Dual Fingerprints Fusion for Cryptographic Key Generation

M.Marimuthu
Assistant Professor
Coimbatore Institute of Technology

A.Kannammal
Professor
Coimbatore Institute of Technology

ABSTRACT
Secured data transfer is a critical issue through open networks due to attackers and intruders. This paper presents a new cryptographic key generation algorithm from dual fingerprint biometric template; the suggested approach has simplified the generation of cryptographic keys and reduces the complexity of traditional cryptosystem. . Fingerprints are permanent throughout person's lifespan. Keys are generated from the fingerprint template for encrypting and decrypting the content of the user. This method can be implemented in MATLAB and it generates different size cryptographic keys, with limited amount of time complexity and space complexity. This is appropriate for all real time applications that establish secured information exchange between the users. Proposed method is evaluated using publicly available FVC2002 database and achieves better result.

General Terms
Pattern Recognition, Security, Cryptography

Keywords
Biometrics, Fingerprint, Minutiae points

1. INTRODUCTION
A biometric is a science and it defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being [1]. A number of biometric characteristics are being used in various applications as Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability, and Circumvention [2]**.** The most common physical biometric patterns used for security purposes are the fingerprint, hand, eye, face, and voice. Compare with all biometric trait, fingerprints are highly explored in academic and research areas. With the widespread use of information exchange across the Internet, and storing the sensitive data on open networks, cryptography plays a major role for providing data security. Many cryptographic algorithms like AES, DES, DSA, DSS and RSA are proposed and revealed its ability of securing the information. Naturally, a growing popular research direction is to fuse different features together. Fusing of biometric trait and cryptography is a better idea to protect the message from attackers and unauthorized user.

Normally traditional cryptosystem have a numerous of associated demerits and problems such as [3]

1. Traditional cryptography authenticates messages based on the key but not on the user. The method is unable to differentiate between the legitimate user and a hacker.

2. Cryptographic keys can be easily guessed or cracked.

3. Large size of strong keys takes more time for message encryption/decryption.

4. It is tedious to remember the keys, storing them in a database might be insecure.

5. Moreover, maintaining and sharing lengthy, random keys is the critical problem in the cryptography system.

1.1 Levels of Fusion
Biometric fusion can be defined broadly as the use of multiple types of biometric data or methods of processing to improve the performance of biometric systems. Fusion can be categorized into three types. They are Feature Level Fusion, Score Level or Matching Level Fusion and Decision Level Fusion. Fusion types can be chosen based on the application requirements because each fusion has its own merits and demerits, so application decides which type of fusion is required to fulfill the task.

1.1.1 Feature Level Fusion
Fusion at feature level refers either the data itself or the feature sets originating from multiple sensors / sources are fused. There are several feature sources: (i) feature vectors acquired from different sensors based on a single biometric trait, (ii) feature vectors obtained from different entities based on a single biometric trait, like fingerprint feature vectors obtained from thumb and index finger, (iii)feature vectors obtained from multiple biometric traits[5].

1.1.2 Score Level or Matching Level Fusion
Score level fusion refers that the scores generated by different classifiers related to different biometrics are combined to match at this level. Fusion at score level can be approached in two different ways [4]. One is treated as a classification problem and the rest one is treated as an information combination problem. In the classification method, a feature vector is reconstructed using matching scores output by individual matchers. Then these feature vectors are classified into "Accept" (genuine user) or "Reject" (impostor). In the information combination approach, individual matching scores are combined to generate a single scalar score that is used to make final decision.

1.1.3 Decision Level Fusion
Decision level fusion means the final output of different classifiers are consolidated via techniques to make final decision. There are several fusion techniques are available at decision level fusion. For example, majority voting, Bayesian inference, weighted voting based on Dempater-Shafer theory, AND or OR logical rules, etc. However, there is lot of difficulties to achieve better results from feature level fusion in practice. The major difficulties are (i) feature spaces of different biometric trait features are unknown in most cases,

(ii) data sets at feature level may be incompatible, (iii) combining two feature vectors may lead to dimension redundancy as the substantial increase of the fusion feature vectors.

Table 1.1 Characteristic of Levels of Fusion [5]

Characteristic	Feature Level Fusion	Score Level Fusion	Decision Level Fusion
Amount of information	rich	moderate	poor
Difficulty of achievement	large	moderate	small
Efficiency	high	medium	low

The table 1.1 discusses the characteristics of levels of fusion. From the table 1.1 it is concluded that the amount of information is rich and efficiency is high for feature level fusion alone rest of the fusion levels are moderate and poor. To generate best cryptographic key amount of information to be rich and to achieve good result efficiency must be high. While considering the single biometric multiple unit difficulty of achievement would be too small. It is not required to employ different methods and algorithms. Time complexity and space complexity can be easily reduced by applying same method for biometric trait and feature vector dimension would be same.

This paper is organized as follows. In Section 2 presents the review of existing work in the literature and Section 3 discusses about fingerprint feature extraction process. Section 4 describes the generation of cryptographic keys. Section 5 discusses about security analysis of the proposed approach. Section 6 presents experimental results and Section 7 provides conclusion and suggestion for future work.

2. LITERATURE REVIEW

Hung-I Hsiao et al. [6] presented a new multiple chaos-based biometric image cryptosystem for fingerprint security. This encryption algorithm is constructed with four chaotic systems namely logistic map, HULA, Chebyshev map and APFM nonlinear adaptive filter. The advantage of the proposed scheme is that it possesses a large secret key space enough to empower the security strength to protect fingerprint image, which is enough to prevent any brute-force attacks.

K. Xi et al. [7] proposed an efficient bio-cryptographic security protocol designed for client/server authentication in current mobile computing environment, with a reasonable assumption that server is secure. In this protocol, fingerprint biometric trait is used in user verification, protected by a computationally efficient Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC). The fingerprint information is hidden in the feature vault which is the combination of genuine and chaff features.

Feature level fusion of fingerprint and iris is suggested by A.Jagadeesan et al. [8] for cryptographic key generation. Fingerprint and iris are preprocessed and values are generated and stored for fingerprint x and y coordinate values as two vectors and iris vice versa. With the help of permutation, shuffling values are interchanged finally cryptographic key is generated for encrypting the message.

To overcome server side attack Rajeswari Mukeshi et al. [9] proposed a system that user fingerprint template is divided into two or more shares using visual cryptographic technique followed by compression. One of these shares is stored into the server and the rest of the shares are given to the users. Only the two participants who possess these transparencies can reconstruct the biometric template by superimposition of shares. The approach solves two major problems related to fingerprint based automatic access control systems such as falsification and reduces the maintenance cost of the large fingerprint database.

Shin-Yan Chiou [10] presents a new secure cryptographic authentication method using biometric features. The proposed system combines the advantages of biometric identification and cryptographic techniques. Existing biometric recognition systems are enhanced with subsystems; it can simultaneously achieve the security of cryptographic technology and the error tolerance of biometric recognition. Author recommended that this method can be used for biometric data encryption, signatures, and other types of cryptographic computation. The method offers a high degree of security with protection against power analysis attacks, fault-based cryptanalysis, and replay attacks. Results are compared with existing protocols of biometric-based cryptographic key generation (BCKG), fuzzy extractors (FZ) and application to combine iris recognition and cryptography (ACIRC). This scheme offers error tolerance in biometric data matching.

Feature-level fusion framework for the design of multibiometric cryptosystems proposed by Abhishek nagar et al. [11] that simultaneously protects the multiple templates of a user using a single secure sketch. Fingerprint, face, Iris are taken into account and the functionalities of the modules are Embedding algorithm, fusion module and biometric cryptosystem. The feasibility of such a framework has been demonstrated using both fuzzy vault and fuzzy commitment using real multimodal database and virtual multimodal database. Comparing to real multimodal, virtual multimodal performs better.

2.1 Limitations of Existing System

Different biometric traits are taken into account it employs different types of sensors, algorithms, feature extraction and matching modules. Existing approaches incorporate complex algorithms and different processing procedures; either it increases time complexity or space complexity. In order to minimize complexity dual fingerprints fusion for cryptographic key generation is proposed in this paper.

3. FINGERPRINT FEATURE EXTRACTION PROCESS

Fingerprint acquisition is the first step in processing; with the help of sensor fingerprints are gathered from user for processing

Figure 3.1 depicts the overview of the Fingerprint Feature Extraction Process. Image Binarisation is the process of converting 8-bit gray image with 0-value for ridges and 1-value for furrows. After image Binarisation, ridges in the fingerprint are displayed with black while furrows are in white color.

Orientation flow estimation representation gives an intrinsic property of the fingerprint images and defines invariant coordinates for ridges and valleys in a local neighborhood.

The orientation field of a fingerprint image defines the local orientation of the ridges contained in the fingerprint. Orientation angle is represented by θ. Removal of unwanted background information and selecting the foreground information is the part of Region of Interest.

Ridge thinning converts the normal pixels into one pixel wide to make ease of operation. False minutiae are presented in the fingerprint due to over ink or less amount of ink in the sensor; it generates false minutiae which severely degrades and

significantly reduce recognition rate in order to achieve high success rate false minutiae to be removed from fingerprint. Spike, dot, island, bridge, hole, break, spur and ladder are the false minutiae types [12]. After removal of false minutiae, true minutiae sets are stored in the database.

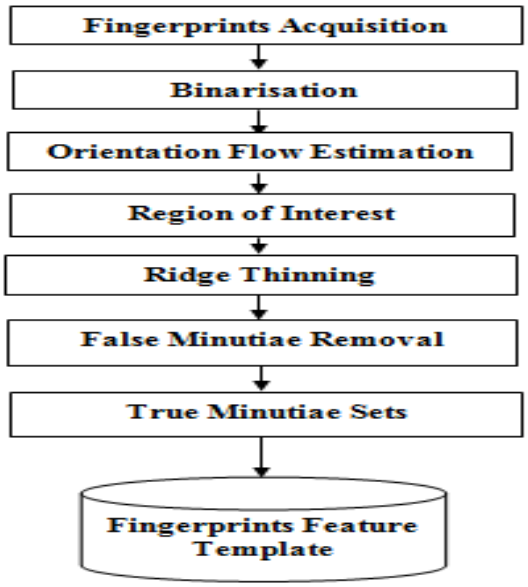

Figure 3.1 Overview of Fingerprint Acquisition and Feature Extraction Process

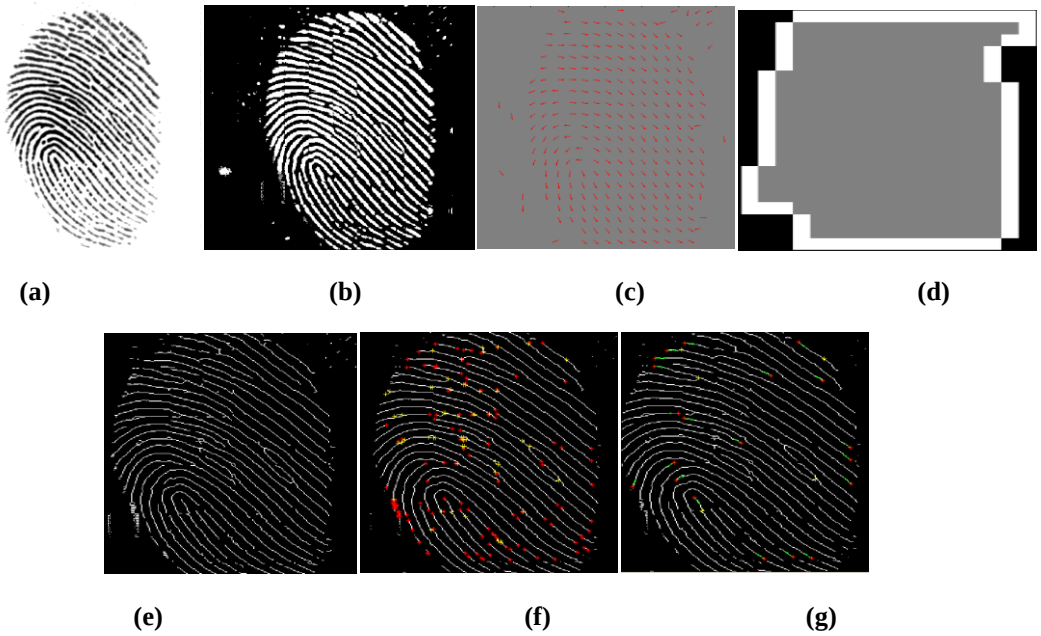

Figure 3.2 (a) Raw image (b) Image Binarisation (c) Orientation Flow Estimation (d) Region of Interest (e) Thinned Image

(f) Extracted minutiae points (g) True Minutiae points

Figure 3.2 depicts the corresponding output for the overview of fingerprint acquisition and feature extraction process steps mentioned in Figure 3.1 True minutiae points are saved in database for further operation.

4. CRYPTOGRAPHIC KEY GENERATION

The core of cryptography lies in the stability of cryptographic keys generated from uncertain biometrics. Message is encrypted and decrypted using dual fingerprint biometric cryptographic key. Encryption and decryption procedure is as follows.

4.1 Encryption

Encryption is the process of converting original message into unreadable form to protect from attackers. The true minutiae points of the fingerprints are stored in database as Fingerprint feature template; it is nothing but minutiae position (x, y co-ordinates).

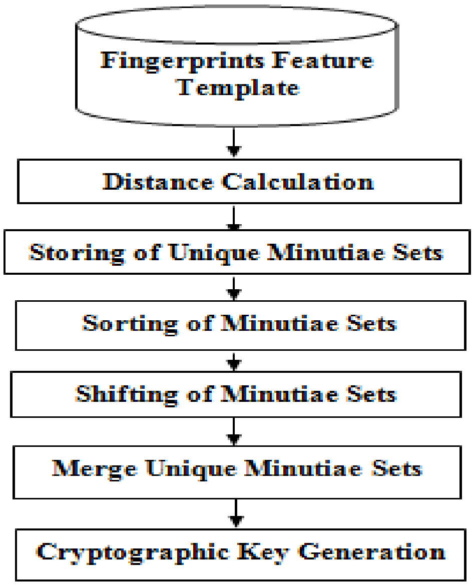

Figure 4.1 Cryptographic key Generation

Figure 4.1 describes the below steps to generate cryptographic key for secured communication. Let us consider two fingerprints of the same user for cryptographic key generation. Two fingerprints (FP_a and FP_b) are fetched from database and represented as FP_a = { FP1, FP2, FP3, ...FPm } and FP_b = { FP1, FP2, FP3, ...FPn }. Where FP1, FP2, FP3, ...FPm and FP1, FP2 ,FP3, ...FPn represents the fingerprint minutiae points with co-ordinates (x, y) for each set.

The distance D_M between two minutia points is defined as FP_i and FP_j are calculated using the following equation (4.1) suggested by karthik nandakumar et al. [13]

$$D_M(FP_i,\ FP_j) = \sqrt{(U_i - U_j)^2 + (V_i - V_j)^2} \qquad (4.1)$$

Where (U_i , V_i) , (U_j , V_j) are co-ordinates of points P_i and P_j respectively. Distance value is calculated for the minutiae points and unique values alone stored in two different arrays for two different fingerprints.

The distance value is represented by array D_a=[D1, D2, D3,…..Dm] and D_b=[D1, D2, D3,…..Dn]

After distance calculation values from the first array is sorted by ascending order and second array is sorted by descending order.

SortAsc[D_a] = [AscD1, AscD2, AscD3,…..AscDm]

SortDes[D_b] = [DesD1, DesD2, DesD3,…..DesDn]

Convert the sorted ascending order of array each value is shifted by one bit right and descending sorted order of array is one bit left in order to increase the complexity for the attacker and to improve the security for the user.

RS[D_a] = [RSD1, RSD2, RSD3,…..RSDm]

LS[D_b] = [LSD1, LSD2, LSD3,…..LSDm]

Finally the two matrixes are sorted and merged together to generate a cryptographic key.

$MergedD_x$ = RS[D_a] ∪ LS[D_b]

$MergedD_x$ alone taken into account for generating cryptographic key for secured communication. Below is the generated 256 bit cryptographic key by proposed approach.

11110001111111111110001111111011111110110111111111
11111001111110111111111110011111111111111100111001
10111101111111101111111011111111101111111111100111
11111111111111111111101111011111011111111011111001
11110111111100111111100111111001000111111011111110
111111

4.2 Decryption

Decryption is the inverse process of encryption. All the key values and steps that are used in this encryption technique are required to be known by the receiver for decryption of the message. So the key values and steps are conveyed to recipient in order to get original message from sender.

5. ANALYSIS OF SECURITY

Cryptographic key is generated using dual fingerprints fusion. Further, this proposed approach is analysed for its strength, features and performance using the following security measures.

5.1 Security measures of the Proposed Approach

Confidentiality: The privacy of the message is protected by this approach. Suppose if the attacker wants to derive the original message from the encrypted text, he/she needs the cryptographic key. The key can be obtained only by using the fingerprint biometric trait of the receiver. Even if attacker obtain fingerprint it is impossible to decrypt the message, because dual fingerprints are used for cryptographic key generation. Participants alone know which two fingerprints are considered for key derivation. So, it is computationally infeasible to get the key.

Integrity: In the proposed method, the recipient can verify whether the received message is the original one that was sent by the sender. If the attacker modifies the cipher text, the original plain text cannot be generated after decrypting with the key created by using receiver's biometric trait. By the property of one-way hash function, it is computationally impossible for the attacker to modify the cipher text.

5.2. Man in the Middle Attack

An attacker sits between the sender and the receiver and sniffs any information being sent between two ends is called man in the middle attack (MITM). Even though the attacker can get the cipher text he/she cannot view the original content since it is secured by using dual fingerprint based biometric cryptographic key.

5.3. Exhaustive Search Attack

If the hacker does not have any information regarding the solution space or key statistics information, he or she has to perform an exhaustive search in the entire key space. If the key space is very large, the expected number of guesses by exhaustive search is also very large i.e. a longer key is more secure under exhaustive search attack. In the proposed approach, since different fingerprints are used for key generation, computationally infeasible to get the key by this method.

5.4. Brute Force Attack

An attacker using trial-and-error method plan to obtain original information of the encrypted data. Even though attacker used to generate a large number of consecutive guesses as to the value of the desired data it is impossible to get the original text. Computationally infeasible to generate the original key by this method.

6. EXPERIMENTAL RESULTS

The table 6.1 discusses the analysis of the security parameters like Revocability, Security, Speed, Encryption, Decryption and Inherent Vulnerabilities. For experimentation, we have employed the fingerprint images obtained from publicly available database FVC2002 [14], which contains 40 different gray-scale fingers and 8 impressions of each finger (40x80=320 fingerprints). The images in DB1, DB2, DB3 and DB4 are 388x374, 296x560, 300x300, 288x384 and each fingerprint has a resolution of 500 dpi. DB1 is divided into two groups as 5 users in one group, like the entire fingerprint database has been divided and grouped. Experimental result reveals that proposed approach is secure, speed, reliable, revocable, encryption and decryption is faster and finally it is attack free.

Table 6.2 and 6.3 reveals the experimental results of the proposed approach. The metrics used for evaluation are False Acceptance Rate(FAR) and False Rejection Rate(FRR). The FRR is the frequency that an authorized person is rejected access.

Table 6.1 Security Parameters

Encryption Algorithm	Revocability	Security	Speed	Encryption and Decryption	Inherent Vulnerabilites
RSA	No	Least Secure	Slowest	Slower	Brute force and Oracle Attack
DES	No	Not secure enough	Slow	Moderate	Brute Force, Linear and differential cryptanalysis attack
3DES	No	Adequate Security	Very slow	Moderate	Brue Force Attack
Proposed Approach	Yes	Excellent Security	Fast	Faster	Attack Free

The resulted(FRR) is obtained from Equation (6.1). The FRR is calculated for true fingerprints and dual fingerprints.

$$FRR=\frac{1}{N}\sum_{n=1}^{100} FRR(n) \qquad (6.1)$$

Where $FRR(n) = \left[\frac{\text{Number of rejected verification attempts for a qualified person n}}{\text{Number of all verification attempts for a qualified person n}}\right]$

Table 6.2 FRR(%) for various users

No. of Users	FRR for true fingerprints	FRR for dual fingerprints cryptographic key generation (Proposed)
1-5	3.78	3.40
6-10	3.60	3.36
11-15	3.53	3.25
16-20	3.70	3.30
21-25	3.65	3.42
26-30	3.75	3.45
31-35	3.50	3.28
36-40	3.67	3.34

The FAR is the frequency that an unauthorized person is accepted as authorized. The resulted(FAR) is obtained from Equation (6.2). The FAR is calculated for true fingerprints and dual fingerprints.

$$FAR=\frac{1}{N}\sum_{n=1}^{100} FAR(n) \qquad (6.2)$$

Where $FAR(n) = \left[\frac{\text{Number of successful independent fraud attempts against a person n}}{\text{Number of all independent fraud attempts for a qualified person n}}\right]$

Table 6.3 FAR(%) for various users

No. of Users	FAR for true fingerprints	FAR for dual fingerprints cryptographic key generation (Proposed)
1-5	0.25	0.20
6-10	0.27	0.23
11-15	0.26	0.21
16-20	0.27	0.22
21-25	0.25	0.21
26-30	0.28	0.20
31-35	0.26	0.22
36-40	0.25	0.23

7. CONCLUSION

In this paper, we have attempted to derive a secure cryptographic key by incorporating dual fingerprints of human being, so as to provide better security. Feature level fusion of fingerprints is suggested for cryptographic key generation. Fingerprints are acquired, processed and finally extracted features are combined together to generate 256 bit cryptographic key. The experimental results have demonstrated the efficiency of the proposed approach to produce user-specific strong cryptographic keys. As a future work this may be extended with different databases or remote locations to store fingerprint biometric trait to achieve more security.

8. REFERENCES

[1] Colin Soutar, Danny Roberge , Alex Stoianov, Rene Gilroy, B.V.K. Vijaya Kumar, Biometric Encryption™, chapter 22 in ICSA Guide to Cryptography, McGraw-Hill (1999) pp.1-28.

[2] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain, Biometric Cryptosystems: Issues and Challenges Proceedings of the IEEE, Vol. 92, NO. 6, JUNE 2004, pp.948-960

[3] B.Raja Rao, Dr.E.V.V.Krishna Rao, S.V.Rama Rao,M.Rama mohan rao, Finger Print Parameter Based Cryptographic Key Generation, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 6, November- December 2012, pp.1598-1604.

[4] A.K. Jain, K. Nandakumar, A. Ross, Score normalization in multimodal biometric systems, In Pattern Recognition, pp. 2270 – 2285, 2005.

[5] Feifei CUI, Gongping YANG, Score Level Fusion of Fingerprint and Finger Vein Recognition, Journal of Computational Information Systems 7: 16 (2011), pp.5723-5731.

[6] Hung-I Hsiao, Junghsi Lee Fingerprint image cryptography based on multiple chaotic systems, Signal Processing113(2015) pp.169–181.

[7] Kai Xi, Tohari Ahmad, Fengling Han and Jiankun Hu, A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment, Security And Communication Networks, Security Comm. Networks (2010), Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.225

[8] A.Jagadeesan Dr. K.Duraiswamy, Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010, pp.296-305.

[9] Rajeswari Mukeshi, V.J.Subashini, Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique , IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30 - 31, 2012, pp.16-19.

[10] Shin-Yan Chiou, Secure Method for Biometric-Based Recognition with Integrated Cryptographic Functions, Hindawi Publishing Corporation, BioMed Research International, Volume 2013, Article ID 623815, http://dx.doi.org/10.1155/2013/623815 1-12.

[11] Abhishek Nagar, Karthik Nandakumar, AnilK. Jain Multibiometric Cryptosystems Based on Feature-Level Fusion, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, February 2012, pp.255-268.

[12] M. Tico and P. Kuosmanen, An Algorithm for Fingerprint Image Postprocessing, Proc. 34th Asilomar Conf. Signals, Systems and Computers, vol. 2, October 2000, pp. 1735-1739.

[13] Karthik Nandakumar, Anil K. Jain, Sharath Pankanti, Fingerprint-Based Fuzzy Vault: Implementation and Performance, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, December 2007, pp.744-757.

[14] FVC2002, http://bias.csr.unibo.it/fvc2002/, 2002.