Secure Communication in BAN using Modified Fuzzy Vault Scheme

R.Rekha
Assistant Professor,
Department of IT,
PSG College of Technology,
Coimbatore, India

R.Vidhyapriya, Ph.D
Professor,
Department of IT,
PSG College of Technology,
Coimbatore, India

R.Geetha Rajakumari
PG Scholar,
Department of IT,
PSG College of Technology,
Coimbatore, India

ABSTRACT

Wireless Body Sensor Network (WBSN) is an emerging technology in the area of telemedicine. It helps doctors to remotely monitor the health condition of patients. The success of usage of WBSNs for health care monitoring relies mainly on the security provided to the private information collected by the sensors. Security depends on key agreement scheme used. This paper aims at developing a fuzzy based key agreement scheme that uses ECG signal to protect the symmetric key to be exchanged. Here the correlation attack is overcome by using two different polynomial of different order due to which the integrity property of system is preserved. The effectiveness of the proposed scheme is to improve the performance of the system by overcoming correlation and collusion attacks. It also aims at minimizing False Acceptance Rate (FAR) and False Rejection Rate (FRR).

General Terms

Body Area Networks, secure communication, security, False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Keywords

Physiological signals, key agreement, fuzzy vault scheme.

1. INTRODUCTION

The rapid growth of telecommunication has contributed much for remote healthcare monitoring of elderly people and patients by the doctors. A number of intelligent sensors on human body form a Wireless Body Sensor Network. These sensors will monitor the health conditions of that body and collect information regarding the physiological changes, and transmit them wirelessly to an external medical information system immediately. This is done through a central control unit which may be placed nearer to or on the same body. If the doctor identifies an emergency situation, then appropriate actions can be taken. Unlike conventional sensor networks, these networks work with sensitive medical data. Hence security requirements are crucial in these networks.

In a broad spectrum, cryptography is used to achieve secure communication. The level of security provided by cryptographic algorithms depends mainly on the key and key distribution scheme used. Complex key distribution schemes cannot be used in WBSNs due to the following constraints of biosensors like ,

- Low power
- Limited memory
- Low computation capability

Because of these constraints, WBSNs should try to use the already available resources like physiological signals for key agreement.

In WBSNs, it is assumed that the sensor nodes are either implanted in the body or placed on the surface of human body. Hence it is not possible to physically capture the medical sensors without the knowledge of the persons on whom sensors are deployed. But there is a chance for an attacker to steal the keying materials contained in the node, if the node on the body surface is lost. Moreover, sensors on same body communicate with each other and also with the control unit wirelessly. Hence there may be chance of passive attacks, like monitoring of information exchanged or eavesdropping of medical data, which affects secrecy of patient's health details. Active attacks like modification of information sent to the receiver may lead to life threatening situation.

A good key distribution technique should provide the following security requirements.

- Data confidentiality
- Data availability
- Data authenticity
- Data integrity

In order to satisfy these security requirements, key used for encryption/decryption should meet the design goals like long and random keys, time variance nature, universally measurable and distinctiveness.

2. RELATED WORK

Krishna K. Venkatasubramanian [1], has presented a methodology which performs Usable and Secure Key Agreement Scheme for Body Area Networks using PSKA. This paper presents Physiological Signal based Key Agreement (PSKA), a scheme for enabling secure inter-sensor communication within a BAN in a usable (plug-n-play, transparent) manner. PSKA allows neighboring nodes in a BAN to agree to a symmetric shared cryptographic key, in an authenticated manner, using physiological signals obtained from the subject. No initialization or pre-deployment is required; simply deploying sensors in BAN is enough to make them communicate securely.

Juel and Sudan [2] proposed the Fuzzy Vault scheme. By characterizing the key as a set of symbols instead of a sequence and combining them with the proper error correction code, the scheme achieves the property of order-invariance. Recognizing its potential as a replacement for key release based biometrics systems, several researchers [3, 4] and [5] have already provided implementations of the Fuzzy Vault scheme. Studies have also emerged identifying potential flaws in chaff point placements [6,7] and susceptibility to brute-force attack [8] in fingerprint applications. To improve the security of the scheme, some have proposed techniques such as key encapsulation [9] and the addition of a password [10].

3. PROPOSED SYSTEM

Proposed system with wavelet based decomposition is shown in figure 1.

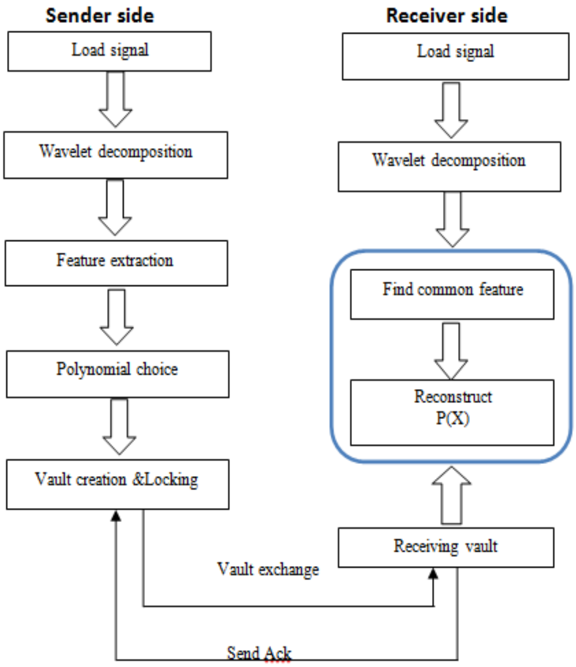


Fig 1: System Flow

3.1 Feature Extraction

Both the sender and the receiver obtain physiological signal based features. Then the signal is processed into small wave for more accurate analysis of wavelet, for that multi-level decomposition procedure is applied. In the figure 2, 'h' is low-pass filter, 'g' is high-pass filter, '↓2 'is down sampling.

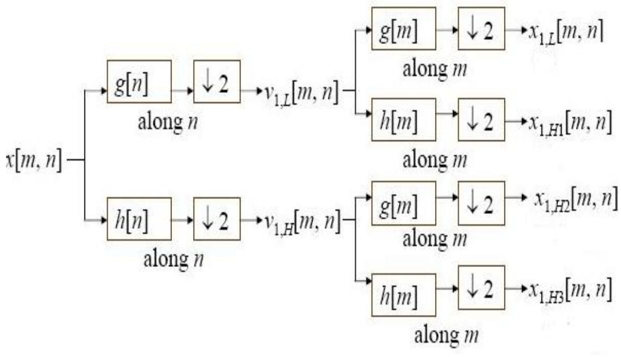


Fig 2: Multi-level decomposition

3.1.1 Daubechies wavelets

Daubechies wavelets are a family of wavelets that form an orthonormal basis via a multi-resolution analysis and are optimal in a certain sense. There are two properties of a mother wavelet:

- A minimal, compact support: The smaller the support of the wavelet is the less of the signal it picks up in a certain wavelet coefficient.
- Vanishing moments: When a wavelet is orthogonal to the polynomials 1, t,t2,...,tn, and we approximate the signal f on the support of the wavelet with its Taylor series, then the wavelet will ignore the first terms of the Taylor series. The better the signal is approximated by its Taylor series, the smaller the wavelet coefficients.

For a wavelet these two properties are not independent.For a given number of vanishing moments, there is a minimum, non zero length of the support of the mother wavelet. This is a famous theorem by Ingrid Daubechies. The Daubechies wavelets are optimal in the sense that they have the minimal support for a prescribed number of vanishing moments.

3.2 Fuzzy Vault Creation

Sender

1. Assume that k denote the secret to be locked using set A= {a1, a2, a3…an} available in sender.

2. Select a single variable polynomial p with degree d and embed the secret k on its coefficients.

3. Treating the elements of set A as distinct coordinate values of the polynomial, evaluate the polynomial p on the elements of A and compute the set V = {ai, p(ai)} , i=1 to n.

4. Create a number of random chaff points F that do not lie on the polynomial p. (i.e.) F = {fj,tj} , where fj does not belong to set A , tj p (tj) and j=1 to m.

5. The entire point's i.e. valid points and chaff points constitute the vault S that is sent to the receiver.

3.2.1 Chaff Point Generation

The security of the fuzzy vault scheme depends on the number of additional chaff points added along with the valid points. These chaff points conceal the valid points from the hackers. Moreover, the chaff points are selected in such a way that they also lie in the same range as that of valid points. For example, if A can have any value between 0 to 256, then F can also be within the same range. Interval value calculated using template is checked and random chaff points are placed apart from that interval.

Receiver

i. Set B = {b1, b2, b3…..bn } is the feature vector generated at the receiver and it substantially matches with set A.

ii. Compute a set M, with the help of received vault and elements of B, such that M = {(b, c)|(b, c) S and b B}.

iii. With the set M, the receiver then tries to compute the actual polynomial generated at the sender.

To a hacker, it is very difficult to guess the valid points from the vault received and hence difficult to reconstruct the actual polynomial. To overcome correlation attack here polynomial of different order are considered and validation is done between these polynomial outcome among sender and receiver values.

4. ALGORITHM OF THE PROPOSED SYSTEM

Sender side algorithm

Step: 1 Load ECG signal.

Step: 2 Append 100 zeros before and after the signal to remove the possibility of window crossing the signal boundaries while looking for peak locations.

Step: 3 Perform wavelet decomposition.

Step: 4 Extract the Coefficients after the transform.

Step: 5 Select Polynomial, where the value of the coefficients are selected randomly.

Step: 6 Select a different order polynomial as before and form the vault to overcome correlation attack.

Step: 7 The polynomial and feature vector are available.The sender now creates the fuzzy vault, by computing the set and $1 \leq i \leq N$. It also computes a much larger set of M random chaff points of the form C = {cj, dj}, where cj not equal to Fs, dj not equal to p(cj), and $1 \leq j \leq M$.

Step: 8 The sender communicates the vault R to the receiver using the following message: Sender → Receiver :IDs, IDr, R, No,MAC(Key, R|No|IDs). Here, IDs and IDr are the ids of the sender and receiver, respectively, No is a nonce (unique random number) for transaction freshness. MAC is a message authentication code (e.g. HMAC-SHA1);and, the key (Key) used is the one that is being locked in the vault.

Receiver side algorithm

Step: 1 Load ECG signal.

Step: 2 Append 100 zeros before and after the signal to remove the possibility of window crossing the signal boundaries while looking for peak locations.

Step: 3 Perform wavelet decomposition.

Step: 4 Extract the Coefficients after the transform.

Step: 5 Select Polynomial, where the value of the coefficients are selected randomly.

Step: 6 For the receiver to be successfully able to unlock the vault, the condition |Q| > v should hold. It then takes v + 1 point (from Q) at a time and tries to unlock the vault. The coefficients of the resulting polynomial are then used to verify the MAC.This not only confirms the correctness of the unlocking process, but also authenticates the sender to the receiver, confirms that the sender is on the same BAN as the receiver.

Step: 7 If unlocking was successful, the receiver then sends a reply back to the sender to inform it of its correct unlocking of the vault using the following message: Receiver → Sender : MAC(Key, No|IDs|IDr).

5. IMPLEMENTATION OF PROPOSED SYSTEM

Both, sender and receiver nodes capture ECG signals simultaneously for a period of about 4s. Experimentation is done using signals obtained from MIT-BIT Arrhythmia database of Physionet. Captured signals are sampled at sampling rate of 60 Hz.Figure 3 shows the original ECG signal of the Person. The original ECG signal is processed into small waves using multi-level decomposition as shown in Fig.4. Multi-level decomposition of wavelet is done using matlab command wavedec().

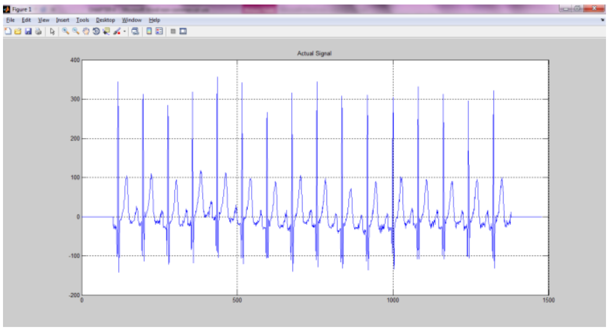


Fig 3: Original ECG signal of the Person

[C,L] = wavedec(X,N,'wname') returns the wavelet decomposition of the signal X at level N, using 'wname'. N must be a strictly positive integer. The output decomposition structure contains the wavelet decomposition vector C and the bookkeeping vector L. The structure is organized as in this Figure 5 into level-8 decomposition.

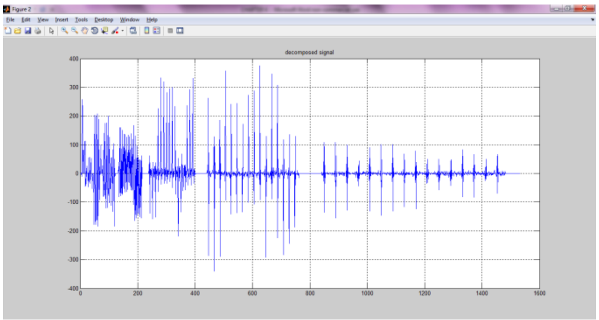


Fig 4: Decomposed signal

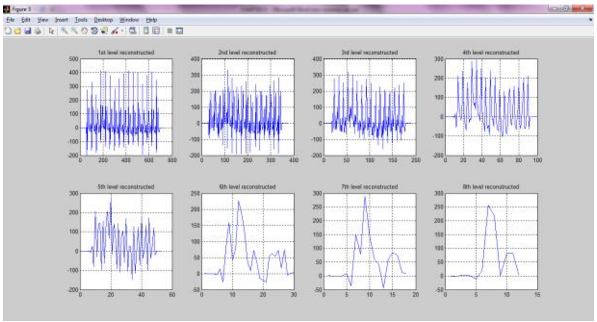


Fig 5: Level-8 decomposed signals

These features are evaluated on the polynomial and the vault is created by the sender. Fig.6 shows the vault in which it contains 2 sets of features derived from two different order polynomial. The main drawback of the existing system is that sometimes the set vault values matches with other signal which increase FAR .To overcome this two set of features are used. Vault of the proposed system is shown in Fig 7, where the two set polynomial values are differentiated using red and green markers.

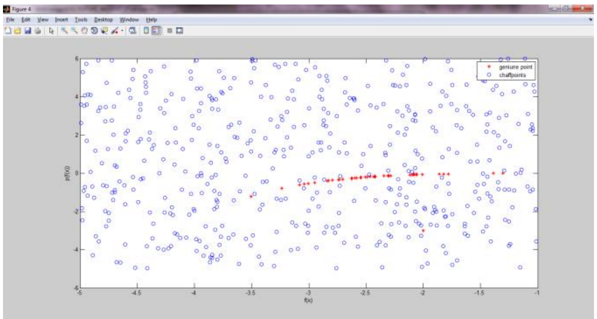


Fig 6: Vault locking in Existing system

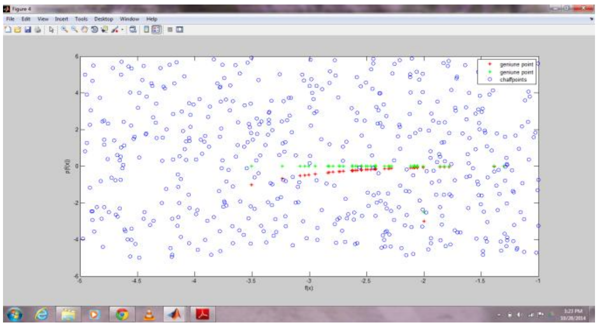
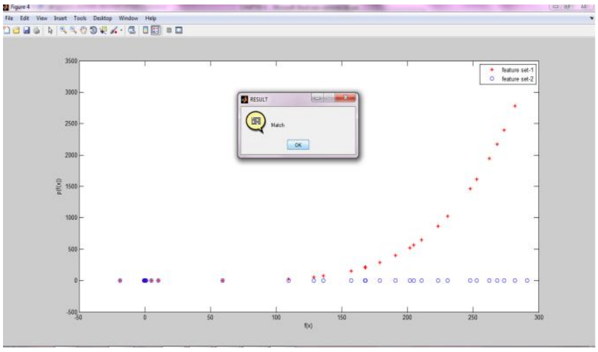


Fig 7: Vault locking in proposed system

Then the vault is exchanged to receiver and there the validation process is carried out using MAC algorithm to overcome the integrity attack. Then from the set of features genuine point are classified and the result is declared as shown in the Fig 8.


RESULT

Match

Fig 8: Vault Acknowledgement

6. CORRELATION ATTACK

PSKA depends upon the high degree of correlation between loosely synchronized physiological signals of the same subject to enable key agreement between sensors deployed on a subject. Coherence is a measure of the cross correlation between the coefficients of two signals. The vault created by a sensor in one BAN when unlocked by another sensor located on another subject from its measurements can cause correlation attack. Therefore it is necessary to make sure the number of common features for sensors on the same subject be “significantly” more than the number of common features for sensors on the different subject. But such differentiation increase time complexity.So to overcome that, from two sets of features, validation and verification is carried out in this proposed system. The below figure 9 shows vault of two different individual person’s ECG signal where the signal still has overlap to each other which is overcome by using two different polynomial order generated features.

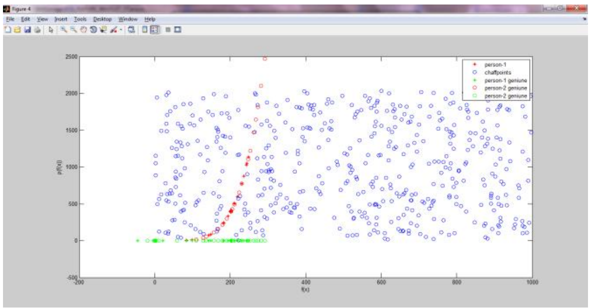


Fig 9: Vaults generated from 2 person’s ECG signal

7. PERFORMANCE EVALUATION

In the existing method Fast Fourier Transform is used in feature extraction process. This is a method to calculate the discrete Fourier transform and it’s inverse. It breaks down a signal into sinusoids of different frequencies transforms from time domain to frequency domain, whereas in proposed system the feature is extracted using Wavelet decomposition. It is one of the methods of the time-frequency-transformations. It decomposes the signals into different frequency ranges and allows extraction of features relating to quality. The wavelet transform is easy and faster than FFT.

Long and Random Keys: The keys to be agreed upon are generated by the sender in the form of polynomial coefficients using a pseudorandom number generator. The length and randomness of the keys agreed can therefore be ensured.

Performance Evaluation: The performance of the system is evaluated based on FAR, FRR and EER. The threshold depending fraction of the falsely accepted patterns divided by the number of all impostor patterns is called False Acceptance Rate (FAR). The fraction of the number of rejected client patterns divided by the total number of client patterns is called False Rejection Rate (FRR). The value of the FAR and the FRR at this point, which is of course the same for both of them, is called the Equal Error Rate (EER).Below chart shows the False Acceptance Rate (FAR) and False Rejection Rate (FRR) of 25 patient’s features with respect to order of polynomial.

From the graph it is inferred that for higher order polynomial, the FAR is nearly equal to zero and the FRR increases. Hence this significant result of proposed method results in better performance efficiency of the system than the existing method. Hence validating some other point as genuine is minimized when the higher order of polynomial is chosen.

The performance evaluation of proposed system is shown in figures 10 and 11. Fig 12 and Fig 13 shows the performance evaluation based on FAR rate and FRR rate of existing system.When the order of the polynomial is increased,FAR is decreased.

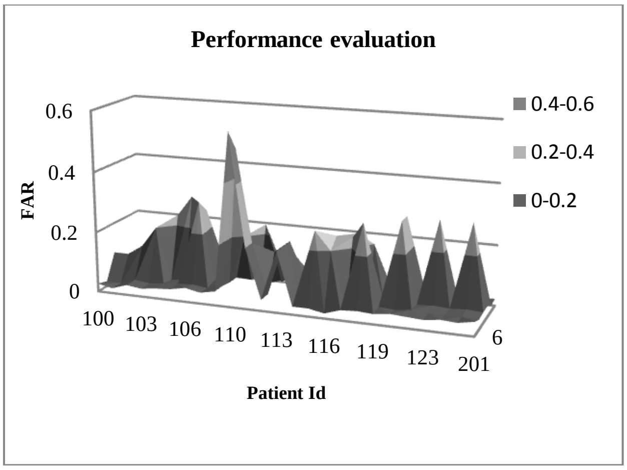


Fig 10: Proposed system-FAR

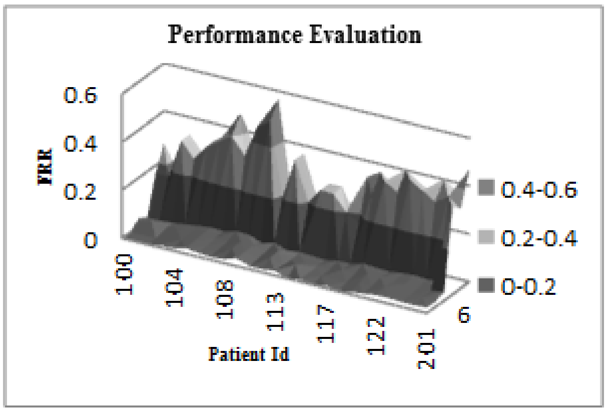


Fig 11: Proposed system-FRR

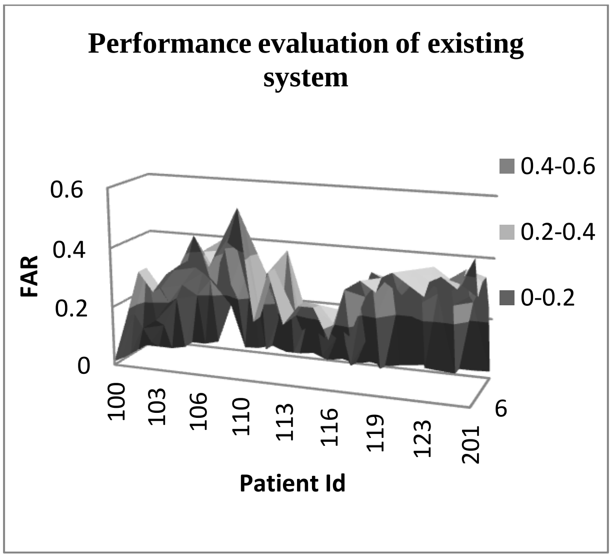


Fig 12: Existing system-FAR

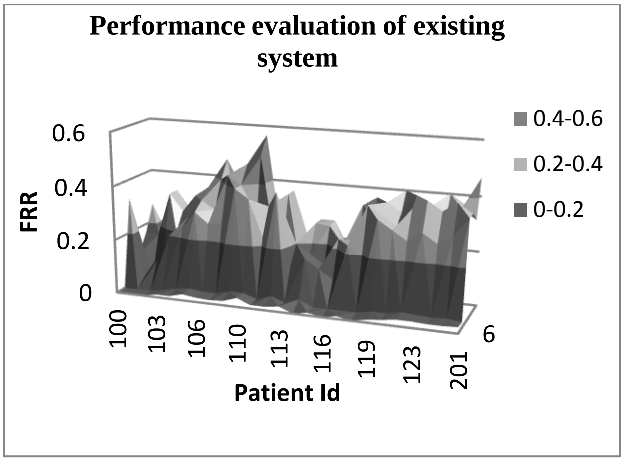


Fig 13: Existing system-FRR

8. CONCLUSION

The proposed system provides a modified fuzzy based key agreement scheme that uses ECG signal to protect the symmetric key to be exchanged. Both integrity and authenticity are preserved in this fuzzy key agreement scheme. Attacks like correlation attack have been overcome in this system using two sets of feature in validation and verification procedure. Choosing order of polynomial plays a major role for better performance. Higher order polynomial gives better efficiency than lower order polynomial .The performance of this scheme is analysed in terms of FAR. Moreover this scheme is fast and efficient and can be applied in frequency domain.

9. REFERENCES

[1] Venkatasubramanian.K.K, Banerjee.A and Gupta.S.K.S, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, Vol.14, No.1, January 2010.

[2] Sriram Cherukuri, Krishna K Venkatasubramanian , Sandeep K S Gupta , "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body" , IEEE International Conference on Parallel Processing, 2003.

[3] Ari Juels and Madhu Sudan. A Fuzzy Vault Scheme.In Proceedings of the IEEE International Symposium on Information Theory (ISIT), page 408, 2002.

[4] T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin.Secure Smartcard-Based Fingerprint Authentication. In Proceedings of the ACM SIGMM Workshop on Biometrics Methods and Applications, pages 45-52, Berkley, California, 2003.

[5] Umut Uludag, Sharath Pankanti, and Anil K. Jain. Fuzzy Vault for Fingerprints. In Proceedings of the Audio- and Video-based Biometric Person Authentication pages 310-319, Hilton Rye Town, USA, 2005.

[6] S. Yang and I. Verbauwhede. Automatic Secure Fingerprint Veri_cation System Based on Fuzzy Vault Scheme. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing pages 609-612, Philadelphia, USA, 2005.

[7] Ee-Chien Chang, Ren Shen, and Francis Weijian Teo.Finding the Original Point Set Hidden among

Cha_.In Proceedings of the ACM Symposium on Information,Computer and ommunications Security pages 182-188, 2006.

[8] Ee-Chien Chang and Qiming Li. Hiding Secret Points Amidst Chaff. In Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 59-72, Petersburg, Russia, 2006.

[9] Preda Mihailescu.The Fuzzy Vault for Fingerprints is Vulnerable to Brute Force Attack.W.L.W. AlTarawneh and W.L Woo. Biometric Key Capsulation Technique Based on Fingerprint Vault: Anatomy and Attack. In Proceedings of the International Conference on Information and Communication Technologies: From Theory to Applications, pages 1-5, Syria, 2008.

[10] Karthik Nandakumar, Abhishek Nagar, and Anil K. Jain. Hardening Fingerprint Fuzzy Vault Using Password. In Proceedings of the International Conference on Biometrics,pages 927-937, Seoul, Korea, 2007.