerous documented cases of fingerprint alteration for the purpose of evading identification. We introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. The proposed algorithm based on the features extracted from the orientation field and minutiae satisfies the three essential requirements for alteration detection algorithm.

1. Determine the alteration type automatically so that appropriate counter measures can be taken.

2. Reconstruct altered fingerprints. For some types of altered fingerprints where the ridge patterns are damaged locally or the ridge structure is still present on the finger but possibly at a different location, reconstruction is indeed possible.

3. Match altered fingerprints to their unaltered mates. A matcher specialized for altered fingerprints can be developed to link them to unaltered mates in

the database utilizing whatever information is available in the altered fingerprints.

These steps may help to improve the goodness index and verification accuracy of fingerprint verification systems.

REFERENCES

[1] J. Feng and A. K. Jain, "*Fingerprint reconstruction: From minutiae to phase*," IEEE Trans. Pattern Anal. Mach.Intell. , vol. 33, no. 2, pp. 209–223, F eb. 2011.

[2] Johannes Merkle, Heinrich Ihmor," Performance of the Fuzzy Vault for Multiple Fingerprints", arXiv:1008.0807v5 [cs.CR],29 Nov 2011

[3] Sheng Li , Student Member, IEEE , and Alex C. Kot , Fellow IEEE," *Fingerprint combination for privacy protection*", IEEE Trans on Informa.forensics and security,vol 8,no 2,Feb 2013.

[4] L.Hong,Y.F.Wan,and A.Jain, "*Fingerprint image enhancement: Algorithm and performance evaluation,*" IEEE Trans. Pattern Anal.Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.

[5] George S. Eskander, Robert Sabourin and Eric Granger,Ecole de technologie sup´erieure, "Offline Signature-Based Fuzzy Vault (OSFV):Review and New Results", IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM),2014.