Integrated Biometric Template Security using Random Rectangular Hashing

Madhavi Gudavalli[1], Dr. D.Srinivasa Kumar[2] and Dr. D.Srinivasa Kumar[3]

[1] JNTU KAKINADA

Received: 11 December 2013 Accepted: 5 January 2014 Published: 15 January 2014

Abstract

Large centralized biometric databases, accessible over networks in real time are especially used for identification purposes. Multimodal biometric systems which are more robust and accurate in human identification require multiple templates storage of the same user analogous to individual biometric sources. This may raises concern about their usage and security when these stored templates are compromised since each person is believed to have a unique biometric trait. Unlike passwords, the biometric templates cannot be revoked and switch to another set of uncompromised identifiers when compromised. Therefore, fool-proof techniques satisfying the requirements of diversity, revocability, security and performance are required to protect stored templates such that both the security of the application and the users? privacy are not compromised by the impostor attacks. Thus, this paper proposes a template protection scheme coined as random rectangular hashing to strengthen the multimodal biometric system. The performance of the proposed template protection scheme is measured using the fingerprint FVC2004 and PolyU palmprint databases

Index terms— biometric cryptosystems, cancellable biometrics, feature level fusion, multimodal biometric systems, random rectangular hashing, template protection.

1 Introduction

biometric system automatically recognizes the person based on his/her physiological or behaviour characteristics [1]. As the biometric features are distinct to each person, it establishes direct connection between users and their identity. These systems are more ease and secure as they are not needed to remember any password or carry any token to gain access to the applications. The biometric systems which rely on the evidence of a single source of information for authentication (e.g., single fingerprint, iris, palm-print, retina, voice, ear or face) are known as Unimodal biometric systems. They often suffer from enrolment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data. One of the methods to overcome these problems is to make use of multimodal biometric systems, which combines information from multiple inputs of one or more modalities to arrive at a decision [2]. Depending on the level of information that is fused, the fusion scheme can be classified as sensor level, feature level, match score level and decision level fusion. The sensor level and the feature level are referred to as pre-mapping fusion while the matching score level and the decision level are referred to as post-mapping fusion [3]. The acquisition and processing sequence of these systems can be either serial or parallel. In the serial or cascade or sequential architecture, the acquisition and processing of the different sources take place sequentially and the outcome of one matcher may affect the processing of the subsequent sources. In the parallel design, different sources are processed independently and their results are combined using an appropriate fusion scheme [4].

The security of the system will be determined by the integrity of the biometric database. The conventional biometric systems elevate privacy and protective problems to the users [6]. A stolen template yields ruinous issues to the biometric system i.e an attacker recapitulates the seized template to the matching module to get admitted or the snatched template can be misused across other biometric systems for crossmatching that uses the same biometric modality [5]. Therefore, if the stored template is compromised, it becomes useless forever. A compromised template cannot be revoked because of the significant link between a biometric trait and its template. Thus, template protection has come into existence due to the intrinsic weaknesses of traditional biometric systems.

In general, a template protection scheme must fulfil the following requirements [5] In literature, Cancellable Biometrics [17] known as Transformation-based Approach and Biometric Cryptosystems [7] known as Helper Data Methods are the two approaches to secure stored single biometric template. Cancellable Biometrics facilitates the template to operate like a password which can be cancelled and reinstated if required. This approach assures the privacy and security of the actual biometric template by employing an irreversible transformation. Thus, the transformed biometric data is stored in the database instead of original template. This approach is furthermore organized as biometric salting and noninvertible transform. In [8] Soutar et al. suggested biometric encryption method. Three non-invertible transformation functions were proposed for cancellable fingerprint template generation by Ratha et. al. in [9] namely Cartesian transformation, surface folding transformation and polar transformation. In [10], Teoh et. al. proposed Bio-Hashing technique to produce cancellable fingerprint templates. A new token will be reissued in the case of compromised template. Biometric Cryptosystems circumscribe the template protection design by including biometric data into cryptographic bounds. This method stringent the template security by employing the biometrics data to determine an encrypted template. In [13] Dodis et al. introduced secure sketch and fuzzy extractor concepts in key generation from biometrics. A two-level quantization method was introduced by Li and Chang in [14] to obtain secure sketches. The practical issues in secure sketch construction and secure sketch quantization for face biometric were discussed by Sutcu et al. [15]. Buhan et al. in [11] addressed the problem of generating fuzzy extractors from continuous distributions.

The secure sketch construction is proposed for fingerprints in [12] and for multimodal systems (face and fingerprint) in [16].

This paper proposes a well-defined key-based transformation technique for integrated template of fingerprint and palmprint obtained by combining their respective feature vectors at feature level. In the proposed scheme, it is difficult to reconstruct the original template form the transformed template without submitting the distinctive secret key. A different key can be assigned to the biometric template for the generation of new one if the transformed template is compromised.

2 II.

3 Proposed System

The proposed scheme analyses the performance of multimodal biometric system that integrates extracted feature vectors of fingerprint and palmprint at feature level. This fusion level is preferred as it contains much richer information on the source data. The acquisition and processing sequence employed for this system is serial i.e each biometric source is obtained and processed independently with a short time interval between their successive acquisitions and processing.

4 a) Methodology

The following steps show the process of proposed template protection scheme.

Step 1: The user U i with identity ID i inputs fingerprint and palmprint data to get registered in the system.

Step 2: Feature Extraction-The acquired fingerprint and palmprint data are pre-processed and enhanced by adopting a two dimensional discrete wavelet transform (2D-DWT). The mutual attributes such as ridges of fingerprint and palmprint images are preserved using 2D Gabor filter.G(x, y, f, ?) = exp?? x? 2 +y? 2 2? 2 ?cos(2?fx?)

Where x?=xcos?+ysin? and y?=-xcos?+ysin?, f is the frequency of the sinusoidal plane wave along the direction ? from the x-axis, ? 2 is the standard deviation of the Gaussian envelope. The values considered for experiment are f= 10, ? 2 =16, and ?=?/8.

Step 3: Normalization-As the intensity domains of filtered palmprint and fingerprint are different, they are normalized to the same domain by employing Gaussian normalization.

5 G(x, y) =

??(??, ??) ? µ I ? I

Where I(x, y) denotes the pixel intensity at coordinate (x, y), µ I denotes the intensity mean, and ? I denotes the intensity standard deviation.

Step 4: Feature Level Fusion-The normalized LL subband images are combined at feature level using Daubechies Wavelet.

Step 5: Random Tiling-A set of rectangles with random characteristics of the user U i are generated from the fused feature using random tiling. The magnitude of each rectangle is obtained by computing the standard deviation. These magnitudes are concatenated to generate a feature vector. The random tiling is a function 'f' which accepts two parameters and returns a feature vector 'V'. V = f (I fused , K), Where I fused represents the fused feature, and 'K' is the user specific key to obtain the rectangles' characteristics. A set of random numbers r w , r h ? [-1,1] are generated using 'K' as the seed. A new set of features can be extracted from the fused feature in the case of a compromise using newly generated key 'K'.

6 Global Journal of Computer Science and Technology

Volume XIV Issue VII Version I Step 6: Cryptographic Key Generation-The biometric secret key 'k' is generated using AES algorithm which is the variableness origin to select the random rectangular regions. Thus, every user has a distinct fused template depending on the different unique keys generated.

Step 7: Helper Data Generation-Cancellable biometric features are generated through Bio-hashing using MD5 (Message Digest) from the random rectangle region. This hashing is a transformation function which represents the ridges in the form of a decimal vector.

The number of ridges falling within the rectangle region is counted. The numbers in the decimal vector form the basis for generating template bit-string. The same process is repeated for remaining rectangular regions. The hash vector is obtained by combining all the 8-digit fixed-length vectors produced from each rectangular region. This hash vector acts as the helper data and is stored in the database. The bit-string representing the biometric features is generated by utilising the hash vector. The process of cryptographic key, 'k' is formulated from the encoded Bio-hash is as follows.?????? ?????????????? ? ?? ?? ? ?????? ?????????????????? ? ?? ? ??? ?? = k ?

where ? is called Biokey, b c and b 'c refer to the encoded Bio-hash and decoded Bio-hash respectively, while ? denotes bitwise XOR operation.

Step 8: Bit-String Generation-The integer hash vector produced is insecure and occupies much of the database. The integer values are transformed to binary bit-string using the bit-block coding technique. This technique first initializes a fixed binary block with zeros. This block values will be reset to ones corresponding to the integer in the hash vector. This process is iterated for the remaining blocks of the hash vector to generate the binary bit-string.

7 III.

8 Experimental Results

The databases fingerprint FVC2004 [18] and PolyU palmprint **??**19] are used for performance analysis of the proposed integrated template security approach. The experiments were conducted on the randomly selected 10 samples of fingerprint and palmprint images of respective databases. The present work assumes that each user is allotted with a secret key which is stored in the database and these keys are lost by no means. The enrolled and query binary vectors are produced based on the secret keys and the scores for identification between the enrolled bit-strings (e) and query bit-strings (q') were computed using the formula:??????????(??, ??) = ? (?? ??=1

?? ?? ,?? ? ?? ??,??) ?? where ? represents the XOR operation, while e j,r , and q i,r corresponds to the r-th bit in e j and q i ,. L denotes the length of e j and q i . The collation between the enrolled and query binary templates is shown in Figure 2. The performance in terms of equal error rate (EER) with various random rectangles is listed in Table 1. It is observed that the rise in random rectangles lowers the EER. The root cause is that more features can be extracted with more number of random rectangles there by features more distinct.

The recognition rate obtained is lower than 1% when tested on public databases of FVC2004 [18]

9 IV. Conclusions

A novel scheme based on key based hashing with randomized rectangle is presented in this paper that produces short hash strings for integrated templates. These hashes cannot reproduce the original template without knowledge of the unique key. Further, the use of Bio-hash as the mixing process provides the one-way transformation and deters exact recovery of the biometric features when compromised. When the template is compromised, it is difficult to construct the original hash vector because the impostors cannot figure out the exact location of each ridge as the count of number of ridges is only contained in the random rectangle. In the current work, the performance attained is lower than 1%. The diversity property of proposed scheme is examined by evaluating the correlation of the bit-strings obtained by using different user specific keys as seed in random tiling process. In this case, a high positive correlation indicates that the old bit-string falls into the region of acceptance of the refreshed bit-string. Thus, the proposed scheme satisfies all the four requirements of template protection scheme namely, revocability, security, performance and diversity. The future work signifies the stolen-token scheme, where the attacker grabs the secret key to get access to the system.

V.

36

[1]

1

Figure 1: Figure 1 :

2

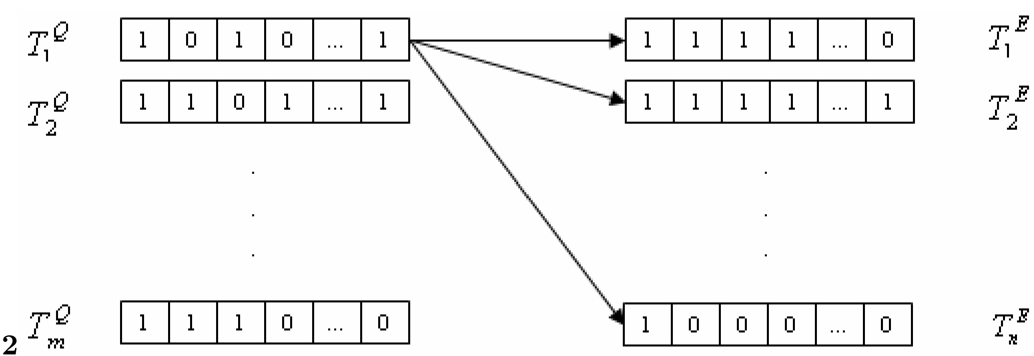

Figure 2: Figure 2 :

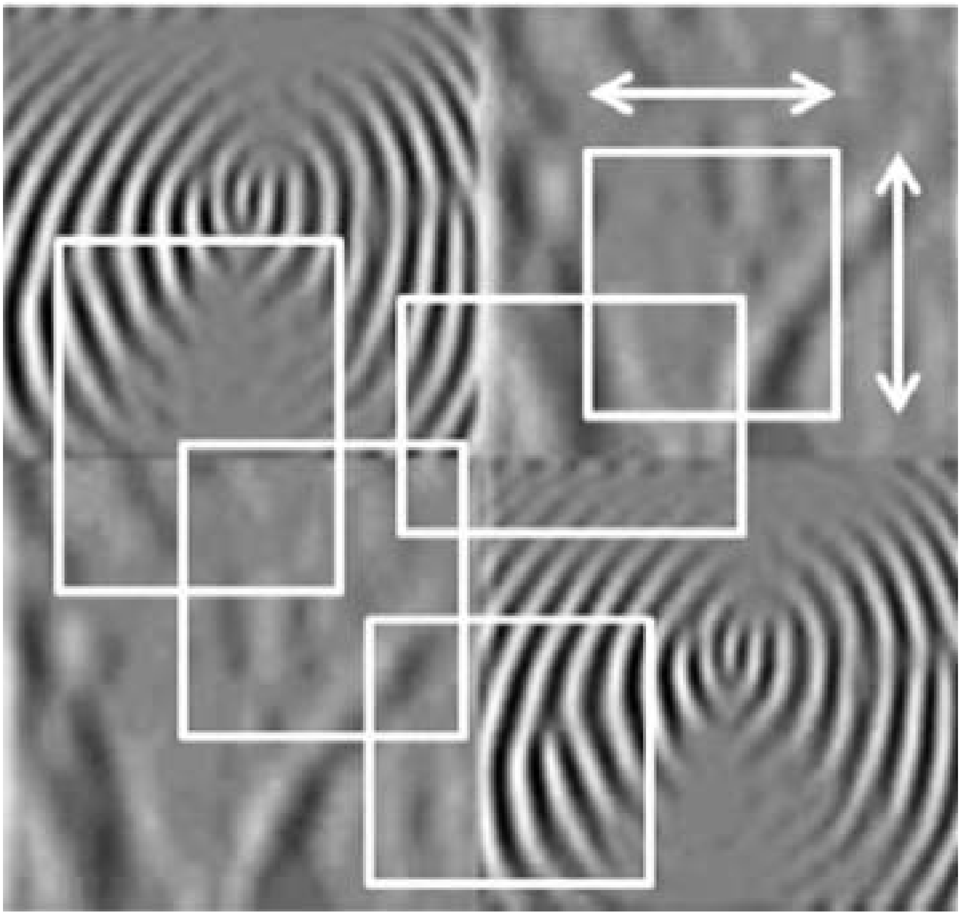

Figure 3:

1

Number of Random Rectangles	EER
10 Random Rectangles	2.81%
15 Random Rectangles	0.32%
20 Random Rectangles	0.20%

Figure 4: Table 1 :

.1 Acknowledgement

We would like to express our gratitude to all the referees' authors of the papers who have helped directly or indirectly the possibility to complete this research work.

[Gudavalli et al. ()] 'A Template Protection Scheme for Multimodal Biometric System with Fingerprint, Palmprint, Iris and Retinal Traits'. Madhavi Gudavalli , S Dr , Viswanadha Raju . ACM 978-1-4503-1185-4/12/09. *CUBE 2012 International IT Conference*, (Pune, Maharashtra, India) September 3-5, 2012. p. .

[Teoh et al. ()] 'BioHashing: Two factor authentication featuring fingerprint data and tokenised random number'. A B J Teoh , D C L Ngo , A Goh . *Pattern Recognition* 2004. 37 p. .

[Uludag et al. ()] 'Biometric Cryptosystems: Issues and Challenges'. U Uludag , S Pankanti , S Prabhakar , K Anil . *Proceedings of the IEEE* 2004. 92 (6) p. .

[Roberge et al. ()] *Biometric encryption. ICSA Guide to Cryptography*, C S D Roberge , A Stoianov , R Gilroy , B V Kumar . 1999.

[Anil et al. ()] 'Biometric Template Security'. K Anil , Karthik Jain , Abhishek Nandakumar , Nagar . *EURASIP Journal on Advances in Signal Processing* 2008. 2008. p. 17.

[Buhan et al. (2007)] 'Fuzzy Extractors for Continuous Distributions'. I R Buhan , J M Doumen , P H Hartel , R N J Veldhuis . *Proceedings of ACM Symposium on Information, Computer and Communications Security*, (ACM Symposium on Information, Computer and Communications SecuritySingapore) March 2007. p. .

[Arakala et al. (2007)] 'Fuzzy Extractors for Minutiae-Based Fingerprint Authentication'. A Arakala , J Jeffers , K J Horadam . *Proceedings of Second International Conference on Biometrics*, (Second International Conference on BiometricsSeoul, South Korea) August 2007. p. .

[Dodis et al. ()] 'Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data'. Y Dodis , R Ostrovsky , L Reyzin , A Smith . *Cryptology ePrint Archive* February 2006. 2004. (Technical Report) (A preliminary version of this work appeared in EUROCRYPT)

[FVC2004 Fingerprint Database] `http://bias.csr.unibo.it/fvc2004/` *FVC2004 Fingerprint Database*,

[Ratha et al. ()] 'Generating Cancelable Fingerprint Templates'. N K Ratha , S Chikkerur , J H Connell . *IEEE Pattern Analysis and Machine Intelligence*, 2007. 29 p. .

[Ratha et al. ()] 'Generating Cancelable Fingerprint Templates'. N K Ratha , S Chikkerur , J H Connell , R Bolle . *IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics* 2007. 29 (4) p. .

[Anil et al. ()] *Handbook of Biometrics*, K Anil , Patrick Jain , Arun A Flynn , Ross . 2007. Secaucus, NJ, USA: Springer-Verlag New York, Inc.

[Sanderson and Paliwal ()] *Information Fusion and Person Verification Using Speech and Face Information*, C Sanderson , K K Paliwal . IDIAP-RR 02-33. 2003.

[Madhavi Gudavalli et al. ()] Madhavi Gudavalli , . S Dr , Dr A Viswanadha Raju , Dr D Vinaya Babu , Kumar . 10.1109/ISBAST.2012.24. *IEEE-International Symposium on Biometrics and Security Technologies (ISBAST'12)*, (Taipei, Taiwan) March 26-29, 2012. p. . (MultiModal Biometrics-Sources, Architecture & Fusion Techniques: An Overview)

[Nandakumar ()] Karthik Nandakumar . *Multibiometric Systems: Fusion Strategies and Template Security*, 2008. (Ph.D Thesis)

[Sutcu et al. (2007)] 'Protecting Biometric Templates with Sketch: Theory and Practice'. Y Sutcu , Q Li , N Memon . *IEEE Transactions on Information Forensics and Security* September 2007. 2 (3) p. .

[Li and Chang (2006)] 'Robust, Short and Sensitive Authentication Tags Using Secure Sketch'. Q Li , E C Chang . *Proceedings of ACM Multimedia and Security Workshop*, (ACM Multimedia and Security WorkshopGeneva, Switzerland) September 2006. p. .

[Sutcu et al. (2007)] 'Secure Biometric Templates from Fingerprint-Face Features'. Y Sutcu , Q Li , N Memon . *Proceedings of CVPR Workshop on Biometrics*, (CVPR Workshop on BiometricsMinneapolis, USA) June 2007.