ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Securing UniBiometric Template Using Fuzzy Vault Cryptosystem

[1]B. Sophia,[2] V. Sujitha,[3] Dr. D. Chitra,

PG Student, Department of CSE, P.A. College of Engineering and Technology, Pollachi, Tamilnadu, India[1]

Assistant Professor, Department of IT, P.A. College of Engineering and Technology, Pollachi, Tamilnadu, India[2]

Professor and HOD, Department of CSE, P.A. College of Engineering and Technology, Pollachi, Tamilnadu, India[3]

ABSTRACT: Biometric systems collect evidence from biometric trait of an individual and used to uniquely verify the individual with the distinguishing characteristics of the biometric trait. The greatest challenge in designing a biometric system is to ensure the storage of the biometric templates without compromising the security and privacy. Biometric Cryptosystems are used to ensure the security of the biometric templates of the user and reduce the risk of spoofing attacks and functional creep. The proposed system implements a fingerprint authentication framework with a template protection scheme using fuzzy vault biometric cryptosystem to secure the fingerprint templates. We propose a fully automatic implementation of the Fuzzy vault scheme based on Finger print Minutiae. The Cryptographic key value is calculated based on polynomial value of minutiae points (Extracted from finger image) and added chaff points. During Authentication Process, the Key value is calculated based on newly enrolled image and then verification is performed with Database image. To evaluate the performance of the system using FVC2004 fingerprint database and the implementation is done in MATLAB.

KEYWORDS: Biometric Cryptosystem, Fingerprint template, Fuzzy vault, Biometric Recognition, Fingerprint Minutiae.

I. INTRODUCTION

The biometrics is the study of physical or behavioral characteristics used for the identification of a person. Biometric recognition refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Fingerprint authentication systems are the most widely used biometric technology. Security of the stored biometric templates is one of the major issues to be addressed during the design of the biometric system design.

Template protection schemes are broadly classified into two main categories namely template transformation approach and biometric cryptosystem as shown Figure 1. In template transformation approach a transformation scheme is applied to the biometric template and only the transformed template is stored in the database. The template transformation scheme can be further categorized into salting and noninvertible transformation scheme depending on the transformation function characteristics. In Salting, if an adversary gains access to the key and the transformed template, he can recover the original biometric template or a close approximation of it so the transformation function is invertible. Whereas in noninvertible transformation scheme, a one way function is applied on the template and it is computationally hard to invert a transformed template even if the key is known.

In biometric cryptosystem, some public information called helper data of the biometric template is stored. While the helper data does not reveal any significant information about the original biometric template, it is needed to extract a cryptographic key from the query biometric features.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

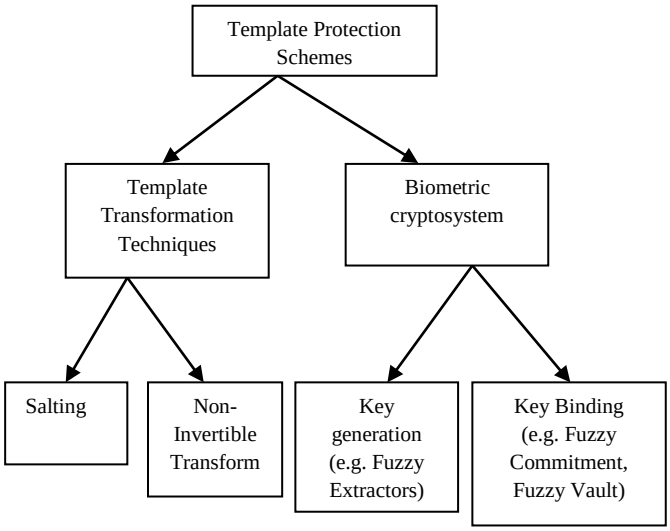

Figure1 Classification of Template Protection Schemes

The biometric cryptosystems can be further classified into key generating and key binding biometric cryptosystems depending on how the helper data is obtained. In key generating biometric cryptosystem, the helper data is derived only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features. Whereas in key binding biometric cryptosystem the helper data is obtained by binding a key that is independent of the biometric features with the biometric template [3, 4]. Fuzzy vault is an example of key binding biometric cryptosystem.

The rest of the paper is organized as follows: a brief survey of related work is discussed in Section II and Section III describes the proposed methodology. Experimental results and analysis is given in Section IV and finally, the paper is concluded in Section V.

II. RELATED WORKS

Fingerprint authentication is a very effective technique to replace traditional passwords or pin codes. The main challenge for fingerprint authentication systems is to provide a secure storage of the reference template. Embedded devices are vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be investigated. Combining biometrics and cryptographic technique called the fuzzy commitment scheme has been proposed for biometric authentication [1].The scheme integrates well-known error-control coding methods and cryptographic techniques to construct a novel type of cryptographic system. A reasonable close witness can be accepted to decrypt the commitment instead of the need for an exact, unique decryption key so it possible for protecting the biometric data using traditional cryptographic techniques. The fuzzy commitment scheme does not have the property of order invariance so any elements missing or added will result in a failure of the matching.

To overcome this problem, [5] proposed a new version, which possesses the advantage of order-invariance. At the same time, the authors suggested that one of the important applications of the fuzzy commitment is to secure biometric systems. The system did not include practical implementation of the fuzzy vault.

The method employed in [13] incorporates the fuzzy vault scheme on a secure smartcard system. The fingerprint vault construction is based on the assumption that the fingerprint features are extracted and aligned in a black box. Multiple minutiae locations are used as elements of locking set. This method assumed the pre-alignment of fingerprints minutiae locations in the vault and the query.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Yang and Verbauwhede [12] introduced alignment in fuzzy vault system for fingerprints by proposing the use of reference minutiae, which are extracted during vault encoding and decoding. The alignment is established if these two references are same and thus the origins of coordinate frames to be used.

Hao, Anderson, and Daugman [7] implemented the basic idea of fuzzy commitment for IrisCode features by using Reed-Solomon code to correct errors at the block level and Hadamard code to correct random errors at the binary level. This implementation actually adds a second authentication factor password or a token and leads to promising experimental results.

In [15], a method was proposed for fuzzy vault for fingerprints using simple translation and rotation for alignment because reference minutiae may not be same in number or in position during enrolment and verification. This algorithm used cyclic redundancy check and Lagrange interpolation instead of Reed Solomon decoding. The main drawback of Reed Solomon coding scheme are that the input data set only contain integer within limited range and vault may leak some information because it is stored without transformation.

In [14], the template is stored after transforming to other set of coordinates to provide security but it then becomes difficult to align query with stored template. With the use of helper data, the stored template in transformed domain is used for alignment and comparison with the query data. It does not leak minutiae information while aligning the query template.

Karthik Nandkumar and Anil K Jain [10] further improved fuzzy vault by using minutiae matcher to compensate for non-linear distortion in fingerprints and considering orientation in addition to the location of the minutiae point. They also used local image quality index estimated from fingerprint to select the most reliable minutiae.

Abhishek Nagar et al [2] proposed a technique of evaluating the polynomial using helper data using encryption. Orientation and ridge frequency information in minutiae neighborhoods are the two attributes used for minutiae description for securing polynomial evaluations. Authentication system is simulated to evaluate template security of the proposed technique.

The research of Jason Jeffers and Arathi Arakala [9] is directed to methods of realizing the fuzzy vault for the fingerprint biometric using minutiae points described in a translation and rotation invariant manner. The variation in different samples of the same biometric makes it difficult to replace passwords directly with biometrics in a cryptographic scheme.

Hoi Ting Poon and Ali Miri [8] discussed that CRC decoders are most commonly used decoders in fuzzy vault but they have some flaws. They proposed a new decoder which is based on Euclidean algorithm and origins from Reed Solomon (RS) codes. This new scheme has considerably decreased the decoding time as compared to CRC decoders and also maintains security.

III. PROPOSED FRAEWORK FOR BIOMETRIC CRYPTOSYSTEM

In the proposed system, a fingerprint authentication system framework is implemented with a biometric cryptosystem scheme for securing the fingerprint templates. The proposed system combines biometrics and cryptography by using a key-binding biometric cryptosystem known as fuzzy vault.

The fuzzy vault is a cryptographic construct with a key to encode a polynomial function and the polynomial projections for the fingerprint minutiae points are generated for the fingerprint template. Additional chaff points are added randomly to enhance the security of the secure sketch. The proposed scheme ensures the protection of the fingerprint template and also the key stored as the secure sketch in the fuzzy vault cryptosystem.

The following six modules are the main components of our cryptosystem:

- Data Preprocessing

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

- Extraction of the fingerprint Minutiae point locations
- Constructing the fingerprint fuzzy vault
- Vault Encoding and Decoding
- Vault Unlocking
  - Matching process and retrieving the key

A. PREPROCESSING

The Fingerprint image is preprocessed before the extraction of the feature points. The preprocessing includes the following steps:

1. Binarization

The enrolled fingerprint template is Binarized with a threshold value.

$$I_B[i,j] = \begin{cases} 1 & if\ X_{i,j} > t_{i,j} \\ 0 & if\ X_{i,j} < t_{i,j} \end{cases} \quad (1)$$

2. Thining

The morphological operation of thinning is done to extract the fingerprint and to remove the unwanted noise.

Figure 2 shows the Preprocessing of the enrolled fingerprint template. The process is done to for all the enrolled fingerprint templates.

Figure2 Preprocessing of Enrolled Fingerprint Template

B. FEATURE EXTRACTION

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns.

The major Minutia features of fingerprint ridges are ridge ending, ridge bifurcation, and short ridge or dot. The ridge ending denotes the point at which a ridge terminates. Bifurcations denote the points at which a single ridge splits into two ridges. Short ridges or dots denote ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Given the template fingerprint image T, we first obtain the template minutiae set

$$M^T = \{m_i^T\}_{i=1}^{N^T} \quad (2)$$

where N^T is the number of minutiae in T.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Figure 3 shows the minutiae feature points extracted namely the ridge endings and ridge bifurcation points.

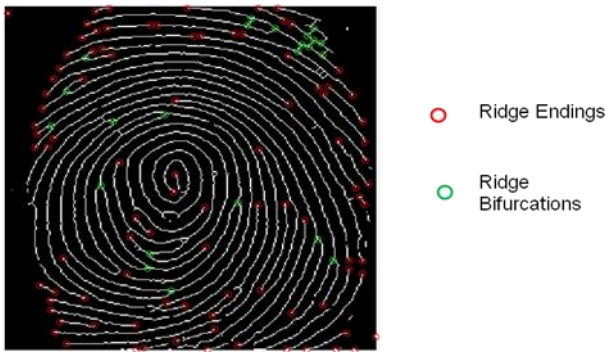

Figure3 Feature Extraction

The false Minutiae points are removed and the only well-separated minutiae points are selected so that the minimum distance between any two selected minutia points is greater than a threshold δ1.

$$D_M(m_i, m_j) = \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2} + \beta_M \Delta(\theta_i, \theta_j) \quad (3)$$

where

$$\Delta(\theta_i, \theta_j) = \min(|\theta_i - \theta_j|, 360 - |\theta_i - \theta_j|) \quad (4)$$

and β_M is the weight assigned to the orientation attribute.

C. FUZZY VAULT CONSTRUCTION

Fuzzy vault is useful for securing point-set based biometric features such as fingerprint minutiae.

Let $M^T = \{m_1, m_2, ..., m_r\}$ denote a biometric template consisting of a set of r minutiae point locations. In order to secure M^T, a cryptographic key k_c is used and this key is transformed into coefficients of polynomial P of degree k. All the elements in M^T are then evaluated on this polynomial to obtain the set $\{P(x_i)\}^r_{i=1}$.The set of points $\{(m_i, P(m_i))\}^r_{i==1}$ is then secured by hiding them among a large set of q randomly generated chaff points $\{(aj, bj)\}^q_{j=1}$ that do not lie on the polynomial P. The set of genuine and chaff points along with their polynomial evaluations constitute the sketch or vault y_c.

In the authentication stage, if the query biometric set M^Q is sufficiently close to M^T, the polynomial P can be successfully reconstructed by identifying the genuine points in y_c that are associated with M^T. For successful reconstruction of P of degree k, a minimum of (k + 1) genuine points need to be identified from y_c.

$$\{(aj, bj)\}^r_{q=1}$$

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

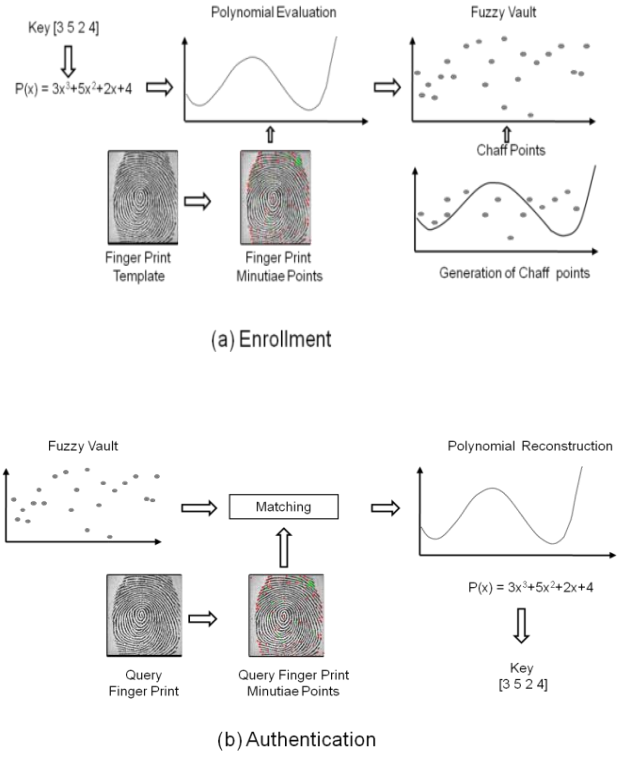

Figure4 Fingerprint Fuzzy Vault Framework

D. VAULT ENCODING

All operations in this algorithm are carried out over a field *F*. The algorithm has three parameters, namely, *n*, *r* and *s*. Here, *r* depends on the number of features that can be extracted from a user's biometric template (e.g., number of minutia points in the user's fingerprint). The parameter *s* represents the number of chaff points that are added to the vault and this parameter influences the security of the fuzzy vault construction. If no chaff points are added, the vault leaks the information about the template and the secret. As more chaff points are added, the security of the vault increases. Figure5 shows the fingerprint fuzzy vault encoding process. The degree of the polynomial, *n*, controls the tolerance of the system to errors in the biometric data during decoding.

The vault encoding consists of the following steps

1. Create a polynomial by encoding a Key to the coefficients of the Polynomial
2. Project locking Elements to the Polynomial and add the Chaff points
3. Construction of the fingerprint fuzzy vault with the locking set and chaff points

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

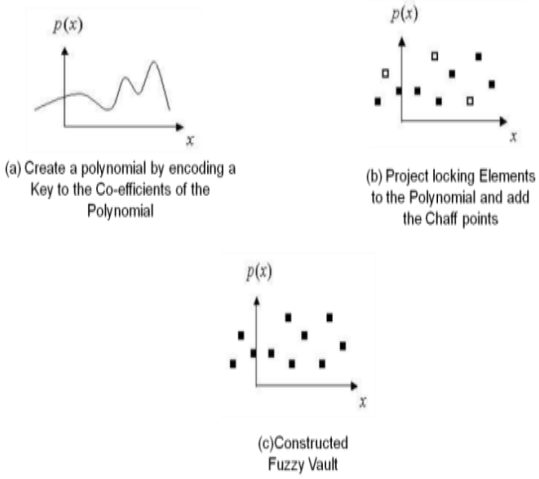

Figure5 Fingerprint fuzzy vault encoding

E.VAULT DECODING

The vault can be unlocked and the key can be retrieved only when there is sufficient match between the query image and the original image.

The vault Decoding consists of the following steps

Step1: Extract the Minutiae points from the Query Fingerprint Template Q. The points form an unordered set B.

Step2: Compute the polynomial projections, P(X), for the elements of B.

Step3: Compare the points of the sets in the vault and the Query template.

Step4: If the sets overlap substantially then the vault is unlocked and the key is retrieved by the user.

IV. EXPERIMENT AL RESULT AND ANALYSTS

In Proposed system, fingerprint image is used as input biometric feature. The experiment is conceded out to generate cryptographic key for Encoding and Decoding using Fuzzy vault method. We detect the similarities between the keys generated from different positions of identical fingerprint image. In this method examine the strength of the key with respect to the impostor key which is generated from impostor's fingerprint image.

Fingerprint from fingerprint database FVC2004 is used as input fingerprint in our experiment. The FVC2004 database consists of four datasets like DBl, DB2, DB3 and DB4. Fingerprints of DB4 dataset are synthetic fingerprint but remaining datasets consist of real fingerprints. Each dataset consists of 800 fingerprints of 100 persons with 8 samples of each person.

In our method, the Fingerprint template image for each subject is enrolled in the database. Initially, the preprocessing is done and the fingerprint minutiae points are extracted. The features extracted from the preprocessed image. The green points show the ridge bifurcations and red shows ridge endings. Then the validation features extracted from the preprocessed image.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Figure6 Fingerprint Minutiae Locations Extraction

The fuzzy vault cryptosystem is constructed with a polynomial function that is encoded from a key and the extracted minutiae points are projected using the polynomial function (Fig 7). The random chaff points should also be added with the extracted key points. The vault consists of randomly added chaff points in addition to the projected points to ensure security of the fingerprint template. Finally, the Key Points should be stored in database.

During authentication, the query finger print image enrolled and then compared with the stored template. The vault can be unlocked and the key can be retrieved only when there is sufficient match between the query image and the stored image.

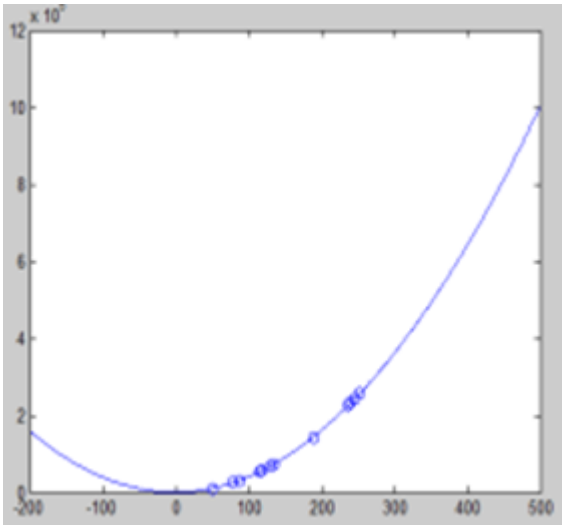

Figure7 Polynomial Projections for Extracted Minutiae Points

V. CONCLUSION AND FUTURE SCOPE

The proposed system Securing fingerprint templates using Fuzzy Vault Cryptosystem, incorporates a fuzzy vault scheme to implement the biometric cryptosystem approach for securing the fingerprint templates. The proposed system secures the template using a key-binding cryptosystem called the fuzzy vault. The fuzzy vault is a cryptographic construct with a key to encode a polynomial function and the polynomial projections for the minutiae points are generated for the fingerprint template. Additional chaff points added randomly to the polynomial projections enhance the security of the secure sketch. The proposed scheme ensures the protection of the fingerprint template and also the key stored as the secure sketch in the fuzzy vault cryptosystem.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

In future, the biometric cryptosystem can be extended to multimodal biometric systems to include other modalities like iris, face and palm print for ensuring the security of the multiple biometric templates. It can also be extended to include algorithms to incorporate the different representations of the acquired biometric templates.

REFERENCES

[1]. A. Juels and M. Wattenberg, "A fuzzy commitment scheme" ,6th ACM Conf. on Computer and Communications Security, pp. 28–36, 1999.
[2]. Abhishek Nagar, Karthik Nandakumar and Anil K. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors," in International Conference for Pattern Recognition, Tampa, pp. 1-4, 2008
[3]. Anil K. Jain, Arun Ross and Patrick Flynn, "Handbook of Biometrics", pp. 1-10, 2008.
[4]. Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security," in Journal on Advances in Signal Processing, Michigan State University; pp. 1-17, 2007.
[5]. Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme," in IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408, 2002.
[6]. Cengiz Orencik, "FuzzyVault Scheme for Fingerprint Verification: Implementation, Analysis and Improvements", Sabanci University, pp. 1-50, 2008.
[7]. F. Hao, R. Anderson, and J. Daugman, "Combining Cryptography with Biometrics Effectively", IEEE Transactions on Computers, pp.1081–1088, 2006.
[8]. Hoi Ting Poon and Ali Miri, "On Efficient Decoding of the Fuzzy Vault Scheme", in 11th International Conference on Information Sciences, Signal Processing and their Applications: Main Tracks, pp.454-459, 2012
[9]. Jason Jeffers and Arathi Arakala, "Fingerprint Alignment for a Minutiae-Based Fuzzy Vault," in Biometric Symposium IEEE, pp. 1-6, 2007
[10]. Karthik Nandakumar, Anil K. Jain and Sharath Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," IEEE Transition for Information Forensics & Security, pp. 744-757, 2007.
[11]. Mohammad Khalil-Hani, Rabia Bakhteri, "Securing Cryptographic Key with Fuzzy Vault based on a new Chaff Generation Method," in proceedings of IEEE, pp. 259-265, 2010.
[12]. S Yang and I Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme" in Proceedings of IEEE ICASSP, Philadelphia, PA, Vol. 5, pp. 609-612, , 2005
[13]. T Clancy, D Lin and N Kiyavash, " Secure smartcard-based fingerprint authentication" in Proceedings of ACM SIGMM Workshop on Biometric Methods and Applications, Berkley, CA, pp. 45-52, 2003.
[14]. Umut Uludag and Anil K. Jain, "Securing fingerprint template: Fuzzy vault with Helper Data," in Proceedings of CVPR Workshop Privacy Research Vision, New York, pp. 163, 2006.
[15]. Umut Uludag, Sharath Pankanti and Anil K. Jain, "Fuzzy vault for fingerprints," in Proceedings of Audio- and Video- based Biometric Person Authentication, Rye Town, NY, 2005
[16]. W. Stallings, Cryptography and Network Security: Principles and Practices, 3. Ed., Prentice Hall, 2003.