J Electr Eng Technol.2016; 11(5): 1509-1519
http://dx.doi.org/10.5370/JEET.2016.11.5.1509

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

A Novel Fuzzy Based Bio-Key Management scheme for Medical Data Security

K. Kalaivani† and R. Sivakumar*

Abstract – Medical data security has drawn much attention from research community in recent years. Medical sensor networks are playing a major role to assure the security of medical data in health care monitoring. A critical issue in providing security for the streaming medical data is how to protect the security aspects like confidentiality, integrity, authentication and non-repudiation of a patient's medical data over networking environment in a resource efficient manner. This paper presents a novel fuzzy based bio-key management scheme (FBKM), which can provide secure medical data communication without any overhead. We have presented the simulation results, which exhibit that the proposed FBKM scheme can achieve better security performance in terms of various metrics such as False Acceptance Rate (FAR), Genuine Acceptance Rate (GAR) and False Rejection Rate (FRR) than other existing approaches.

Keywords: Medical sensor networks, Telemedicine, Electrocardiogram (ECG), Polynomial, Key management

1. Introduction

The rapid development of computer networks and telemedicine based applications has enabled effective real-time medical data transmission and reception. It has also led to quick and proper exchange of medical information in the digital form. Medical sensor networks offer economic solution to the present healthcare system, in which the status of the patient can be sent to physicians any time through interconnection of networks. Code Blue [1], Live Net [2], MobiHealth [3], Alarm-Net [4], Ubi-Mon [5] are some of the health care projects that can take care of patients in homes, hospitals, health centers, catastrophe sites and the open environment.

Medical sensor networks consist of a group of tiny and movable sensors that are capable of communicating with each other. Sensors can be wearable or implanted into the patient's body to observe the parameters as ECG, EEG and blood pressure level. Diagnostic equipments embedded with imaging technologies, genetic analysis etc., are used for collecting realistic data from patients [6-8]. Conversely, there are numerous difficulties to be faced by medical sensor networks before its deployment in the real world. First the sensors have limited resources in terms of power consumption, memory and computational potential. Since the sensors are battery operated, power consumption and energy are the main factors to be considered. So, Medical sensor networks require manageable and secure communication to assure confidentiality, integrity, authentication and non-repudiation of real-time medical data.

Medical data security is mainly based on cryptography. Symmetric key cryptography and Asymmetric key cryptography are the two types of cryptosystems available to ensure data security. All symmetric key cryptography depends on common secret key shared between sender and receiver. AES, DES, Triple DES, IDEA, FEAL, RC5 are some of the very popular symmetric key cryptosystem available in the cryptography. The conventional cryptographic techniques provide confidentiality but fail to provide the other security aspects. These symmetric key cryptography methods require smaller key size, much faster computation and smaller memory requirements than asymmetric key cryptography techniques. These advantages can be used in medical sensor networks. Asymmetric key cryptography uses the Public key and Private Key for encryption and decryption. Some of the most popular asymmetric key cryptography techniques are RSA, El-Gamal, ECC, and many more. Public key cryptography assures all security aspects. Many algorithms have been developed by combining public key cryptography and secure hash functions that enable digital signatures, authentication and integrity. However these are not only slower but also requires large memory and computational power. Due to this reason, medical sensor networks cannot use this type of public key cryptography techniques.

In medical sensor networks, sensors mainly depend upon cryptographic keys to secure real-time medical data communication. Based on that fact, various number of key management techniques have been developed. But all those techniques cannot be applied directly in medical sensor

† Corresponding Author: Dept. of Electronics and Instrumentation Engineering, Easwari Engineering College, Tamilnadu, India. (kvani2007@gmail.com)
* Dept. of Electronics and Communication Engineering, R.M.K Engineering College, Tamilnadu, India. (rsk.ece@rmkec.ac.in)
Received: January 23, 2015; Accepted: May 30, 2016

networks due to the limitations of biomedical sensors. Therefore, designing an efficient key management scheme in medical sensor networks is a challengeable problem. Due to the need for more security in telemedicine based applications [9], we require an efficient cryptography scheme. The proposed Fuzzy based Bio-Key Management (FBKM) scheme, which would serve as a better and efficient cryptography solution for secured real-time medical data communication.

The rest of this paper is organized as follows. Section II outlines the related works, section III depicts system model and gives the detailed procedure of the proposed scheme. Section IV discusses the simulation results in detail. Finally, Section V concludes the paper.

2. Related Works

In Medical sensor networks, various types of medical sensors like ECG, Blood pressure, EMG, Glucose, Pulse oxymeter, inertial sensors, etc., can be connected to other medical sensors or to the control nodes. Interconnected sensors could interface with Internet to further carry medical information to the medical expertise or emergency services. Secured communication scheme is required to support secure communication in medical sensor networks as shown in Fig. 1.

In [10], the authors describe deployment knowledge-based random key pre-distribution scheme. This scheme is said to be efficient in reducing memory requirement of sensors in networks.

Fuzzy vault scheme [11] is error-tolerant and secret sharing scheme, which deals with unordered sets of different cardinalities. This scheme is based on polynomial reconstruction problem and well suitable for biometrics based applications [12].

In Physiological Signal based Key Agreement (PSKA) [13-16], inter-sensor communication within a BAN is enabled allowing neighboring nodes to agree to a symmetric cryptographic key. Though this scheme proves to be better, it causes additional overhead through chaff points introduced in key generation. In [17], the author presents ECG-IJS scheme to improve authentication of real-time messages. Here, both the sender and receiver are capable of sampling the ECG signal from the human body. A similar feature extraction algorithm is used at receiver to generate features from the sampled ECG signals.

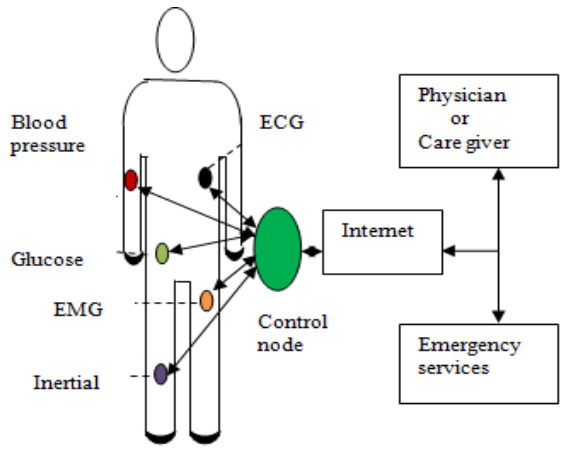


Fig.1. Telemedicine scenario

This scheme exhibits error tolerance better than previous schemes and reduces the entropy loss to near optimal value. The performance of this ECG-IJS scheme can be further improved by implementing the best possible vault size and best different tolerance values. In this paper, a new scheme called Fuzzy based Bio-Key Management (FBKM) scheme is proposed to implement the key agreement procedure in more efficient manner in telemedicine, mobile applications [18] and Cloud based Internet of Things [19-21].

3. System Description

3.1 System design of Fuzzy Based Bio-Key Management (FBKM) scheme

A standard proposed FBKM design for the authentication procedure followed by sender is explained in Fig. 2(a). The figure shows how medical sensor network triggers alert to the hospital, even before the patient has severe problems like heart attack. Sensors are implanted in the human body to measure the change in temperature, pulse rate, blood pressure, respiratory rate etc.,. The parameter level is transmitted to physician working in the intensive care unit in hospital to take necessary steps to prevent a critical incident. Critical care units have multi-modal monitors that concurrently measure and display the related fundamental parameters. In such scenario, this real-time medical data among sensor nodes must be well protected against attackers and security aspects must be ensured [20].

When the receiver gets the packet, decrypts the original message by using the key generated from ECG signal measured by the receiver. Receiver recalculates the new hash value using the same SHA-1 algorithm. Health care units without proper security arrangement for real-time medical data communication will lead to wrong diagnosis and treatment.

In the proposed scheme, both the sender and the receiver have the capability to sample the ECG signals from the human body. System model diagram that depicts the process involved at sender and receiver using FBKM scheme is shown in Fig. 2(a) and Fig. 2(b). Detailed architectural flow followed at sender and receiver is explained in Section III. B.

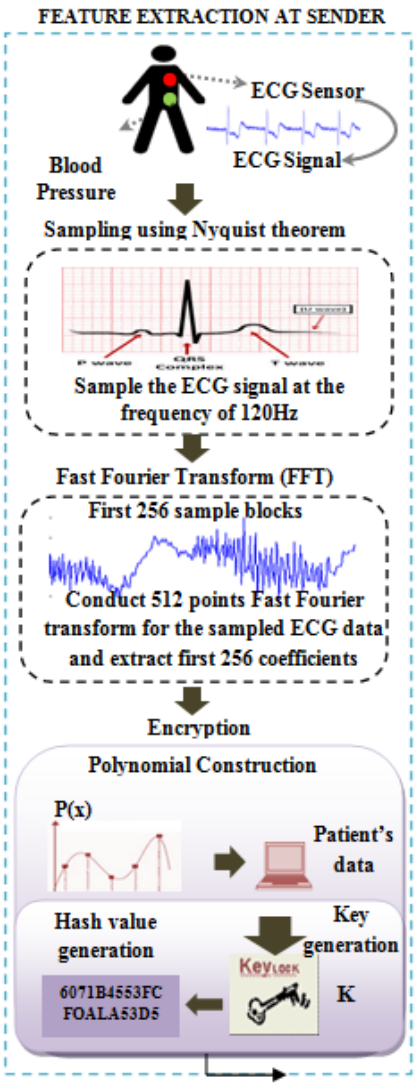


Fig. 2(a): FBKM scheme procedure followed by Sender

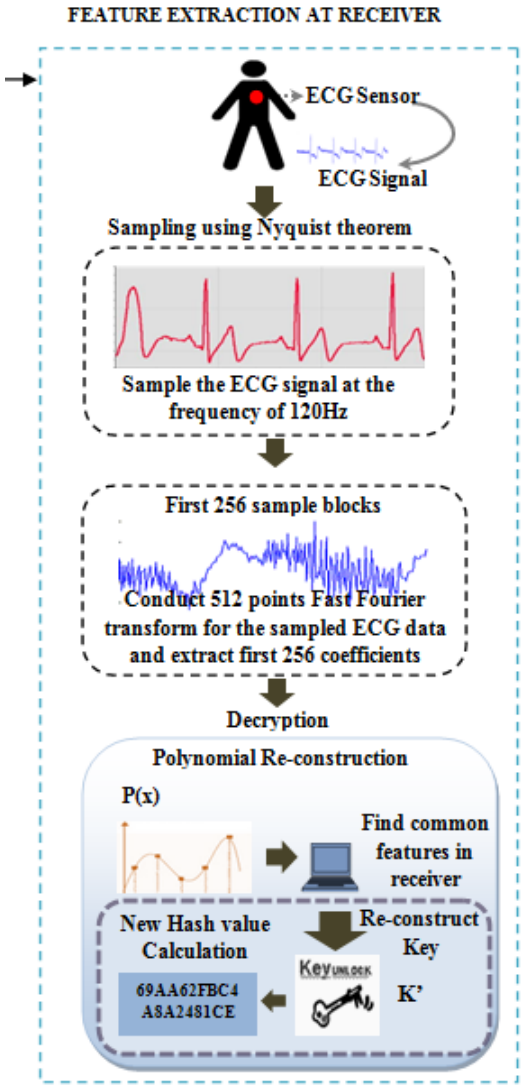


Fig. 2(b): FBKM scheme procedure followed by Receiver

3.2. Detailed Architecture of FBKM scheme

Objective of FBKM scheme is to protect the integrity and confidentiality of sensitive medical data among sensor nodes.

Procedure at Sender:

The procedure to be done by the sender is described as follows:

a) Feature extraction at sender: Feature extraction plays a vital role in protecting the confidentiality during communication. Features when carefully chosen are expected to perform desired task efficiently. In our proposed method, from the sample ECG signal, the ECG features are extracted. FBKM scheme uses frequency-domain analysis of ECG signals for generating the features. Process followed for extracting ECG features using sample ECG signal in FBKM is explained below:

Step 1: Get the analog ECG signal (ECG_{analog_sig}) from the human body using ECG sensor for fixed duration of 4 sec (reason for choosing 4 sec is to include one heart beat) as shown in Fig. 3.

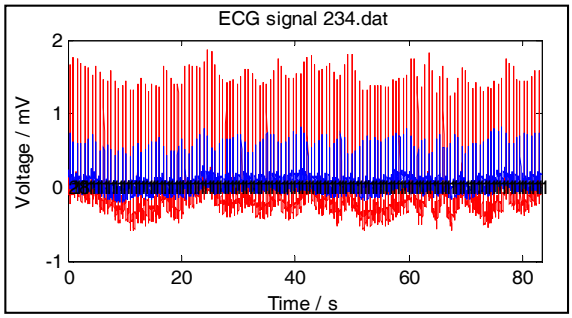


Fig. 3. ECG signal captured using ECG sensor

Step 2: Resample the captured ECG signal, using the Nyquist theorem at the frequency of 120Hz to filter the noise. The filtered ECG signal $ECG_{an\_sig\_org}$ is processed through FFT in next stage.

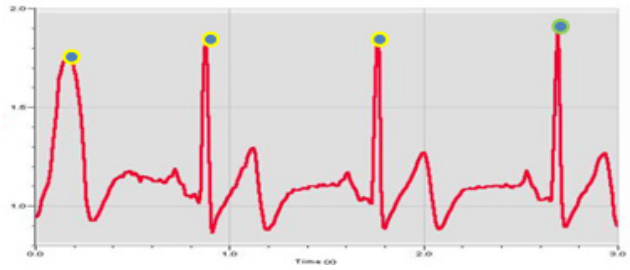


Fig. 4. ECG sample blocks with peak limits

Step 3: The ECG signal ($ECG_{an\_sig\_org}$) is divided into 512 sample blocks $\{Ecg_{b1}, Ecg_{b2} \ldots . Ecg_{b512}\}$ to detect the local peak limits within each block. Local peak limit from each block is stored in an array vector named $ECG_{peak} = (P_0, P_1, \ldots P_n)$ where 'n' varies from 0 to 511.

Each of the peak limit can be used as a feature as shown in Fig. 4. Conduct 512 points FFT to the ECG sample blocks and retrieve first 10 FFT peak location index $(P_0, P_8, P_4, \ldots, P_{14}, P_1)$ as the extracted feature set or coefficients subset sub set $Coeff_{subset} = (C_0, C_1 \ldots C_9)$. The peak location index is a good candidate that can be used to differentiate measurements (collected by a sensor) of one patient from those of different patients. This extracted feature provides an efficient representation of ECG signals for the data authentication and secret key agreement.

Step 4: Extract the first 10 coefficients of peak values from coefficient sub set $Coeff_{subset} = (C_0, C_2 \ldots C_9)$ i.e peak values of the peak index $(P_0, P_8, P_4, \ldots, P_{14}, P_1)$ and store it in set A=$\{a_0, a_2, a_3 \ldots a_9\}$. Extracted feature set A is used to generate the polynomial (P_A) where, $P_A = \{p(a_0), p(a_1), p(a_2) \ldots . p(a_9)\}$ with degree D varying from 1 to 10. Project the locking key elements (i.e. Sender A's features) on the polynomial and evaluate the polynomial 'P' on the elements of A and compute the Genuine set (G_A) where,

$$G_A=\{(a_0, p(a_0)), (a_1, p(a_1)), (a_2, p(a_2)), \ldots (a_9, p(a_9))\}$$

b) Private key-1 generation using feature set:

Non overlapping 10 segments are created considering each pair of the constructed set say, $\{(a_0, p(a_0))\}$. Each segment is declared as a specific private key coefficient. The genuine set G_A is finally passed through a scrambler which randomizes the list, with the aim of removing any stray information that can be used to fetch genuine points. This results in private key set K_{SA}, where $K_{SA} = \{k_1, k_2, k_3, \ldots k_{SM}\}$ here SM is 10. Along with the key set K_{SA}, the polynomial of degree D a final private key '$\boldsymbol{K_{s\_private}}$' is generated using feature set where '$K_{s\_private}$' denotes the sender's private key-1.

c) Fuzzy vault locking:

Fuzzy vault scheme is an Artificial Intelligence technique well suitable for biometrics based applications. It is an error-tolerant and secret sharing scheme, which deals with unordered sets of different cardinalities. Fuzzy vault utilizes fuzzy logic that comprises of four components namely, fuzzification, fuzzy inference engine, fuzzy rule base and defuzzification as shown in Fig. 5.

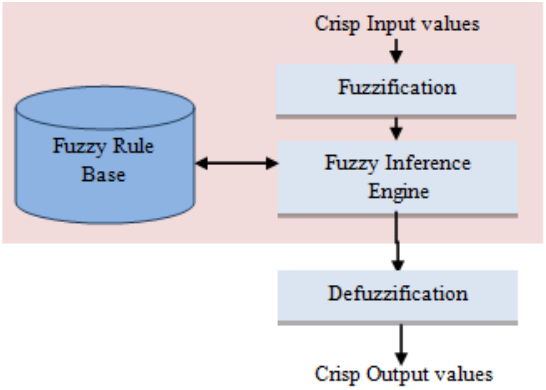


Fig. 5 Structure of Fuzzy Logic Model

Table 1. Classification of Blood pressure

Input field	Range	Fuzzy set (Membership function)
Blood pressure	<75	Low
	80-100	Medium
	95-199	Normal
	>185	High

Table 2. Classification of Heart rate

Input field	Range	Fuzzy set (Membership function)
Heart rate	<50	Low
	53-100	Medium
	95-110	Normal
	>125	High

Table 3. Classification of Blood sugar

Input field	Range	Fuzzy set (Membership function)
Blood sugar	<63	Low
	63-72	Medium
	70-110	Normal
	>140	High

The sensor at sender measures the ECG signals, heart beat rate, pulse rate, blood pressure, respiration rate and oxygen levels and sends the data to the receiver. In FBKM, for designing the fuzzy logic system three input variables i.e. blood pressure, heart rate, and blood sugar are considered. These inputs are called vital signs and use to predict the health status of person. After choosing the input variables the next step is to fuzzify the variables referred to as fuzzification. *Fuzzification* is the first step in the design of any fuzzy logic system. To fuzzify the variables, we have to determine the fuzzy sets for each input variable and the corresponding range for each fuzzy set. Formation of fuzzy set is through classification of vital sign with its corresponding triangular membership functions are referred in Table 1, Table 2 and Table 3. In this fuzzy

system, there is one output variable i.e. the Risk Level (RL), which refers to the degree of illness of the patient. Larger the value of this output variable more will be the health risk of the patient.

In FBKM, we have considered 4 fuzzy sets RL_{low},RL_{medium},RL_{normal}, RL_{high} for the output variable Risk Level. The fuzzified values are processed by the inference engine, which consists of a rule base and various methods for inferring the rules. The rule base is the main part in the fuzzy inference system and the quality of results in a fuzzy system depends on the fuzzy rules. In FBKM, the number of rules are obtained using $N_{rule} = I(1) * I(2) * I(3) * I(4) \dots I(n)$, where, N_{rule} is the total number of possible rules for a fuzzy system and $I(n)$ is the number of linguistic terms for the input linguistic variable varying from 1 to *n*. We use logical combination of inputs with '**and**' operator as all the inputs are dependent among each other. Sample fuzzy rules used in FBKM are referred below:

If (Blood pressure is low) **and** (Heart rate is low) **and** (Blood sugar is low) **then** (Risk_level is RL_{high})

If (Blood pressure is low) **and** (Heart rate is high) **and** (Blood sugar is low) **then** (Risk_level is RL_{medium})

If (Blood pressure is normal) **and** (Heart rate is normal) **and** (Blood sugar is high) **then** (Risk_level is RL_{normal})

If (Blood pressure is normal) **and** (Heart rate is high) **and** (Blood sugar is normal) **then** (Risk_level is RL_{medium})

If (Blood pressure is high) **and** (Heart rate is normal) **and** (Blood sugar is normal) **then** (Risk_level is RL_{normal})

If (Blood pressure is high) **and** (Heart rate is low) **and** (Blood sugar is high) **then** (Risk_level is RL_{high})

In our case, the logical combination for input values Blood Pressure = 120, Heart Rate = 75 and Blood Sugar = 95, original message or data (**M**) is to given the fuzzy inference engine to produce a crisp output (O_1) risk level is RL_{normal} = 0.126 as shown in the below Table 4. Similar manner, five combinations of inputs are captured using the sensor to produce 5 crisp output (O_1, O_2, O_3, O_4, O_5) using fuzzification. Crisp output is obtained by applying one of strategies called Centroid of Area.

Table 4. Fuzzification process produces crisp output using inputs

Blood pressure	Hert rate	Blood sugar	Risk Level (RS)
120	75	95	RL_{normal}=0.126

d) Private key-2 generation:

Extracted crisp output set $C_{output} = (O_1, O_2, O_3, O_4, O_5)$ is used to generate the polynomial 'P_{cp}' with degree D_{cp} varying from 1 to 5.

Polynomial Construction:

Treating the elements of set $C_{output} = (O_1, O_2, O_3, O_4, O_5)$ as distinct coordinate values, the polynomial is constructed, $P_{cp} = \{p(O_1), p(O_2), \dots p(O_5)\}$. Project the locking key elements (i.e. Crisp output set values) on the polynomial and compute the Genuine private set G_{ACP}, $G_{ACP} = \{(O_1, p(O_1)), (O_2, p(O_2)), \dots (O_5, p(O_5))\}$ Non overlapping 5 segments are created considering each pair of the constructed set say, $(O_1, p(O_1))\}$. Each segment is declared as a specific private key coefficient. The genuine private set G_{ACP} is finally passed through a scrambler which randomizes the list, with the aim of removing any stray information that can be used to fetch genuine points. This results in private key set K_{fuzzy}, Along with the key set K_{fuzzy}, the polynomial of degree D_{cp} a final private vault key '$\boldsymbol{K_{s\_vault}}$' is generated where '$\boldsymbol{K_{s\_vault}}$' denotes the sender's private key-2.

e) Encryption:

In our proposed FBKM, using the features extracted, the sender generates a private key-1 ($\boldsymbol{K_{s\_private}}$). Sender uses the private key-1 to encrypt the crisp output set 'C_{output}' (secret data) to generate an encrypted message (E_{cp_msg}).

f) MAC generation using SHA-1:

Proposed FBKM scheme uses Secure Hash Algorithm 1 (SHA-1) for Message Authentication Code (MAC) generation. The same SHA-1 hash algorithm must be used by the receiver. The Vault Key (K_{s_vault}), the secret data (C_{output}), original message (M) and ID of the sender (IDs) are processed using SHA-1 algorithm to generate the hash code (H_{s_value}) referred as MAC. i.e. H_{s_value} = MAC (K_{s_vault}, C_{output}, M, IDs). Then the sender sends the following 'packet' to the receiver:

{IDs, IDr, $Coeff_{subset}$,E_{cp_msg}, $K_{s\_private}$, K_{s_vault},H_{s_value}}

Fig. 6. shows a sample packet sent from sender to receiver.

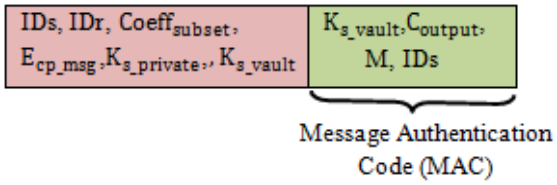


Fig. 6. Packet sent from sender to receiver

where, IDs and IDr are the ID's of the sender and receiver, $Coeff_{subset}$ is the subset of coefficients generated using features extracted (feature set A), E_{cp_msg} is the encrypted message of the crisp output, $K_{s\_private}$ is the private key-1 of the sender, K_{s_vault} is the private key-2 of the sender and MAC or H_{s_value} contains the vault key K_{s_vault}, crisp output set C_{output}, original message (M) and sender ID (IDs).

Procedure at Receiver:

The receiver receives the packet from the sender and performs the following verification and validation to confirm user authenticity to retrieve the original data.

a) Feature extraction at receiver: The receivers have statistically similar ECG signals when two sensors measure the ECG from the same body. The procedure to be done by the receiver is described as follows:

Step 1: Get the ECG signal from the same human body using ECG sensor in order to extract features at the receiver.

***Step 2*:** The receiver B follows the similar steps (Step2 and Step3) as like in Sender's procedure to extract the feature set i.e. the first 10 coefficient subset $\mathrm{RCoeff_{subset}} = (\mathrm{RC_0}, \mathrm{RC_1} \ldots \mathrm{RC_9})$. Both the sender and the receiver use the same feature extraction algorithm to generate coefficient subset.

Step 3: Extract the first 10 coefficients of peak values from coefficient subset $\mathrm{RCoeff_{subset}} = (\mathrm{RC_0}, \mathrm{RC_1} \ldots \mathrm{RC_9})$ i.e values of the peak index $(\mathrm{P_0}, \mathrm{P_8}, \mathrm{P_4}, \ldots, \mathrm{P_1}, \mathrm{P_9})$ and store it in set B= $\{\mathrm{b_0}, \mathrm{b_2}, \mathrm{b_3} \ldots \mathrm{b_9}\}$. The Extracted feature set is used to re-construct the polynomial at receiver. Polynomial reconstruction is performed using the feature set B= $\{b_0, b_2, b_3 \ldots b_9\}$ following similar steps referred in sender procedure. Therefore, receiver B constructs the polynomial P_B. where, $P_B = \{\mathrm{p(b_0)}, \mathrm{p(b_1)}, \mathrm{p(b_2)} \ldots . \mathrm{p(b_9)}\}$. Evaluate the polynomial 'P_B' on the elements of B and compute the Genuine set G_B, where,

$$G_B = \{(\mathrm{b_0}, \mathrm{p(b_0)}), (\mathrm{b_1}, \mathrm{p(b_1)}), (\mathrm{b_2}, \mathrm{p(b_2)}), (\mathrm{b_9}, \mathrm{p(b_9)})\}$$

where b_i denotes the $\mathrm{i^{th}}$ element and 'i' varies from 0 to 9 of set B and $p(b_i)$ indicates the generated polynomial of $\mathrm{i^{th}}$ element. Similar way, using the coefficients ($\mathrm{Coeff_{subset}}$) received from sender, receiver re-constructs the polynomialP'_A. Evaluate the polynomial P'_A on the elements of A (using coefficients received from sender) and compute the Genuine set G'_A. Where, $G'_A = \{a'_0, \mathrm{p}(a'_0)), (a'_1, \mathrm{p}(a'_1)), (a'_2, \mathrm{p}(a'_2)), \ldots (a'_9, \mathrm{p}(a'_9)\}$

Genuine set$G_B$is matched with the genuine set G'_A and search to meet most of the pairs.

b) Private Key-1 Generation at Receiver: Non overlapping 10 segments are created considering each pair of the constructed set say, $\{(\mathrm{b_0}, \mathrm{p(b_0)})\}$. Each segment is declared as a specific private key coefficient. The genuine set G_B is finally passed through a scrambler which randomizes the list, with the aim of removing any stray information that can be used to fetch genuine points. This results in private key set K_{SB}, where $K_{SB} = \{\mathrm{k_1}, \mathrm{k_2}, \mathrm{k_3}, \ldots \mathrm{k_{SM}}\}$ here SM is 10. Along with the key set K_{SB}, the polynomial of degree D a private key $\boldsymbol{K_{r\_private}}$ is generated where $K_{r\_private}$ denotes the receiver's private key-1. Receiver now verifies the private key-1 received from sender ($\boldsymbol{K_{s\_private}}$) with private key-1 generated at receiver ($\boldsymbol{K_{r\_private}}$),

if ($\boldsymbol{K_{s\_private}} == \boldsymbol{K_{r\_private}}$) *then*
  "Authentication is successful"
else
  "Authentication is rejected"
end

If both the private key-1 matches, then the user is said to be authenticated user and provided access to validate private key, otherwise the user is prevented further access to the system. Receiver performs Fuzzy vault unlocking mechanism only for users whose private key-1 verification is successful.

c) Fuzzy Vault Unlocking: Receiver decrypts the encrypted message E_{cp_msg} using the private key-1($\boldsymbol{K_{r\_private}}$)to generate the set of crisp output $C_{r\_output} = (O_{r1}, O_{r2}, O_{r3}, O_{r4}, O_{r5})$.

d) Private Key-2 generation: Extracted crisp output set $C_{r\_output} = (O_{r1}, O_{r2}, O_{r3}, O_{r4}, O_{r5})$ is used to generate the polynomial 'P_{r_cp}' with degree D_{r_cp} varying from 1 to 5.

Polynomial reconstruction: Treating the elements of set C_{r_output}=$(O_{r1}, O_{r2}, O_{r3}, O_{r4}, O_{r5})$as distinct coordinate values, the polynomial constructed is, $P_{r\_cp} = \{\mathrm{p}(O_{r1}), \mathrm{p}(O_{r2}), \ldots \mathrm{p}(O_{r5})\}$. Project the locking key elements (i.e. Crisp output set values) on the polynomial and compute the Genuine private set (G_{BCP}) where,

$$G_{BCP} = \{(O_{r1}, \mathrm{p}(O_{r1})), (O_{r2}, \mathrm{p}(O_{r2})), \ldots (O_{r5}, \mathrm{p}(O_{r5}))\}$$

Non overlapping 5 segments are created considering each pair of the constructed set say, $(O_{r1}, \mathrm{p}(O_{r1}))\}$. Each segment is declared as a specific private key coefficient. The genuine private set G_{BCP} is finally passed through a scrambler which randomizes the list, with the aim of removing any stray information that can be used to fetch genuine points. This results in private key set K_{rfuzzy}, Along with the key set K_{rfuzzy}, the polynomial of degree D_{r_cp} a final private vault key '$\boldsymbol{K_{r\_vault}}$' is generated where '$\boldsymbol{K_{r\_vault}}$' denotes the receiver's private key-2. Receiver now verifies the private key-2 received from sender ($\boldsymbol{K_{s\_vault}}$) with private key-2 generated at receiver ($\boldsymbol{K_{r\_vault}}$),

if ($\boldsymbol{K_{s\_vault}} == \boldsymbol{K_{r\_vault}}$) *then*
  "Authorized user to perform decryption"
else
  "Unauthorized user"
end

Once the private key verification is successful, the receiver using the C_{r_output} to perform defuzzification process to produce the original message 'M'. i.e. each crisp output undergoes a defuzzification process. *Defuzzification* is the inverse process of fuzzification. The crisp output is given as input to the defuzzification process to generate set of outputs which is the original message 'M' (representing the set of input values passed through the fuzzification

stages). The receiver now performs message authentication.

e) Message Authentication: Authentication often involves verifying the validity of at least one form of identification. The receiver uses the same authentication (SHA-1) algorithm as like the sender to recalculate the MAC.

if $(MAC_{receiver} == MAC_{sender})$ then
"Authentication succeeds"
"Received packet accepted"
else
"Authentication Fails"
"Received packet will be discarded"
end

Message authentication is important for many applications in sensor networks. An adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. If hash value calculated by the sender and receiver matches, then the data is said to be an authenticated data. Thereby, the vault unlock scheme successfully authenticates the sender. This, not only confirms the correctness of the unlocking process, but also authenticates the sender to the receiver confirming that the sender is on the same Body Area Network (BAN) like the receiver. In FBKM, using the above said procedure, parameters like False Acceptance Rate (FAR), Genuine Acceptance Rate (GAR) and False Rejection Rate (FRR) are calculated for the polynomial degree from 5 up to 10. Proposed FBKM scheme through Fuzzy vault scheme implementation proved to be more efficient and secure compared to ECG-IJS scheme in terms of reduced FRR, FAR and higher GAR (TPR) by adopting optimal tolerance limit to 2.

4. Simulation Results

This section validates the proposed Fuzzy based Bio-Key Management scheme. Experimental analysis was done using a self-written script in MATLAB. Security analysis and performance of the proposed FBKM scheme was analyzed using the following metrics:

Genuine Acceptance Rate (GAR): The percentage of times a system (correctly) verifies a true claim of identity.

False Acceptance Rate (FAR): The percentage of times a system produces a false accept, which occurs when a sender key is incorrectly matched to receiver key.

False Rejection Rate (FRR): The percentage of times the system produces a false reject. A false reject occurs when a sender key is not matched to receiver key.

In this process, twenty person's ECG signals are downloaded from "*MIT-BIH Arrhythmia*" database. This

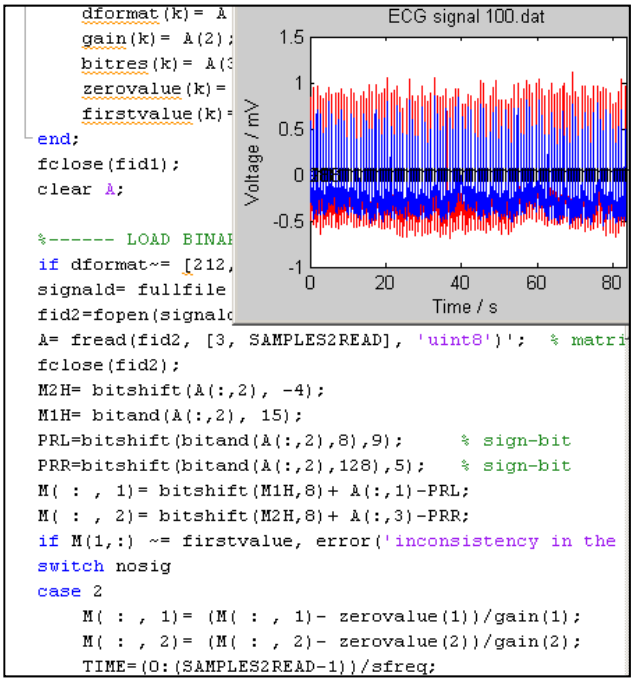


Fig. 7. Snapshot of Matlab script processing the output ECG signal

database contains 48 half-hour excerpts of two-channel ambulatory ECG recordings. The recordings were digitized at 360 samples per second per channel with 11-bit resolution over a 10-mV range. ECG data was resampled at 120 Hz. Coefficients from the ECG data were obtained using FFT technique.

Fig. 7. shows the evaluation process done using MATLAB script to fetch the peak index values using the ECG signal. Then peak index values on the extracted coefficients are identified as features. The features present a resourceful representation about ECG signals for the data authentication and secret key agreement. Moreover, the peak index values are used to characterize and tolerate the differences on the same body, and they significantly differ on different bodies. Fig. displays sample ECG signal. We can observe that the resulting ECG signals contain little baseline wandering but keeps the main characteristics of the original ECG signals, we can also see that the wideband noises are suppressed while almost all the information of the ECG signal are maintained.

4.1. Receiver Operating Characteristic Curve (ROC):

Performance of FBKM scheme is evaluated by analyzing ROC against existing ECG-IJS scheme. ROC considers only the Genuine Acceptance Rate (GAR) or True Positive Rate (TPR) and False Acceptance Rate (FAR) or False Positive Rate (FPR) . The True positive in this case occurs when an authorized user's key generation and key verification results in a success when the user do have the vault key and hash code. A false positive on the other

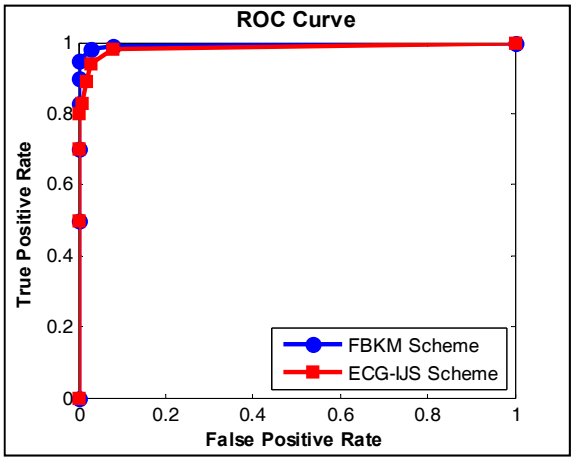
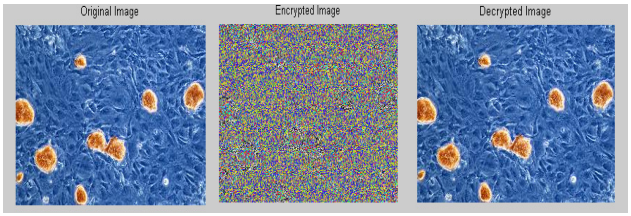
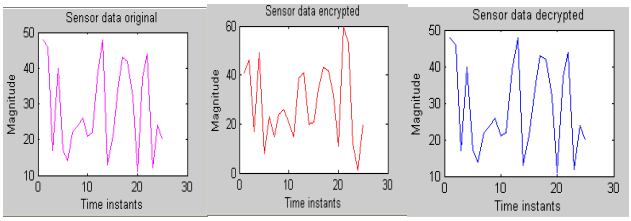


Fig. 8. ROC curve comparison graph between FBKM Vs Existing scheme



(a) Original image (b) Encrypted image (c) Decrypted image



(d) Original data (b) Encrypted data (c) Decrypted data

Fig. 9. FBKM process verification for Authenticated users

hand occurs when an unauthorized user's attempt for key generation and verification results in success when the user actually do not have the correct vault key and hash code.

The ROC curve referred in Fig. 8. proves that, the attempt made by authorized person's success rate increases (True positive rate is higher) while the attempt made by unauthorized person's success rate never occurs nor is very minimal.

The ROC curve in Fig. 8. proves that the performance of FBKM is better compared to existing ECG-IJS scheme due to the factor that in FBKM scheme a combination of fuzzy vault (private key) and MAC (Hash code) provides higher security ensuring confidentiality, integrity and authenticity at the receiver. i.e. without a similar feature set and crisp output, the attacker would not be able to regenerate the key. Fig. 9. below displays the glioblastoma cancerous cell image and sensor data sent from authorized sender to receiver. Sender executes the FBKM procedure converting

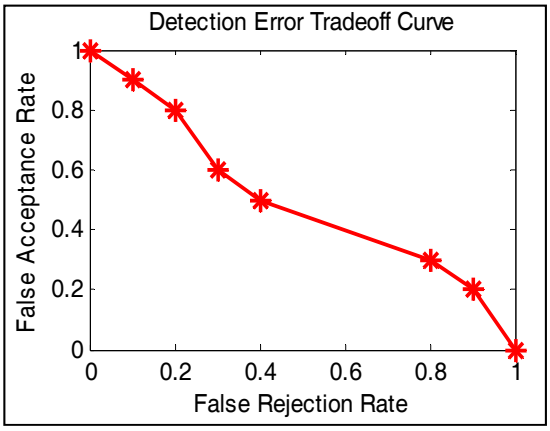


Fig. 10. Detection Error Tradeoff Curve for FBKM scheme

a real image and valid sensor data to an encrypted format, which when received at the receiver is validated through key generation and verification. Once the key is validated and authentication is successful, decryption process is done to retrieve the original image and sensor data.

4.2 Detection Error Tradeoff (DET):

Error rates in FBKM scheme was derived through Detection Error Tradeoff (DET) graph plotting False Rejection Rate (FRR) against False Acceptance Rate (FAR).

This analysis is done to verify if the system could tolerate more different features between the sender and the receiver. Fig. 10. shows the DET curve for FBKM scheme.

The DET curve proves that, when the attempt made by authorized person's failure rate increases (FAR), the attempt made by unauthorized person's success rate decreases (FRR). The possibility of matching two feature sets that do not belong to the same person increase and thus the FAR increase. As we predict from the results at higher false acceptance rate the rejection rate is null. When the FAR is challenged continuously with respect to injection of False Rejection Rate, it gradiently decreases and becomes ineffective.

4.3 False acceptance rate:

False Acceptance Rate performance is illustrated in Fig. 11., when the polynomial degree 'D' changes with tolerance value set as 2. The False Acceptance in this case occurs when the system incorrectly verifies an unauthorized person. FAR is considered the most serious biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out. Security level is assured with higher degree of polynomial 'D' varying between 5 and 10. When the polynomial degree is high at particular tolerance value, then maximum number of shared features must be recovered to find out the secret information. Thus, the

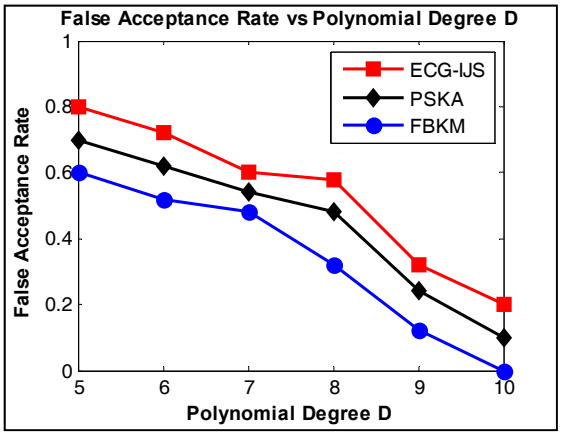


Fig. 11. FAR versus Polynomial Degree 'D'

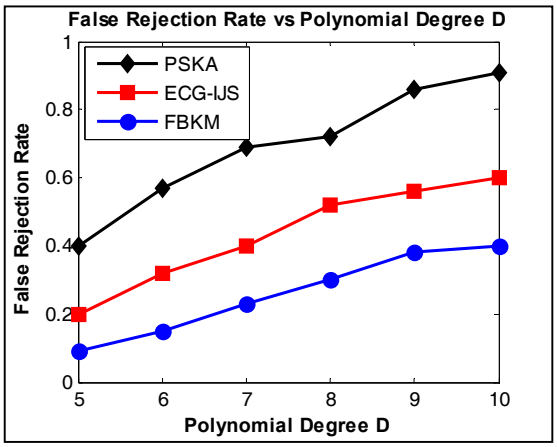


Fig. 12. FRR versus Polynomial Degree 'D'

probability of mismatching the feature sets decreases. Performance of FAR is illustrated comparing PSKA [13-16], ECG-IJS [17] scheme with the proposed FBKM. From the figure, it is understood that FAR decreases when polynomial degree D increases. This comparison results indicates the performance of proposed Fuzzy based bio-key management scheme is more efficient and secure than PSKA and ECG-IJS scheme. The fuzzy vault (private key) and MAC combination generated in the proposed FBKM scheme facilitates reducing the FAR.

4.4 False rejection rate:

The False Rejection in this case occurs when the security system will incorrectly reject an access attempt by an authorized user. False Rejection Rate performance is illustrated in Fig. 12., when the polynomial degree 'D' changes with tolerance value set as 2. It is understood that FRR increases when the polynomial degree 'D' increases. FRR is increased, due to the fact that, when more common elements of the feature are required to authenticate, the system may reject the two-feature sets when received from the same person. This comparison results indicate that the performance of FBKM is more robust against existing PSKA and ECG-IJS scheme.

5. Conclusion

Secured communication is strongly required in tele-medicine based applications to ensure the privacy and safety of a patient. In this paper, we present an efficient bio-key management scheme for medical data security using fuzzy logic. This scheme has made the security system stable by providing low FRR value. This novel scheme provides less computation complexity and communication overhead. This efficient scheme offers the security in terms of authentication, data confidentiality and data integrity. It remains future work to investigate the energy analysis and various network layer related attacks such as wormhole attack, sinkhole attack, and Sybil attack.

References

[1] Malan D, Jones T. F, Welsh M. Moulton, S. Code Blue, "An Ad-hoc Sensor Network Infra structure for Emergency medical Care", In proceedings of the Mobisys 2004 workshop on Applications of Mobile Embedded systems(WAMES 2004), Boston, MA, USA, June 2004, p. 6-9.

[2] Chenb. R, Peterson. G, Mainland. G, Welsh. M. LiveNet. "Using passive Monitoring to Reconstruct Sensor Network dynamics", Proceedings of the 4 th IEEE International Conference on Distributed computing in Sensor system(DCOSS'08), santorini island, greece, june 2008, p. 11-14.

[3] Halteren A. V, Bults R, Wac K, Konstantas D, Widya I, Dokovsky N, Koprinkon G, Jones V, Jerzog R, "Mobile patient Monitoring", The Mobi Health System. Jouranal of Information Technology, 2004, p. 365-373.

[4] Wood A, Virone G, Doan T, Cao Q, Selavo L, Wu Y, Fang L, He Z, Lin S, Stankovic J. Alarm-Net," Wireless Sensor Networks for Assisted-Living and Residential Monitoring", Technical Report CS-2006-01, Department of Computer science, university of Virginia: Charlottesville, VA, USA, 2012.

[5] Ng J. W. P, Lo B. P. L, Wells O, Sloman. M, Peters N, Darzi A, Toumazou C, Yang G., "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors(UBIMON)", Proceedings of 6th International Conference on Ubiquitous computing (UbiComp'04), am, UK, September 2004, p. 7-14.

[6] Degan Zhang, Xuejing Kang. A novel image de-noising method based on spherical coordinates system, EURASIP Journal on Advances in Signal

Processing, 2012, 2012(110):1-10 DOI:10. 1186/ 1687-6180-2012-110
[7] Degan Zhang, Guang Li, Ke Zheng. An energy balanced routing method based on forward-aware factor for Wireless Sensor Network. IEEE Transactions on Industrial Informatics, 2014, 10(1): 766-773
[8] Degan Zhang. A new approach and system for attentive mobile learning based on seamless migration. Applied Intelligence, 2012, 36(1): 75-89
[9] C. Poon, Y. T. Zhang, S. D. Bao, "A Novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health", IEEE Communication Magazine, 2006, p. 73-81
[10] Wenliang Du, Jing. Deng, Yunghsiang S. Han, Shigang Chen, And Pramod K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", Proceedings of INFOCOM, 2004, 5p. 86-597.
[11] K. Venkatasubramanian, A. Banerjee, S. Gupta, "EKG-based key agreement in Body sensor networks", INFOCOM workshop, . 2008, p. 1-6.
[12] Degan Zhang, Xiang Wang, Xiaodong Song. A Novel Approach to Mapped Correlation of ID for RFID Anti-collision. IEEE Transactions on Services Computing, 2014, 7(4):741-748
[13] Degan Zhang, Xiaodan Zhang. Design and implementation of embedded un-interruptible power supply system (EUPSS) for web based mobile application. Enterprise Information Systems, 2012, 6(4):473-489
[14] S. D. Bao, Y. T. Zhang, L. F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile health care systems", Proceedings of 27th International conference on eng. Med. Biol. soc, 2005, p. 2455-2458.
[15] K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta, "PSKA:Usable and secure key agreement scheme for bodyarea networks", Trans. Info. Tech. Biomed, 2010, p. 60-68.
[16] F. Miao, S. D. Bao and Y. Li, "A Modified fuzzy vault scheme for biometrics based body sensor networks security", Proceedings of IEEE Global Telecommuni-cation Conference, 2010, p. 1-5.
[17] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilokas, Hua Fang. "ECG-Cryptography and Authentication in Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, 2012, p. 1070-1078.
[18] Degan Zhang, Yanping Liang. A kind of novel method of serviceaware computing for uncertain mobile applications. Mathematical and Computer Modelling, 2013, 57(3-4):344-356
[19] Degan Zhang, Yannan Zhu. A new constructing approach for a weighted topology of wireless sensor networks based on local- world theory for the Internet of Things (IOT). Computers & Mathematics with Applications, 2012, 64(5):1044-1055
[20] H. Wang, D. Peng, W. Wang, H. Sharif, H. Hwa Chen And A. Khoynezhad, "Resource-aware secure ECG health care monitoring through body sensor networks", IEEE Wireless Communications, 2010:vol. 17, p. 12-19.
[21] Degan Zhang, Ke Zheng, Ting Zhang. A Novel Multicast Routing Method with Minimum Transmission for WSN of Cloud Computing Service. Soft Computing, 2015, 19(7):1817-1827.

K. Kalaivani She is currently a Ph. D. candidate at Anna University, Guindy, Chennai, India. She is working as an Assistant Professor in Easwari Engineering College. Her interest in research includes Medical image processing and soft computing techniques.

R. Sivakumar He received his Ph. D. degree from Anna University, Guindy, Chennai, India. He is currently a professor and Head of the department of Electronics and communication engineering at R. M. K Engineering college, India. He is a senior member of IEEE. His major research interests include Signal and Image processing.