Journal of Biometrics & Biostatistics
ISSN: 2155-6180

Brindha, J Biomet Biostat 2012, 3:4
DOI: 10.4172/2155-6180.1000145

Research Article Open Access

Biometric Template Security using Dorsal Hand Vein Fuzzy Vault

V Evelyn Brindha*

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

Abstract

Biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process. More importantly template security is of vital importance in the biometric systems because unlike passwords, stolen biometric templates cannot be revoked. In this paper we describe the various threats that can be encountered by a biometric system. We specifically focus on attacks designed to elicit information about the original biometric data of an individual from the stored template. A few algorithms presented in the literature are discussed in this regard. We also examine techniques that can be used to deter or detect these attacks. Furthermore, we provide experimental results pertaining to a biometric system combining biometrics with cryptography, that converts dorsal hand vein templates into novel cryptographic structure called fuzzy vault. Initially, the pre-processing steps are applied to dorsal hand vein images for enhancement, smoothing and compression. Subsequently, thinning and binary encoding techniques are employed and then feature extracted. Then the biometric template and the input key are used to generate the fuzzy vault. For decoding, biometric template from dorsal hand vein image is constructed and it is combined with the stored fuzzy vault to generate the final key. The experimentation was conducted using dorsal hand vein databases and the FNMR and FMR values are calculated with and without noise.

Keywords: Biometric cryptosystems; Unibiometric template Security; Hand vein pattern; Fuzzy vault; Secret key

Introduction

Personal identity refers to a group of attributes that are linked with an individual such as name, social security number etc. Trustworthy identity management machinery is at once required to battle the scourge expansion in identity theft and to have the improved security need in a diversity of utilizations varying from international border crossing to having personal information [1]. Substitute representations of identity such as passwords and ID cards can be effortlessly mislaid, shared or stolen. Passwords can also be simply guessed using social engineering [2] and dictionary attacks [3] and gives very little security. Biometric authentication, or rather biometrics, gives a likely and consistent answer to the quandary of identity revelation by making use of the identity of a person [4]. Biometric systems by design find out or confirm a person's identity based on his anatomical and behavioral features such as fingerprint, face, iris, voice and gait and these traits cannot be easily lost or forgotten or shared or forged. Since biometric systems need the user to be in attendance at the time of authentication, it can also daunt users from making false denial claims [5].

A typical biometric system comprises of several modules. The sensor module acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template. The matching module compares the feature set extracted during authentication with the enrolled template(s) and generates match scores. The decision module processes these match scores in order to either determine or verify the identity of an individual [6]. Thus, a biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into one of several identities (viz., identification) or into one of two classes - genuine and impostor users (viz., verification) [6]. While a biometric system can enhance user convenience and bolster security, it is also susceptible to various types of threats as discussed below [7,8].

1. Circumvention: An intruder may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the impostor can also modify sensitive data.

2. Repudiation: A legitimate user may access the facilities offered by an application and then claim that an intruder had circumvented the system. A bank clerk, for example, may modify the financial records of a customer and then deny responsibility by claiming that an intruder could have possibly stolen her biometric data.

3. Covert acquisition: An intruder may surreptitiously obtain the raw biometric data of a user to access the system. For example, the latent fingerprints of a user may be lifted from an object by an intruder and later used to construct a digital or physical artifact of that user's finger.

4. Collusion: An individual with wide super user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder.

5. Coercion: An impostor may force a legitimate user (e.g., at gunpoint) to grant him access to the system.

6. Denial of Service (DoS): An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service. For example, a server that processes access requests can be flooded with a large number of bogus requests, thereby overloading its computational resources and preventing valid requests from being processed.

***Corresponding author:** A M Natarajan, Professor and Chief Executive, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India, Tel: 9790601852; Fax:04295226666; E-mail: amn@bannari.co.in

Received March 24, 2012; **Accepted** May 24, 2012; **Published** May 25, 2012

Citation: Brindha VE (2012) Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. J Biomet Biostat 3:145. doi:10.4172/2155-6180.1000145

Ratha et al. [9] identified several different levels of attacks that can be launched against a biometric system (Figure 1): (i) a fake biometric trait such as an artificial finger may be presented at the sensor, (ii) illegally intercepted data may be resubmitted to the system, (iii) the feature extractor may be replaced by a Trojan horse program that produces predetermined feature sets, (iv) legitimate feature sets may be replaced with synthetic feature sets, (v) the matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security, (vi) the templates stored in the database may be modified or removed, or new templates may be introduced in the database, (vii) the data in the communication channel between various modules of the system may be altered, and (viii) the final decision output by the biometric system may be overridden.

The UK Biometric Working Group (UK-BWG) lists several factors that can affect the integrity of the template [10]: (i) accidental template corruption due to a system malfunction such as a hardware failure, (ii) deliberate alteration of an enrolled template by an attacker, and (iii) substitution of a valid template with a bogus template for the purpose of deterring system functionality.

In this paper, we discuss the second factor given above i.e. how deliberate alterations of an enrolled template by an attacker can be prevented?

Need for Template Protection

A template is essentially a compact representation (a set of invariant features) of the biometric sample that is stored in system database. If the security of stored templates is compromised, the attacker can fabricate physical spoof samples to gain unauthorized access. Such efforts have been detailed in [11], [12] and [13]. The stolen templates can also be abused for other unintended purposes, e.g. performing unauthorized credit-card transactions or accessing health related records. Figure 2(c) shows an example of a reconstructed fingerprint image from its minutiae representation (b), which is typically employed for fingerprint templates.

One of the most vital harmful attacks on a biometric system happens when it is against the biometric templates. Attacks on the templates can direct to grave vulnerabilities where a template can be replaced by an impostor's template to achieve unlawful access, or a physical spoof can be fashioned from the template [14,15] to achieve unauthorized access to the system, or the stolen template can be replayed to the matcher to have unauthorized access. Hence, biometric templates should not be stored in plaintext form and fool-proof methodologies are essentially needed to securely store the templates such that both the safety of the application and the users' solitude are not compromised by adversary attacks.

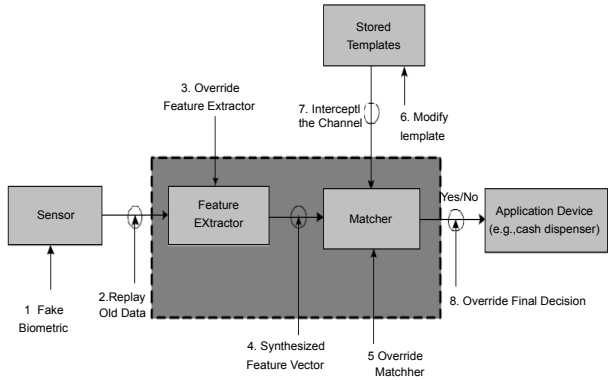

Figure 1: Vulnerabilities in a biometric system (adapted from [9]).

Why Dorsal Hand Vein Pattern?

Hand veins: The pattern of blood vessels hidden underneath the skin is quite distinct in individuals, even among identical twins and stable over long period of time. The primary function of veins is to carry blood from one part of the body to another and therefore vascular pattern is spread throughout the body. The veins that are present in hands, i.e. palm, finger and palm dorsal surface, are easy to acquire (using near infrared illumination) and have been employed for the biometric identification [16]. In this paper we have examined using the dorsal hand vein pattern. The vein patterns are generally stable for adults (age of 20-50 years). The reason for choosing vein recognition in this paper can be well understood from the table 1 given below.

There is no known large scale vascular biometric system. This could be primarily due to concerns about the system cost and lack of large scale studies on vein individuality and stability [17]. On the plus side, these vascular systems are touchless which often appeals to the user [17] and another important it cannot be spoofed easily as that of a fingerprint or palm print or any other traits and also it detects the liveness of the person being authenticated or identified which is very essential for today's world.

Related Works

Several methods that have been suggested in the literature to protect biometric templates some of them have been discussed below. In order to prevent the Hill-Climbing Attack from successfully

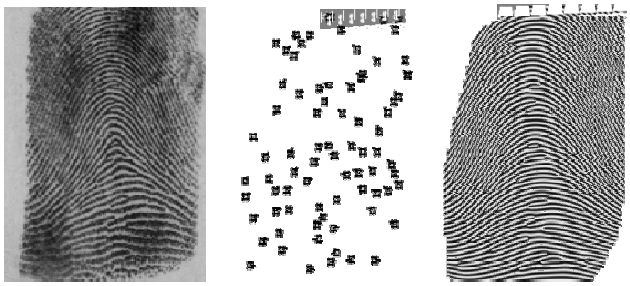

Figure 2: Reconstructing a fingerprint image from minutiae template [13]. (a) Original image, (b) minutiae template, (c) reconstructed fingerprint. Images in Figures 2(a) and 2(c) can be matched with high accuracy

Item	Vein recognition	Iris recognition	smart card identification
Security	The most accurate, and most secure	safer	low-level security
Development period	1998	80's	70's
Copy or Lost	No	Yes	Yes
Identification Speed	0.3 s	1~2 s	0.3 s
FAR	0.0001%	0.0001%	0.0001%
False Recognition Reason	Not exist	Eye diseases	Lost or Broken

Table 1: Comparison of hand vein biometrics with other latest biometric techniques (adapted from [26]).

converging, Soutar [18] has suggested the use of coarsely quantized match scores by the matcher. However, Adler [11] demonstrated that it is still possible to estimate the unknown enrolled image although the number of iterations required to converge is significantly higher.

Yeung and Pankanti [19] describes an invisible fragile watermarking technique to detect regions in a fingerprint image that have been tampered by an attacker. In this scheme, a chaotic mixing procedure is employed to transform a visually perceptible watermark to a random-looking textured image in order to make it resilient against attacks. This "mixed" image is then embedded in a fingerprint image. The authors show that the presence of the watermark does not affect the feature extraction process. The use of a watermark also imparts copyright capability by identifying the origin of the raw fingerprint image.

Jain and Uludag [20] suggest the use of steganography principles to hide biometric data (e.g., fingerprint minutiae) in host images (e.g., faces). This is particularly useful in distributed systems where the raw biometric data may have to be transmitted over a non-secure communication channel. Embedding biometric data in an innocuous host image prevents an attacker from accessing sensitive template information. The authors also have discussed a novel application wherein the facial features of a user (i.e., eigen-coefficients) are embedded in a host fingerprint image (of the user). In this scenario, the watermarked fingerprint image of a person may be stored in a smart card issued to that person. At an access control site, the fingerprint of the person possessing the card will first be compared with the fingerprint present in the smart card. The eigen-coefficients hidden in the fingerprint image can then be used to reconstruct the user's face thereby serving as a second source of authentication. But this system needs the person to carry a smart card with him during authentication.

Ferri et al. [21] propose an algorithm to embed dynamic signature features into face images present on ID cards. These features are transformed into a binary stream after compression (used in order to decrease the amount of payload data). A computer generated hologram converts this stream into the data that is finally embedded in the blue-channel of a face image. During verification, the signature features hidden in the face image are recovered and com-pared against the signature obtained online. Ferri et al. [21] report that any modification of the face image can be detected, thereby disallowing the use of fake ID cards.

Since the biometric trait of a person cannot be easily replaced (unlike passwords and PINs), a compromised template would mean the loss of a user's identity. Ratha et al. [22] propose the use of distortion functions to generate biometric data that can be canceled if necessary. They use a non-invertible transformation function that distorts the input biometric signal (e.g., face image) prior to feature extraction or, alternately, modifies the extracted feature set (e.g., minutiae points) itself. When a stored template is compromised, then the current transformation function is replaced with a new function thereby "canceling" the current (compromised) template and generating a new one. This also permits the use of the same biometric trait in several different applications by merely adopting an application specific transformation function. But matching is not clearly defined in the transformed domain.

In the dominion of template transformation, the so called biometric cryptosystems are in advance popularity. These systems combine biometrics and cryptography at a level that allows biometric matching to effectively take place in the cryptographic domain, hence exploiting the associated higher security. For example, Uludag et al. [23] convert fingerprint templates (minutiae data) into point lists in 2D space, which implicitly hide a given secret (e.g., a 128-bit key). The list does not reveal the template data, since it is augmented with chaff points to increase security. The template data is identified only when matching minutiae data from an input fingerprint is available (Table 2).

Proposed Fuzzy Vault Using Dorsal Handvein Pattern

In this section, we have described the proposed biometric template security using dorsal hand vein fuzzy vault. Proposed technique aim to design and develop, a dorsal hand vein based fuzzy vault technique that improves the biometric template security. The images are taken in touchless mode. In touch mode, the physical contact is made at the

Hand Vein	*key size=2^2*	*2^3*	*2^4*	*2^5*
FNMR	90%	90%	90%	90%
FMR	10%	10%	10%	10%

Table 2: Evaluation metrics obtained for dorsal hand vein with varying key size.

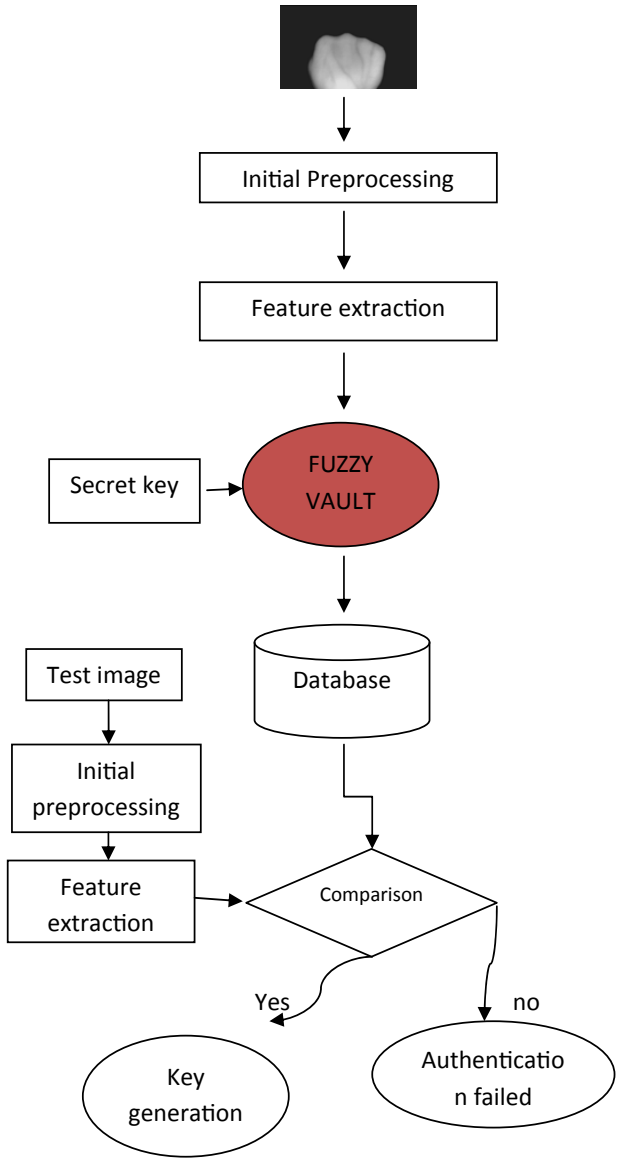

Figure 3: Block diagram of the proposed technique.

time when the image is taken where as in touchless; the direct contact is not there. In this mode the hand is kept at a distance when the image is taken.

The input dorsal hand vein images are pre-processed and subsequently, thinning and binarization techniques are employed and features are extracted. The extracted features from the dorsal hand vein form the biometric template. The biometric template and the input key that is generated using an algorithm are used to create the fuzzy vault. For decoding, the biometric template from dorsal hand vein images will be constructed and it is combined with the stored fuzzy vault to generate the final key. Figure 3 shows the block diagram of the proposed technique [24].

Initial preprocessing

All the input images are initially preprocessed to enhance the quality. The preprocessing consists of the following operations listed as follows

- Image scaling
- Double precision
- Grayscale conversion
- Binary encoding
- Motion filter
- Morphological operations
- Region property

Feature extraction

After the initial preprocessing, feature is extracted from the images of hand vein. Here for every person, four images are given as input and for all images initial process is carried out. The common unique coordinates (points) to all the four figures are found out and random points are selected for an individual.

Let the input hand vein images of i^{th} individual be represented by where $H_{i1}, H_{i2}, ..., H_{iN}$ is the total number of images for each person which is four in our case. After initial process, let the hand vein images of i^{th} individual be represented by $h_{i1}, h_{i2}, ..., h_{iN}$. Let the random unique common points extracted from hand vein of i^{th} individual $\{h_{i1}, h_{i2}, ..., h_{iN}\}$ be $P_{ih1}, P_{ih2}, ..., P_{ihM}$.

Fuzzy vault generation

The secret key along with the concatenated feature vector give rise to the fuzzy vault which provide template security. Points corresponding to the secret key are plotted along with feature vector points to yield the fuzzy vault. Number of points for the secret number will be the number of bits in the secret number. Here the points corresponding to the secret key are made by having x co-ordinate value of the secret number bit and y co-ordinate value of the prime number which comes next to the secret number bit.

The feature vector of the i^{th} individual is given by $\{P_{ih1}, P_{ih2}, ..., P_{ihM},\}$. Let the input secret number be, so there will be three points corresponding to the number as it is a three bit number. The three points are $\{X, X_p\}, \{Y, Y_p\}$ *and* $\{Z, Z_p\}$ denoted by P_{Xi}, P_{Yi} *and* P_{Zi} respectively. Here X_p, Y_p *and* Z_p are prime numbers which come next to X, Y *and* Z respectively. So the fuzzy vault for i^{th} individual will have the points $Fv_i = \{P_{ih1}, P_{ih2}, ..., P_{ihM}, P_{Xi}, P_{Yi}, P_{Zi}\}$.

Decoding module

The hand vein image of an individual is compared with the database fuzzy vault which in turn generates the secret key if matched. Here the images are initially processed and feature extracted. This feature vector is compared to the fuzzy vault database in order to generate the secret key (Table 3).

Let the feature vector of the images be represented by E which is compared to the database D_b having the fuzzy vaults $Fv_1, Fv_2, ..., Fv_K$. If it is such that all the points of the test image feature vector match with the vault, the corresponding images are said to be matched and x co-ordinate of the remaining three points in the vault will give the secret key. Hence the secret key is successfully and securely retrieved from the fuzzy vault and the hand vein template is secured from attackers.

Results and Discussion

Dataset description

Hand vein: Hand vein dataset [15] sample consists of images of 100 hands where each hand has 5 images, hence totaling to 500 images. Each has 5 images per person per each hand and hence it is associated to 50 distinct person for left and right hands of which the first 50 are for the right hands, the last 50 are for the left hand of the same person hand. So 1 in first set is RH HV and 51 is left hand to same person 1 in RH. This dataset is for both females and males in the range of 16-65 years age. Subjects are of healthy conditions and are from all folks of life including students, professors, engineers workers, house wives, etc.

Experimental results

In this section, we have given the images at different levels of execution of our proposed technique. The input image is shown by Figure 4 which is filtered to obtain the filtered hand vein image and is shown in Figure 5. The morphological image is shown in Figure 6 and the extracted hand vein image is shown in Figure 7.

Under noise	*key size=2^2*	*2^3*	*2^4*	*2^5*
FNMR	80%	80%	80%	80%
FMR	20%	20%	20%	20%

Table 3: Evaluation metrics obtained for dorsal hand vein under noise.

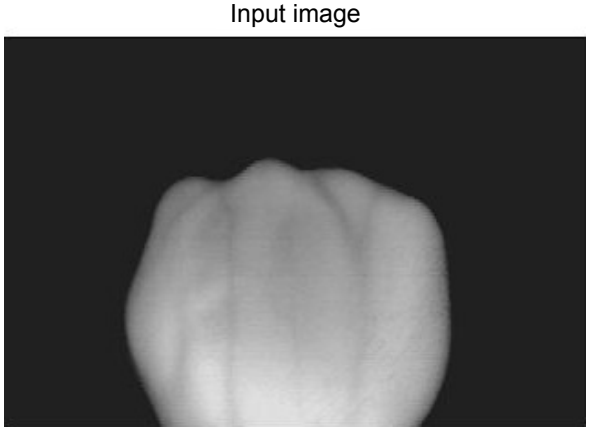

Figure 4: Input image.

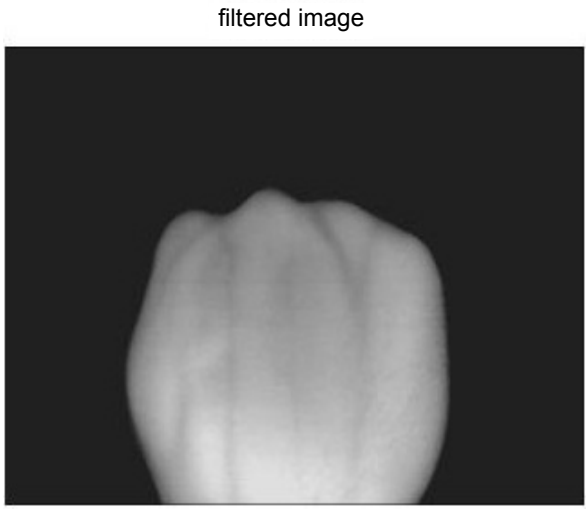

Figure 5: Filtered image.

Figure 6: Morphological image.

Figure 7: Extracted hand vein image.

Performance analysis

In this section, we analyze the performance of the proposed technique 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 in phase two, we consider the noise effects (Figure 8).

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 (Figure 9).

Effect of noise

In this phase, we consider the dataset under noise conditions. Here

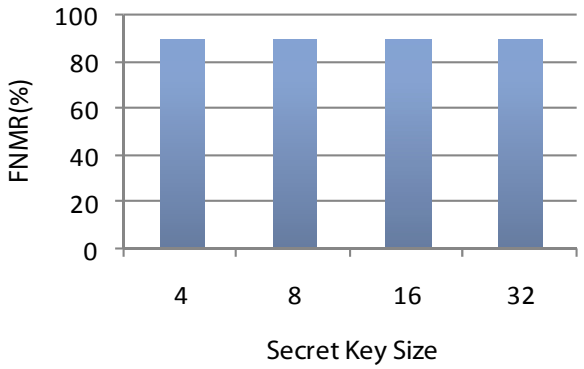

Figure 8: Plot of FNMR values.

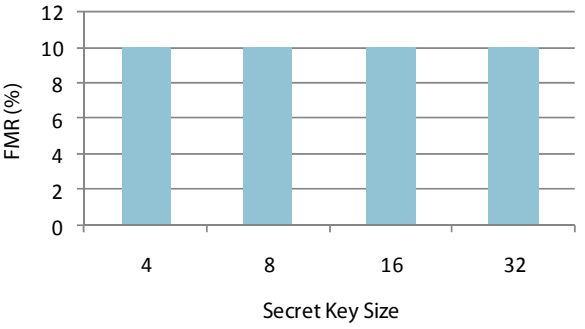

Figure 9: Plot of FMR values.

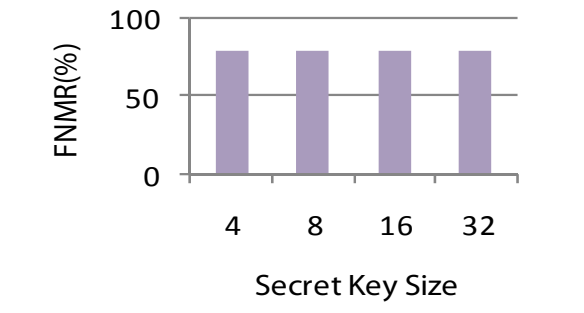

Figure 10: Plot of FNMR values.

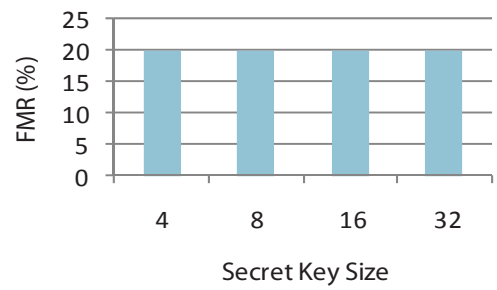

Figure 11: Plot of FMR values.

also we calculate the evaluation metrics for varying key size (Figure 10,11).

Conclusion

The proposed technique aims to improve the template security by the use of fuzzy vault. The inputs are the hand vein which is 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.

Acknowledgement

My sincere and heartfelt thanks to Professor Dr. Ahmed M. Badawi, at systems and biomedical engineering, Cairo University, for providing me the database without which I would not have completed this project.

References

1. IBM Corporation (1970) The Consideration of Data Security in a Computer Environment. Technical Report G520-2169, IBM.
2. Mitnick KD, Simon WL, Wozniak S (2002) The Art of Deception: Controlling the Human Element of Security.
3. Klien DV (1990) Foiling the cracker: A survey of, and improvements to, password security. Proceedings of the Second USENIX Workshop on Security.
4. Jain AK, Bolle R, Pankanti S (1999) Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, USA.
5. Jain AK, Nandakumar K, Lu X, Park U (2004) Integrating Faces, Finger- prints and Soft Biometric Traits for User Recognition. Biometric Authentication 3087: 259-269.
6. Jain AK, Ross A, Uludag U (2005) Biometric Template security: challenges and solutions. Proceedings of European signal processing conference (EUSIPCO), Turkey.
7. Maltoni D, Maio D, Jain AK, Prabhakar S (2003) Handbook of Fingerprint Recognition. Springer-Verlag.
8. Uludag U, Jain AK (2004) Attacks on biometric systems: a case study in fingerprints. Proceedings SPIE Security, Seganography and Watermarking of Multimedia Contents VI 5306: 622-633.
9. Ratha N, Connell JH, Bolle RM (2001) An analysis of minutiae matching strength. Audio- and Video-Based Biometric Person Authentication 223-228.
10. U.K. Biometric Working Group (2003) Biometric security concerns. Technical Report, CESG, http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf
11. Adler A (2004) Images can be reconstructed from quantized biometric match score data. Proceedings of Canadian Conference Electrical Computer Engineering, Niagara Falls, 469-472.
12. Ross A, Shah J, Jain AK (2007) From templates to Images: Reconstructing fingerprints from minutiae points. IEEE Transactions Pattern Analysis and Machine Intelligence 29: 544-560.
13. Feng J, Jain AK (2009) FM Model Based Fingerprint Reconstruction from Minutiae Template. Advances in Biometrics 544-553.
14. Cappelli R, Lumini A, Maio D, Maltoni D (2007) Fingerprint Image Reconstruction From Standard Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29: 1489-1503.
15. Hand Vein database, Prof. Dr. Ahmed M. Badawi at systems and biomedical engineering, Cairo University.
16. Kumar A, Prathyusha KV (2009) Personal authentication using hand vein triangulation and knuckle shape. IEEE Transactions on Image Processing 38: 2127-2136.
17. Jain AK, Kumar A (2010) Biometrics of next generation: An overview. Second generation biometrics, Springer.
18. Soutar C, Biometric system security. White Paper, BioscryptA.
19. Yeung M, Pankanti S (1999) Verification watermarks on fingerprint recognition and retrieval. Proceedings SPIE, Security and Watermarking of Multimedia Contents 3657: 66-78.
20. Jain AK, Uludag U (2003) Hiding biometric data. IEEE Transactions Pattern Analysis and Machine Intelligence 25: 1493-1498.
21. Ferri LC, Mayerhofer A, Frank M, Vielhauer C, Steinmetz R (2002) Biometric authentication for ID cards with hologram watermarks. Proceedings SPIE, Security and Watermarking of Multimedia Contents IV 4675: 629-640.
22. Ratha N, Connell J, Bolle R (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40: 614-634.
23. Uludag U, Pankanti S, Jain AK (2005) Fuzzy vault for fingerprints. Audio- and Video-Based Biometric Person Authentication 3546: 55-71.
24. http://www.pwbio.com/fanan 1.asp?sclass=Hardware solutions & id=82&title=Dorsal hand vein biometric system.