Journal of Biometrics & Biostatistics
ISSN: 2155-6180

Brindha and Natarajan, J Biom Biostat 2012, 3:6
DOI: 10.4172/2155-6180.1000150

Research Article Open Access

Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault

V Evelyn Brindha* and AM Natarajan

Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India

Abstract

Multi-biometric system stores multiple templates for the same user corresponding to the different biometric sources. Infallible security should be provided to the stored biometric templates as biometric is not revocable. In this work, multi-modal biometric template security for palmprint and fingerprint is proposed which is based on the fuzzy vault generation. At first, the preprocessing steps are applied and subsequently, the features are extracted and combined. For recognition, we match the feature vectors of images. The multi-modal biometric template along with the input key are used to generate the fuzzy vault. In the decoding process, the template is given as input and is combined with the stored fuzzy vault to generate the corresponding final key. The experimentation is carried out using CASIA database for palmprint and FVC 2004 database for fingerprint. The evaluation metrics have FMR and FNMR value parameters.

Keywords: Multi-modal biometrics; Template protection; Fuzzy vault; Fingerprint; Palmprint

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 traits also called as *templates*, represent a strong and permanent "link" between a person and his identity and these traits cannot be easily lost or forgotten or shared or forged. Biometric trait, called the *feature set* is unique for each and every person. The feature set obtained during enrollment 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 [1] to gain unauthorized access to the system (as well as other systems which use the same biometric trait). An attacker can furtively acquire the biometric information of a genuine user (e.g., lift the fingerprint from a surface touched by the 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.

The proposed work focuses on biometric systems that combine cues obtained from multiple biometric sources and these systems are commonly referred to as multibiometric systems. Systems that combine evidence from multiple sources of biometric information in order to reliably determine the identity of an individual are known as multibiometric systems [2]. One of the most potentially harmful attacks on a multibiometric system is against the biometric templates. Biometric templates (or the raw biometric images) should not be stored in plaintext form and fool-proof techniques are required to securely store the templates such that both the security of the application and the users' privacy are not compromised by adversary attacks. However, a multibiometric system requires storage of multiple templates for the same user corresponding to the different biometric sources. Hence, template security is even more critical in multibiometric systems where it is essential to secure multiple templates of a user. In this paper, we propose a unified scheme to secure multiple templates of a user in a multibiometric system by (i) transforming features from different biometric sources into a common representation, (ii) performing feature-level fusion to derive a single multibiometric template, and (iii) securing the multibiometric template using a single fuzzy vault construct. Fuzzy vault is a cryptographic construct that is designed to work with biometric features represented as an unordered set (e.g., minutiae in fingerprints).

Fingerprints have been used for over a century and are the most widely used form of biometric 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. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. Sometimes ridge may bifurcate or end. Each and every person in the world has a fingerprint as unique and remains unchanged over a lifetime. Fingerprint based recognition is cheapest and most widely

***Corresponding author:** V Evelyn Brindha, Associate Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India, Tel: 9790601852; Fax: 04295226666; E-mail: evelyn_brinda@yahoo.com

Received May 24, 2012; **Accepted** July 07, 2012; **Published** July 10, 2012

Citation: Brindha VE, Natarajan AM (2012) Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault. J Biom Biostat 3:150. doi:10.4172/2155-6180.1000150

used method for identity. Even identical twins have unique fingerprints. Passwords, PIN codes and smartcards are being used for identification, which may be lost or forgotten. But fingerprints can neither be lost nor forgotten, nor can be stolen.

In recent years, a series of automated biometric-based identification methods have emerged which include fingerprint, palmprint, iris pattern, voice, etc. In these biometric features, palmprint has greater similarity to fingerprint whose identification is rather mature.

Palmprint refers to an image acquired of the palm region of the hand. Palmprint based systems, as a new member in biometric family, has become an active research topic in recent years. The main advantage of palmprint is the availability of large space for extracting biometric features. Usually palmprint images should be normalized and oriented before feature extraction. It contains more information than fingerprints, so they are more distinctive. Palmprint capture devices are much cheaper than other devices like iris. Palmprints contain additional distinctive features such as wrinkles, principal lines which can be extracted from low-resolution images. By combining all features of palm and fingerprint such as ridge and valley features, principal lines and wrinkles, it is possible to build a highly accurate biometric system.

Palmprint is a combination of mainly two features, namely, the palmar friction ridges and the palmar flexion creases [3]. The corrugated skin patterns with sweat glands are known as palmar friction ridges. Discontinuities in the epidermal ridge patterns are called the palmar flexion creases. Further, there are three palmprint regions like interdigital, thenar and hypothenar as shown in Figure 1.

Palmprint has one salient feature called crease (shown in Figure 2). In the palmprint, the creases are large in number and comparatively easy to extract [3]. Creases are also approximately stable in a person's whole life, which qualifies themselves as features in palmprint recognition. To deal with creases in palmprints, both the ridge direction and frequency of minutiae points are calculated which helps to reduce the computational complexity information about the ridges and other minutiae in the neighborhood of a minutia.

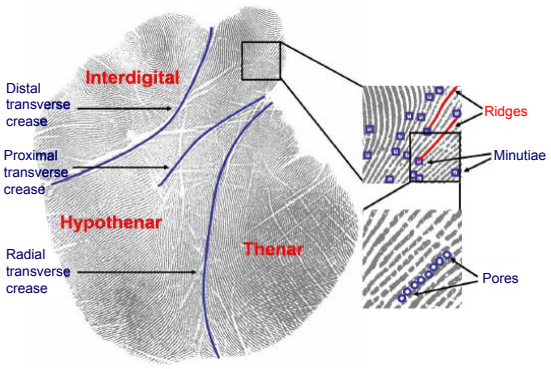


Figure 1: Regions in palmprint (adapted from [14]).

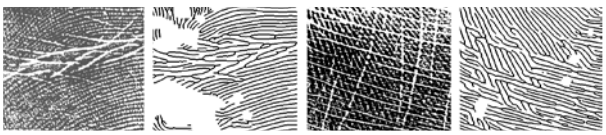


Figure 2: Palmprint regions with creases (adapted from [14]).

Related Works

A number of template protection techniques like fuzzy commitment [4], fuzzy vault [5], shielding functions [6] and distributed source coding [7] can be considered as key binding biometric cryptosystems [8] introduced the concepts of *secure sketch* and *fuzzy extractor* in the context of key generation from biometrics. The secure sketch can be considered as helper data that leaks only limited information about the template (measured in terms of entropy loss), but facilitates exact reconstruction of the template when presented with a query that is close to the template. The fuzzy extractor is a cryptographic primitive that generates a cryptographic key from the biometric features. The fuzzy vault scheme proposed by [5] has become one of the most popular approaches for biometric template protection and its implementations for fingerprint [9], face [10], iris [11] and signature [12] modalities have been proposed. Multibiometric fuzzy vaults based on multiple fingers [13] and fingerprint and voice [14] have also been proposed. In the proposed work, the focus is on a particular biometric cryptosystem known as fuzzy vault using combinations of multi biometric traits. Creating fuzzy vault using palmprint and finger print as a biometric trait is a very new technique.

Proposed Multi Biometric Fuzzy Vault

Pre-processing

Multibiometric vault provides better recognition performance and higher security compared to a unibiometric vault. While multibiometric systems overcome limitations such as non-universality and high error rates that affect unibiometric systems, they require storage of multiple templates for the same user. Multibiometric systems are more secure compared to their single biometric counterparts. In this work, fuzzy vault framework is used to secure both fingerprint and palmprint templates. Securing the different templates of a user separately is not optimal in terms of security. Hence, we propose a scheme for securing multiple templates of a user by creating multibiometric fuzzy vault.

In the proposed system, multimodal fuzzy vault for template security is implemented for protecting the biometric template. Multimodal biometric technology uses more than one biometric identifier to compare the identity of a person. This uses a combination of different biometric recognition technologies. Their performance is well compared to single modal biometric systems. The proposed multimodal biometric fuzzy vault includes combined feature points from palmprint and fingerprint (shown in Figure 3).

Initially, the enrolled image is preprocessed, the following are the steps involved in pre-processing

1. Binarization
2. Thinning
3. Minutiae extraction
   i. Bifurcation
   ii. Termination
4. Region of interest (ROI)

Binarization: The ridges in the fingerprint and palmprint images are highlighted with black color while furrows are white. It transforms

the 8-bit Gray image into a 1-bit image with 0-value for ridges and 1-value for furrows (shown in Figure 4).

Thinning: Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide (shown in Figure 5).

Minutiae extraction: A minutiae descriptor consists of ridge orientation and frequency at 76 equidistant points, uniformly spaced on 4 concentric circles around minutiae. The four concentric circles, with radius 27, 45, 63 and 81 pixels, contain 10, 16, 22 and 28 points, respectively. The radius and the number of points on each circle are selected in such a way that the descriptor values capture the maximum information contained in the neighborhood of minutiae (shown in Figure 6).

Here both bifurcation and termination of ridges in both the fingerprint and palmprint are taken.

- Bifurcation

The ridge pixels with three ridge pixel neighbors are identified as ridge bifurcations.

- Termination

The ridge pixels with two ridge pixel neighbors are identified as ridge terminations.

Orientation field is generated which not only shows the angle formed by ridge. It also represents the directionality of ridges in the fingerprint image (shown in Figure 7).

Region of Interest (ROI): Region of Interest (ROI) is useful for the recognition of each fingerprint image. The image area without effective ridges and furrows is first discarded because it only holds background information. It depends on the locations of minutiae and the directions of ridges at the minutiae location. False minutiae are affecting the accuracy of matching. So, removing false minutiae are essential to keep the system effective (shown in Figure 8).

Feature extraction

After the pre-processing step, both the images of fingerprint and palmprint are feature extracted. Here in our case, for every person, four images are given as input and for all images, pre-processing steps are carried out. The common unique co-ordinates (points) from all the four images are found out to obtain the features. Along with this, some random points (chaff points) are added for an individual to constitute the feature vector elements. The feature vector obtained from both the fingerprint and palmprint are subsequently concatenated. In our work, we have taken 60 unique points from fingerprint and palmprint and 20 chaff points are added to form the feature vector of a person. Figure 9 shows the block diagram of the feature extraction process.

Locking and unlocking of fuzzy vault

The proposed multimodal biometric fuzzy vault includes combined feature points from palmprint and fingerprint. The block diagram of the proposed system is shown in Figure 9. Initially the enrolled image is preprocessed; the steps followed during preprocessing are binarization, thinning, minutiae extraction, removal of false points and Region of Interest (ROI). The feature points extracted from both fingerprint and palmprint images are fused together and projected on the polynomial using the proposed algorithm. If a user wishes to hide a secret K using his biometric template which is represented as an unordered set X. The user selects a polynomial P that encodes the secret K and evaluates the polynomial on all elements in X. Additional dummy minutiae points called chaff points which do not lie on the polynomial P are added to confuse the hacker even if he gets the access of the stored templates. The chaff points hide the genuine points lying on P from an attacker. Since the points lying on P encode the complete information about the template X and the secret K, hiding these points secures both the template and the secret key concurrently.

The user can recover the secret *K* from the vault *V* by providing another biometric sample (query). Let the query be represented as another unordered set *X'*. If *X'* overlaps considerably with *X*, then the user can identify many points in *V* that lie on *P*. If adequate number of

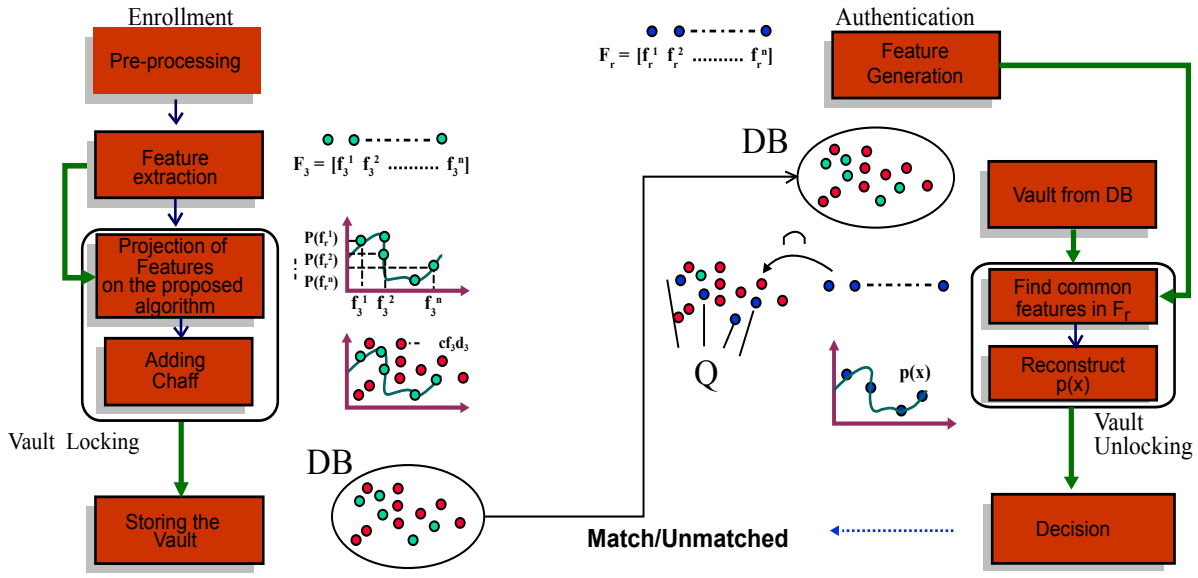
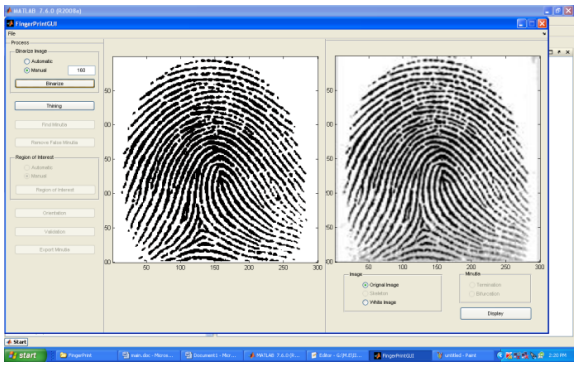
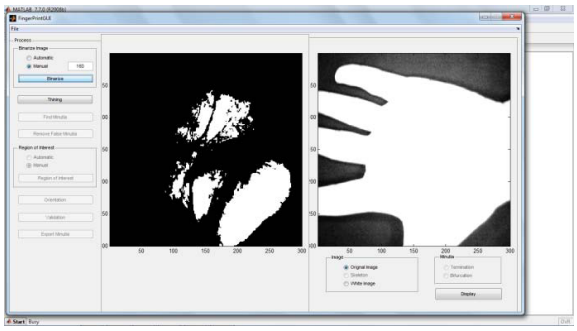


Figure 3: Block diagram of proposed system.

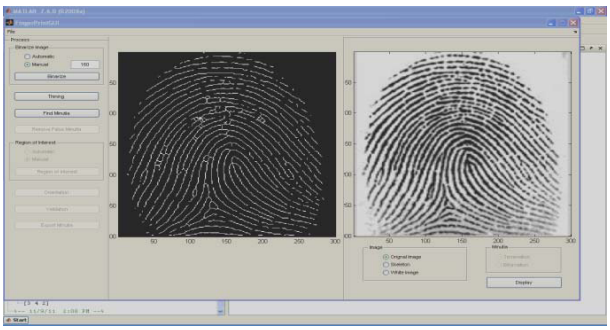


(a)

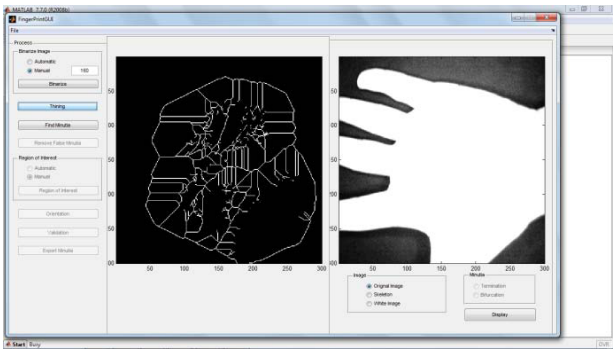


(b)

Figure 4: Binarization image (a) Fingerprint (b) Palmprint.



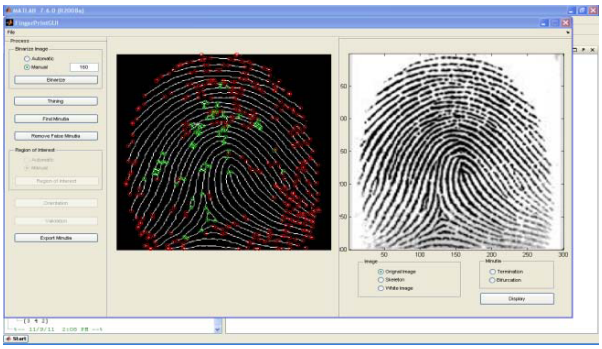
(a)



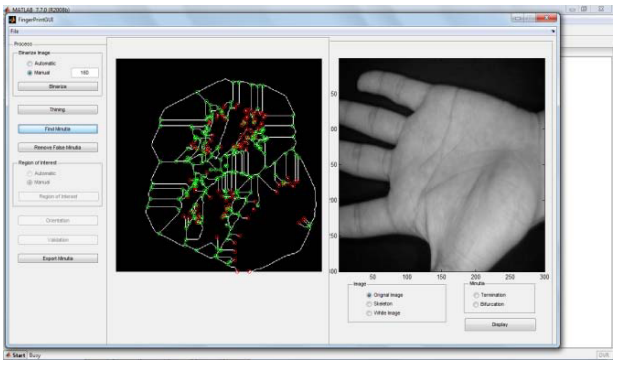
(b)

Figure 5: Thinning image (a) Fingerprint (b) Palmprint.

Figure 6: Minutiae descriptor.



(a)



(b)

Figure 7: Minutiae extracted image (a) Fingerprint (b) Palmprint.

points on *P* can be identified and are able to recreate P, then it is possible to decode the secret *K*. If *X*' does not overlap considerably with *X*, it is infeasible to reconstruct *P* and the authentication is unsuccessful. Since the secret can be retrieved from the vault even when *X* and *X*' are not exactly the same, this scheme is referred to as a *fuzzy* vault (shown in Figure 10).

Results and Discussion

The proposed technique is implemented in MATLAB on a system having 4 GB RAM and 2.10 GHz Intel i-5 processor. Here, the error rates are measured in order to determine the accuracy of the proposed technique. The number of obtained matches is known to be NGRA – (Number of Genuine Recognition Attempts). Rejection may happen

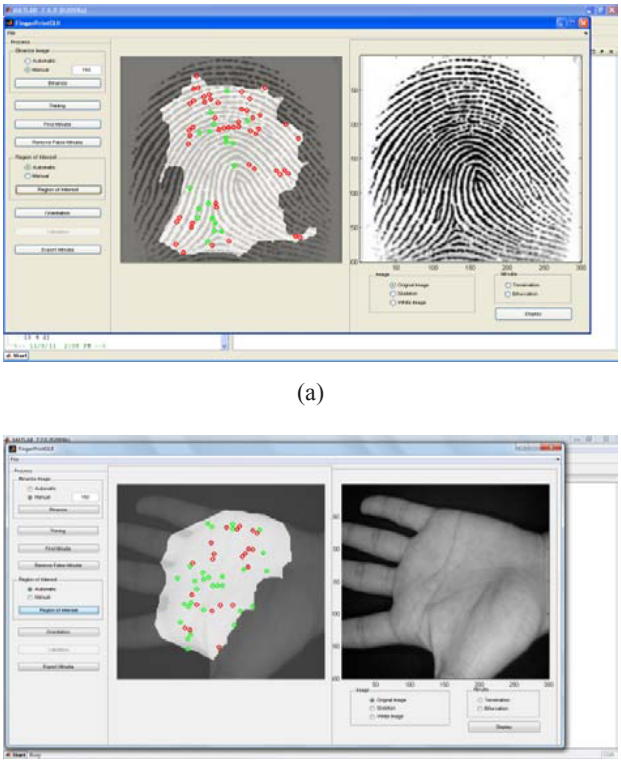


Figure 8: ROI image (a) Fingerprint (b) Palmprint.

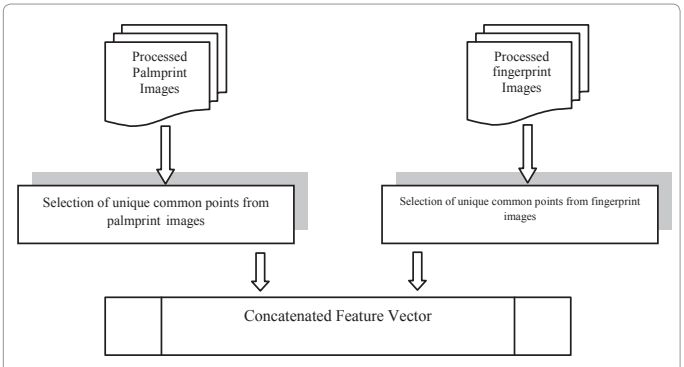


Figure 9: Block Diagram of the Feature Extraction Process.

for each fingerprint and palmprint images F_{ij} and these rejections are summed up and it is stored in REJ_{ENROLL}

$$FNMR(t) = \frac{gms}{NGRA}$$

where, *gms* is the genuine matching score. In addition, with each key from the fingerprint and palmprint K_{1i}, $i = 1,2,...,10$ is matched against with the first set of fingerprint and palmprint images from database $F_{1k}(i < k \le 10)$ and the corresponding Impostor Matching Score (*ims*) is computed. Number of Impostor Recognition Attempts (NIRA)

$$FMR(t) = \frac{ims}{NIRA}$$

Furthermore, the $FMR(t)$ (False Match Rate) and $FNMR(t)$ (False Non-Match Rate) are calculated from the above distributions for t

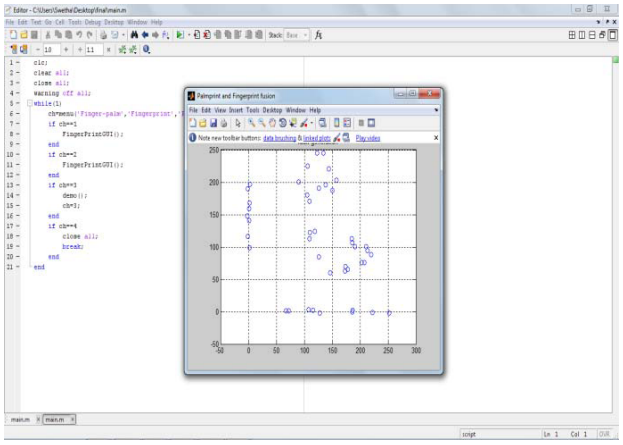


Figure 10: Multibiometric fuzzy vault using fingerprint and palmprint.

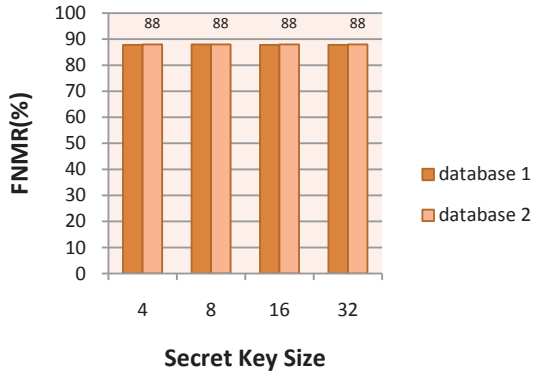


Figure 11: FNMR values without noise.

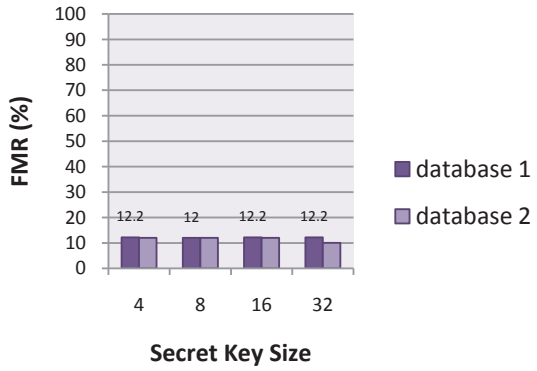


Figure 12: FMR values without noise.

ranging from 0 to 1. Two databases are taken in consideration. The first dataset will have the images of right finger print and the right palmprint. Likewise, the second dataset will have the images of left fingerprint and left palmprint. The performance of the proposed technique is analyzed by finding out the evaluation metrics which consists of values of FNMR and FMR. Here the analysis is carried out in two phases and in the initial phase, the secret key size is varied and the results are shown in Figure 11 and 12. In phase two, the effect of adding various noises are considered and the results are shown in Figure 13 and 14. The analysis

Figure 13: FNMR values after adding salt and pepper noise.

Figure 14: FMR values after adding salt and pepper noise.

Evaluation metrics	*key size=2^2*	*2^3*	*2^4*	*2^5*
FNMR	87.8%	88%	87.8%	87.8%
FMR	12.2%	12%	12.2%	12.2%

Table 1: Evaluation metrics obtained for database 1.

Evaluation metrics	*key size = 2^2*	*2^3*	*2^4*	*2^5*
FNMR	88%	88%	88%	88%
FMR	12%	12%	12%	12%

Table 2: Evaluation metrics obtained for database 2.

Evaluation metrics	*key size = 2^2*	*2^3*	*2^4*	*2^5*
FNMR	72.2%	72%	72.4%	71.8%
FMR	27.8%	28%	27.6%	28.2%

Table 3: Evaluation metrics obtained for database 1 under noise.

Evaluation metrics	*key size = 2^2*	*2^3*	*2^4*	*2^5*
FNMR	72.2%	72%	72.2%	71.9%
FMR	27.8%	28%	27.8%	28.1%

Table 4: Evaluation metrics obtained for database 2 under noise.

is carried out for both the datasets and results are obtained as follows. All the cases results in high FNMR and low FMR values which clearly indicates the effectiveness of the system.

Phase 1: Effect of various key sizes

In this phase, the secret key length is varied and corresponding evaluation metric values are found out. The key word size is varied in powers of two (Tables 1 and 2).

Phase 2: Effect of noise

In this phase, the datasets are considered under noise conditions. The evaluation metrics is calculated for varying key size. The noise which is added to the input image is salt and pepper noise. The noise is added to the image after preprocessing (Tables 3 and 4).

Conclusion

The proposed technique aims to improve the template security by the use of fuzzy vault. The inputs are the fingerprint and the palmprint images which are initially processed in order to smoothen the image and make it fit for feature extraction. Subsequently, feature extraction is carried to have the feature vector. The feature vector along with the key forms the fuzzy vault which is stored in the database. In the testing phase, the features of the test image are extracted and compared to the vault in the database. If all the points in the test image feature match, then the secret key is released which is found out from the points which remain unmatched in the respective vault. The technique yield good scores having FNMR of 88% and FMR of 12%. It performs well even after adding salt and pepper noise to yield FNMR of 72.2% and FMR of 27.8%.

References

1. Adler A (2003) Sample images can be independently restored from face recognition templates. In proceedings of Canadian Conference on Electrical and Computer Engineering, Montreal, Canada 2: 1163–1166.
2. Ross AA, Nandakumar K, Jain AK (2006) Handbook of Multibiometrics. Springer 6.
3. Jain AK, Feng J (2009) Latent palmprint matching. IEEE Transactions on Pattern Analysis and Machine Intelligence, USA 31: 1032-1047.
4. Yanıkoğlu, Berrin and Kholmatov, Alisher Anatolyevich (2004) Combining multiple biometrics to protect privacy. In Proceedings of ICPR Workshop on Biometrics: Challenges arising from Theory to Practice, UK.
5. Camlikaya E, Kholmatov A, Yanikoglu B (2008) Multi-biometric templates using fingerprint and voice. In Proceedings of SPIE Conference on Biometric Technology for Human Identification V, USA 6944.
6. Juels A, Sudan M (2002) A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory, 408.
7. Juels A, Wattenberg M (1999) A fuzzy commitment scheme. In Proceedings of 6th ACM Conference on Computer and Communications Security, USA 28–36.
8. Freire-Santos M, Fierrez-Aguilar J, Ortega-Garcia J (2006) Cryptographic key generation using handwritten signature. In Proceedings of Biometric Technologies for Human Identification III, USA 6202: 225–231.
9. Tuyls P, Akkermans AHM, Kevenaar TAM, Schrijen GJ, Bazen AM, et al. (2005) Practical biometric authentication with template protection. In Proceedings of 5th International Conference on Audio- and Video-Based Biometric Person Authentication, USA 436–446.
10. Draper SC, Khisti A, Martinian E, Vetro A, Yedidia JS (2007) Using distributed source coding to secure fingerprint biometrics. In Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), USA 2: 129–132.
11. Uludag U, Jain AK (2006) Securing fingerprint template: fuzzy vault with helper data. In Proceedings of IEEE Workshop on Privacy Research In Vision, USA 163-169.
12. Feng YC, Yuen PC (2006) Protecting face biometric data on smartcard with reed-solomon code. In Proceedings of Computer Vision and Pattern Recognition Workshop, New York, USA 29.
13. Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM journal on computing 38: 97-139.
14. Lee YJ, Bae K, Lee SJ, Park KR, Kim J (2007) Biometric key binding: fuzzy vault based on iris images. In Proceedings of Second International Conference on Biometrics, Seoul, South Korea 4642: 800–808.