Security Considerations for Prealigned Fingerprint and Palm Vein Templates using Biometric Cryptosystems

V. Sujitha
Department of Computer Science and Engineering
Dr. N. G. P Institute of Technology
Coimbatore, Tamilnadu, India
e-mail : sujithavpacet@gmail.com

In-Ho Ra
School of Computer Information and Communication Engineering
Kunsan National University,
Gunsan, South Korea
e-mail : ihra@kunsan.ac.kr

Han-Gue Jo
School of Computer Information and Communication Engineering
Kunsan National University,
Gunsan, South Korea
e-mail : hgjo@kunsan.ac.kr

Abstract

Biometric is a process for identifying an individual in a reliable way using unique biological features. The most challenging in biometric is to store templates securely. Cryptography is fused with biometrics to attain high security. In this proposed scheme, multimodal biometric verification scheme has been implemented using cryptosystem to overwhelm the problem of unibiometric and increase the security of templates. Fuzzy vault based cryptosystem is created to protect templates and it is the most powerful technique for template security. Finger print and palm vein biometric features are considered for our evaluation. During enrollment stage, obtained finger print and palm vein descriptions are automatically prealigned using directed reference point. Extracted minutiae features are embedded with a secret key and it is used to produce the vault. Generated vault is stored along with chaff points. During authentication query features are generated and matched with stored templates. FVC 2002 and CASIA database are taken for evaluation in this proposed scheme and this scheme gives better accuracy. The performance of the proposed scheme is analyzed against brute force and correlation attacks.

1. Introduction

Biometric is a scheme for authenticating a person using their biological features. Various biometric authentication schemes are developed using Face, Fingerprint, Palm vein, Palmprint, Iris, Hand Geometry and Signature etc [1]. Among these features palm vein and fingerprint schemes produce higher efficiency. Palm vein features are much harder for intruders to copy compared to other biometric features and Fingerprint features are very unique for every individual. Unimodal system may not be able to achieve the desired performance in real world applications. It suffers from registration problems due to noisy data, nonuniversality, spoof attacks and inter class variations that reduce system performance and safety [2]. Multimodal biometric system combines information from various biometric modalities of the same person for identification and authentication [3]. Multimodal biometric system provides better performance than unimodal system and to address the unimodal problems. One of the critical issues in biometric based authentication system is securing the biometric template of a user that is usually stored in the system database. Fuzzy vault is an efficient cryptosystem based on protection scheme to secure biometric template [4]. The present work is planned as follows. Section 2 describe the background works in this area. Section 3 presents the outline of present authentication scheme. The experimental results are discussed in Section 4. Conclusion and Outlook of the present scheme are represented in Section 5.

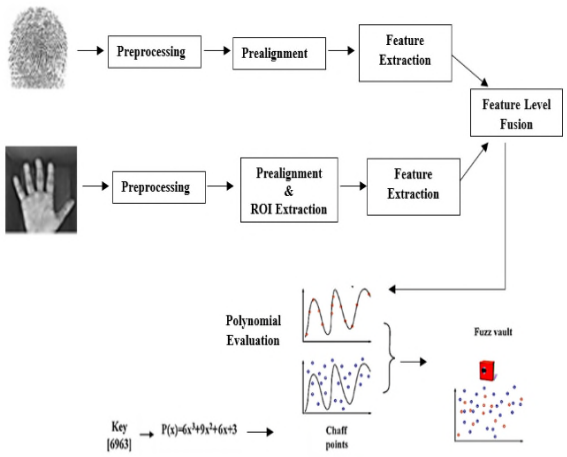
2. Background

Biometric images are mainly secured using two methods such as Cryptosystem and Feature Transformation. In these two methods, Biometric cryptosystems have been developed as a powerful tool for guard templates. Various template security methods such as fuzzy vault [5], fuzzy commitment [6], source coding [7], and fuzzy extractor [8] have developed in biometric cryptosystem. From these various techniques fuzzy vault system provides high security. Fuzzy vault based finger print authentication scheme is developed to secure templates and improve the accuracy [9], [10]. Palm vein recognition exhibit liveness detection, high safety, user satisfactoriness and suitability [11], [12]. Fuzzy vault-based palm vein authentication is developed and it produces high security [13]. Several studies have been proved that the multi biometric template protection scheme using fuzzy vault systems is a more secure method [14], [15]. In our proposed work finger print and palm vein images are prealigned using reference point and fuzzy vault scheme is employed to protect templates.

3. Prealigned Multimodal Biometric Cryptosystem

In this proposed work multimodal biometric authentication is performed using fuzzy vault cryptosystem. Initially, during enrollment stage the fingerprint and hand palm images are obtained. After that, the obtained images are preprocessed to eliminate noise using preprocessing techniques. The attained fingerprint descriptions are prealigned automatically using that orientation points and quantization is also performed. In hand images, after preprocessing palm vein images are prealigned automatically.

After prealignment, ROI (Region of Interest) is extracted using coordinate points. Fingerprint and palm vein features are extracted and extracted genuine points are used to generate fuzzy vault. Genuine points are projected on the polynomial and more chaff points are embedded with genuine points and it improves the security because hackers cannot hack the templates easily. Finally generated vault is stored into the database. Block diagram for proposed multibiometric fuzzy vault system is depicted in figure 1.



(Figure 1) Block diagram for multibiometric system

3.1 Prealigned fingerprint authentication system

A) Preprocessing

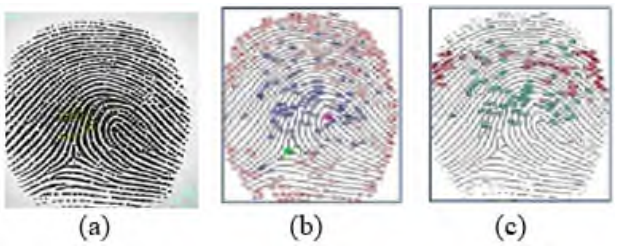
Preprocessing is a technique to remove noise from enrolled image. Histogram equalization is a method to enhance the global contrast and increase the quality of an image. Binarization and segmentation process is carried out to eliminate undesirable edges after enhancement. Morphological operations such as dilation and erosion are carried out to derive the ROI [16].

B) Minutiae Extraction and Prealignment

Minutiae points are extracted using cross numbering method from ROI. The value of cross number (CN) for pixel P is calculated using the following equation (1),

$$N(P)=\frac{1}{2}\sum_{j=1}^{8}|P_j-P_{j-1}| \quad (1)$$

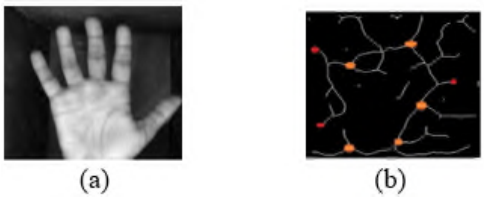
Orientation fields are projected using core and delta points. Euclidean distance is found and false details are omitted. After orientation field estimation, translation and rotation should be carried out to perform prealignment and the finger print images are quantized. The figure 2 shows fingerprint minutiae extraction process.



(Figure 2) Finger print minutiae Extraction. (a) Enrolled Image (b) Core and Delta Point (c) Minutiae Extraction

3.2 Prealigned Palm Vein Authentication System

Initially the hand images are obtained and images are preprocessed to remove noise. During preprocessing median filter is applied to remove noise and the morphological operations are carried out to remove image flaws. Palm vein image alignment and ROI mining process are done by palm contour detection using Sobel operator. Reference points are detected among fingers and centre point is identified. Using centre point rotate the image in clock wise direction. After pose normalization the ROI is cropped from image. Minutiae features of palm vein images are extracted. Based on distance calculation only limited points are taken for evaluation. The Palm vein image extraction process is displayed in figure 3.



(Figure 3) Palm vein feature extraction (a) Input Image (b) Extracted minutiae of Palm Vein image

3.3 Fuzzy vault Construction for multimodal biometrics

Feature vectors are extracted from finger print and palm vein images. The derived features are merged to create single feature vector. During encoding, Genuine points are extracted and along with genuine points

chaff points are added to generate vault (V). Polynomial evaluation is performed along with secret key. Constructed vault stored into the database. During decoding, fingerprint and palmvein images of a query person is given as input that images are preprocessed. The generated feature vector is related to the stored vault.

Algorithmic steps for fuzzy vault construction

Step 1: Fusion of fingerprint and palmvein features

Two set of features F={f_1,f_2,f_3……f_m} and PV={pv_1,pv_2,pv_3…..pv_n} are attained from fingerprint and palm vein images. Feature vectors (FV) are extracted shown in equation 2.

FV={f_1,f_2,f_3,…f_m,pv_1,pv_2,pv_3,…pv_n} (2)

Step 2: Generation of Polynomial

Secret key, $SK = \{K\}_{i=0}^{n-1}$ is used to produce the polynomial P with order n.

Step 3: Produce genuine features

Project the combined feature vector FV by polynomial P to generate genuine facts G shown in equation 3.

$$G = \left[\begin{pmatrix} (f_1, P(f_1)), \cdots \\ (f_m, P(f_m)), (pv_1, P(pv_1)), \cdots \ (p_{vn}, P(pv_n)) \end{pmatrix}\right] \quad (3)$$

Step 4: Creation of Chaff features

Make chaff points, C arbitrarily shown in equation 4.

$$C = [(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots \ (x_p, y_q)] \quad (4)$$

Step 5: Fuzzy Vault creation:

Construct the V =G∪C

(Table 1) Parameters for evaluation

Parameter	Finger print	Palm Vein	Multi modal
Genuine points count, G	40	30	70
Chaff points count, C	400	300	700
Total features, T	440	330	770
Polynomial degree, k	8-12	8-12	8-12

(Table 2) Performance of the current scheme

Polynomial Degree, k	GAR	FAR
8	95.6	0.04
9	93.5	0.03
10	90.5	0.03
11	88.6	0.02
12	83.5	0.01

4. Results and Discussion

Fuzzy vault based fingerprint and palm vein biometric template protection method are executed in MATLAB. FVC 2002 [17] and CASIA [18] databases are used for evaluation. For determining efficiency and accuracy of the template protection scheme Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR) is calculated. Number of parameters are represented in table 1. In table 2 GAR and FAR value are calculated and described.

4.1 Security Analysis

A) Brute Force Attack

Security analysis of the fuzzy vault is performed by evaluation min entropy. The minentropy of fuzzy vault method can be expressed in equation 5.

$$H_\infty = -\log_2\left(\frac{\binom{G}{K+1}}{\binom{T}{K+1}}\right) \quad (5)$$

In table 3 the total numbers of evaluation and security bits of proposed scheme are represented. Efficiency of the current system is compared in table 4.

(Table 3) Security analysis of the current system

Polynomial Degree	Total evaluations	Security Bits
8	1.1881×10^{38}	128
9	1.4682×10^{39}	131
10	1.8268×10^{40}	134
11	2.3466×10^{41}	137
12	3.1490×10^{42}	140

(Table 4) Efficiency of the proposed system

Vault type	Total Points & Degree	GAR & FAR	Total evaluations	Security Bits
Fingerprint [19]	440 & 8	89 & 0.72	5.7371×10^{9}	63
Palmprint [20]	275 & 8	99 & 0.02	1.0629×10^{10}	33
Combined Fingerprint & Palmvein	770 & 8	95.6 & 0.4	1.1881×10^{38}	128

B) Correlation Attack

Correlation attack adopts that some hacker intercepts multiple enrolments that are formed by same person biometric data. Minutiaes are quantized by the scheme described by Tams [21] to resist the correlation attack. In current system the feature space for each vault contains coarsely quantized minutiae that are encoded by the elements in E (x j, j' finite filed elements). This proves that our current method is resistant against a correlation attack.

5. Conclusion & Outlook

Multimodal biometric template protection using fuzzy vault implementation are developed. Fingerprint and palm vein images are used to form the multimodal biometric. Fingerprint and Palm vein images are preprocessed to enhance the quality of the obtained

image. Minutiae points are generated from finger and palm vein images. Extracted points are merged to form a single feature vector. Dummy points are embedded along with genuine points and secret key is used to create the vault. Generated vault is deposited into the database. During verification features are derived and analysed with the stored vault. If the features are matched, secret key is generated else denied. Experimental results shows that GAR performance of the proposed system is better compared to other methods. Also, it proved that the multibiometric scheme is strong against brute force and corelation attack. In forthcoming, the security will be improved by implementation of iris and face biometrics (or even other multi modalities also). Also, deep learning methods should be used to improve the alignment and accuracy.

Acknowledgements

This work was supported by the Human Resources Development Program (Grant No. 20194010201800) of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grants funded by the Korea government (Ministry of Trade, Industry, and Energy).

Reference

[1] Selwal, A, Gupta, SK & Kumar, S, “A Scheme for Template Security at Feature Fusion Level in Multimodal Biometric System”, Advances in Science and Technology, vol. 10, no. 31, pp. 23-30, 2016.

[2] Vandana, Navdeep Kaur, “A Study of Biometric Identification and Verification System” IEEE International Conference on Advance Computing and Innovative technologies in Engineering, 2021.

[3] Jagadiswarya and D. Saraswadya, “Biometric Authentication using Fused Multimodal Biometric”, Procedia Computer Science, vol. 85, pp. 109-116, 2016.

[4] Brindha, V. E., and Natarajan, A. M., “Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault”, Journal of Biometrics & Biostatistics 3(6):1 - 6, 2012.

[5] Juels, A., and Sudan, M., “A fuzzy vault scheme”, Des. Codes Crypt. 38(2):237 - 257, 2006.

[6] A. B. J. Teoh and J. Kim, “Secure biometric template protection in fuzzy commitment scheme”, IEICE Electron. Exp., vol. 4, no. 23, pp. 724 - 730, 2007

[7] Draper, S., Khisti, A., Martinian, E., Vetro, A., and Yedidia, J. S., “Using distributed source coding to secure fingerprint biometrics”, IEEE International Conference on Acoustics, Speech and Signal Processing, IN-9582274, 2007.

[8] Dodis, Y., Reyzin, L., and Smith, A., “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data”, Advances in cryptology-Euro crypt, Springer Berlin Heidelberg, 523 - 540, 2004.

[9] Joni Saputra, Joni Saputra, “Improving the Accuracy of Fuzzy Vault Scheme in Fingerprint Biometric”, IEEE, 2019.

[10] Nancy Singla, Manvjeet Kaur, Sanjeev Sofat, “Secure Fingerprint Fuzzy Vault Including Novel Chaff Point Generation Method”, IEEE International Conference on Computing, Communication and Automation, 2017.

[11] Wirayuda, T.A.B. “Palm vein recognition based-on minutiae feature and feature matching”, Int. Conf. on Electrical Engineering and Informatics, Legian-Bali, Indonesia, pp. 350 - 355, August 2015.

[12] Wei Wu,Stephen John Elliott,Sen Lin,Shenshen Sun,Yandong Tang, “Review of palm vein recognition”, IET Biometrics, Vol 9, Issue 1, 2020.

[13] S. S. Chidemyan, “Palm Vein and Fingerprint Based Multimodal Fuzzy Vault Scheme”, Proceedings of the Yerevan State University, Physical and Mathematical Sciences, 2015.

[14] Dale, MP, “Multimodal Analysis Based on Hand Features”, Ph.D. thesis, University of Pune, Pune, 2012.

[15] Ryszard S. Choras, “Multimodal Biometrics for Person Authentication”, Digital Identity, IntechOpen, 2019.

[16] Singh, R., Shah, U & Gupta, V, “Fingerprint Recognition”, Student Project, Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur, India, 2009.

[17] http://bias.csr.unibo.it/fvc2002/download.asp

[18] http://biometrics.idealset.org/dbDetailForUser.do?id=5

[19] Chitra, D., Sujitha, V. “Security analysis of prealigned fingerprint template using fuzzy vault scheme”, Cluster Computing 22, 12817 - 12825, 2019.

[20] V. Sujitha & D. Chitra, “Highly Secure Palmprint Based Biometric Template Using Fuzzy Vault” in Concurrency and Computation: Practice and Experience journal, vol31, issue 12, 2018.

[21] Tam, B., Mihailescu, P., and Munk, A., “Security considerations in minutiae-based fuzzy vaults”, IEEE Trans. Inf. Forensics Secur. 10(5):985 - 998, 2015.