JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Finger Print Authentication Based Cryptosystems for Electrocardiogram Data Security in Cloud

[1]Ajina Mohamed Ameer, [2]M. Victor Jose
[1]Research Scholar, [2]Associate Professor
[1,2]Department of Computer Science and Engineering,
[1,2]Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India.

Abstract: Electrocardiogram (ECG) biometric recognition is a novel research trend, and many methods have been developed. Due to the influence of physical and psychological activities, there are heartbeats diversities of the same person. However, the existing ECG biometric recognition methods do not make use of sample diversity information. Traditional passwords represent the most common mechanism of authenticating users online, despite numerous usability and security problems. Passwords create a burden for users, as they have to be memorized and, ideally, should be long and unique. It should not come as a surprise, therefore, that many users opt to use easy-to-guess passwords that are reused across different services, leading to account takeovers and personal data compromise. In this research, a biometric based on the electrical activity of the human heart is investigated as recorded by the ECG signals. In order to design an ECG- based biometric system, collecting dataset containing records of differed users. The data collection was performed over a period of four months, which allowed me to investigate the stability of ECG-based biometrics. After collecting the ECG data, the biometric authentication system was designed and implemented. The main objective of this study is to develop a privacy preserving ECG that detects arrhythmia in the early stage.

IndexTerms **- Arrhythmia, Authentication, Biometric, ECG, Fingerprint.**

I. INTRODUCTION

All In today's world, we observe an ever-increasing digitization of most areas of our lives. Every day we make use of online services such as mobile banking or email communication and we do not hesitate to keep our personal information on our devices or cloud storage. Unfortunately, the digital era has also paved the way for a series of new attacks and exploits, including unauthorized access to our personal data and devices by adversaries [1]. It is remarkable how, by and large, users are still burdened by numerous passwords, which have been used for access control since the earliest days of computing. There has been a recent shift of interest towards the field of biometric authentication, which proves the identity of the user using their biological characteristics. The problem of user verification has concentrated much effort of the research community in the last few years. This has resulted in many approaches for personal authentication based on biometric features. Conventional access control systems are typically based on a single time instant authentication. But the demand for robustly preventing fraudulent or unauthorized access to systems led us to another problem [2]. The guarantee that the initially authenticated person is the same that is using the system is the main issue. This problem is addressed by continuous user verification, where biometric authentication (verification) [31]. The main objective of this study is to develop a privacy preserving ECG that detects arrhythmia in the early stage. To investigate whether ECG signals collected using an affordable consumer-grade ECG monitor would provide sufficient data resolution for security applications.

Signal processing involves the analysis, interpretation and manipulation of the signals. Signals are characterized with the electrical representations of time-variation or the spatial varying physical quantities which may arise from different sources. Signals may be sound, image, or the biological such as ECG, EEG, radars signals and many others [3]. A typical waveform of ECG consists of several complexes, the P-complex, the QRS-complex, the T-complex and the U-complex [4]. The dominant component of the ECG is the QRS complex, which indicates the electrical depolarization of the muscles in the ventricle of the heart. Several clinical applications including ECG monitoring system in the intensive care unit, operating room and implantable defibrillator require QRS detection algorithms while the QRS is easily recognized by a human observer. Software QRS detectors are an integral part of modern computerized ECG monitoring systems. The detection of peaks in signals is an important step in many signal processing applications. The goal of this project was to develop complete heart rate variability (HRV) measurement system able to measure, store, and post-process the HRV data obtained from a subject. The QRS detector detects the waves of the electrocardiogram (ECG) signal and calculates the intervals between two successive waves to form beat to beat interval data set. The RR interval data is post-processed in the host computer to calculate statistical figures and visualize them for analysis. The post-processing algorithm is also capable of correcting to some extent the errors occurred in QRS detection by filtering out the false detections caused by noise in the measurement. The HRV measurements are usually affected only by low levels of noise, consisting mainly of amplitude modulation of QRS complex due to base-line wandering [5]. There are many uses for a reliable QRS recognition algorithm but detection is critical, not only due to physiological variation of the QRS complexes, but also due to

artifacts present in the ECG signal. Noise sources include muscle noise, artifacts due to lead movement, power-line interference, baseline wandering, and T waves with higher frequency characteristics similar to QRS complexes. Algorithm is based on optimized filtering and on simple threshold as the optimized filtering is considered to be the factor to achieve good timing accuracy. In this, band pass filter which reduces the low frequency noise and high frequency noise thereby enhance the performance. Current challenges in ECG biometric classification tasks include the extraction of features from the ECG signals to implement a model to learn hidden patterns for accurate generalization, proving the stability of the biometric and protecting against attacks [6]. In this research, we proposed biometric-based ECG signals for human authentication with non-fiducially techniques..

II. LITERATURE REVIEW

The main limitations of the system are spoof attacks, noisy data, distinctiveness, intra-class variations, and non-universality which can be overcome by a multimodal system. Also, apart from the liveliness detection, these systems provide better security against spoof attacks as compared to the uni-modal system. In [7] a prototype design was proposed for a multimodal biometrics system in which ring finger prints and left/right index, left/right near-infra-red dorsal hand vein patterns, etc. were taken. The main advantage of adding these modalities was in liveliness detection. In [8] two novel approaches were proposed, in which one was the extension of likelihood ratio-based fusion and the second was the use of fuzzy logic against spoofing attacks. In this work impact of spoofing attacks was analyzed on the multimodal biometric systems and it was observed that this scheme was more robust against the spoofing attacks as compared to the likelihood ratio and weighted sum. Jiang et al. [15] have been proposed a video based multimodal biometric approach that utilized face and speech fusion in the Laplacean subspace for speaker recognition. Fusion using the presented approach achieved better accuracy as compared to the single face or audio modality. Barrero et al. [7] presented the software-based attack against multimodal systems in which face and iris were used to check the performance. Das et al. [6] proposed a structure for software-based liveliness detection in multimodal ocular biometrics. The proposed scheme is utilized for direct attack detection. The authors also include class level liveliness detection in their work. Kavitha et al. [17] proposed a multimodal biometric framework that utilized feature level fusion to fuse the extracted features and support vector machine (SVM) classifier to detect the fake face and Gabor feature and weber local binary pattern for liveliness detection. Fingerprint images were analyzed in the spatial domain and frequency domain and final features were decided by the co-occurrence probabilities. In [16] non-reference image quality measures were proposed to distinguish between genuine and fake data. In this method, accurate classification of real versus fake iris, fingerprint, face, and finger vein data was achieved. In [20] a sparse representation-based blind image De- blurring algorithm was proposed which helps to learn smaller sub-dictionaries from the patches clustered based on dominant orientation instead of learning a single large dictionary.

The author uses the two tier authentication for secure communication in healthcare application of wireless sensor networks [21]. The unique key is used to encrypt the data in the first phase and it is generated in a decentralized fashion. It gives the security in non-trusted environment. In the second phase unique key is used as session key which is mainly used for authentication of data aggregation node from sensor nodes. This method gives confidentiality, authorization, and secure communication in wireless sensor networks healthcare applications. This security scheme is compared with the other security scheme and it is observed to provide the robust, prompt and scalable security services. In wireless personal area networks security is one of the important issues during the real time implementation of body area sensor network because of the some vulnerability [18]. In this approach, the security scheme used in body area sensor network is mainly for high level security as well as light weight protocol. This security architecture has secure transmission of data using the bio-channel and the several secure aspects for physiological data. Electrocardiographic system is one of the important machines in the medical field and it is mainly based on the wireless body area sensor networks [19]. The energy consumption and data security are two important issues in the ECG system. Many techniques are introduced for the energy consumption and security. In this approach, the author introduces a novel framework for energy consumption and secure communication. The framework is used for secure transmission of the ECG data by using the compression, encryption using RSA. SPHIT is used for compressing the ECG data and the compressed data is encrypted using the selected encryption mechanism which uses RSA. The two rate unequal error protection is used for saving energy in this security scheme. The existing schemes are compared with this security framework and the simulated results are showed improvement of 40% than the other schemes. The quality measurement is used for measuring the framework.

III. PROPOSED METHOD

We propose an intelligent heart monitoring system, which involves a patient worn ECG sensor (e.g., a smart phone) and a remote monitoring station, as well as a decision support server that interconnects these components. The decision support server analyzes the heart activity, using the Modified Pan-Tompkins algorithm based on the slope and amplitude of ECG signal to detect heartbeats and a decision tree to classify them. The QRS complex detection algorithm uses optimized bandpass-filtering to reduce false detection. Our system protects sensing data and user privacy, which is an essential attribute of dependability, by adopting signal scrambling and anonymous identity schemes. The aim of the design work is to achieve higher performance in terms of reliability and better diagnosis of patients through Peak detection. We also employ a public key cryptosystem to enable secure communication between the entities. This poses high security and detection reliability.

3.1 Process of biometric authentication and identification

Identification of a person is the most crucial step today to minimize fraud and identity theft. Hence, biometrics are used to identify an individual uniquely by comparing the original image with the data set governed by different attributes. Biometry means applying statistical analysis on biological data. It is a computerized method of identifying a person and such systems comprises of various stepped modules including a sensor, feature extraction, matching, and decision making, as shown in Figure 1. Encryption means converting data into an unreadable format by any method. This plays a major role in cryptography. Encryption, as well as decryption, is used by it. Cryptography provides authentication, integrity, and confidentiality. Encryption has two categories which are symmetric and public key encryption. The same key is used in symmetric encryption for encrypting and decrypting in symmetric, while different keys are used for encrypting and decrypting messages in public key kind [9,10]. Even after ensuring safe and secure storage and access methods of biometrics in cloud architecture, the database in which the information of biometrics is stored has to be protected from outside attackers.

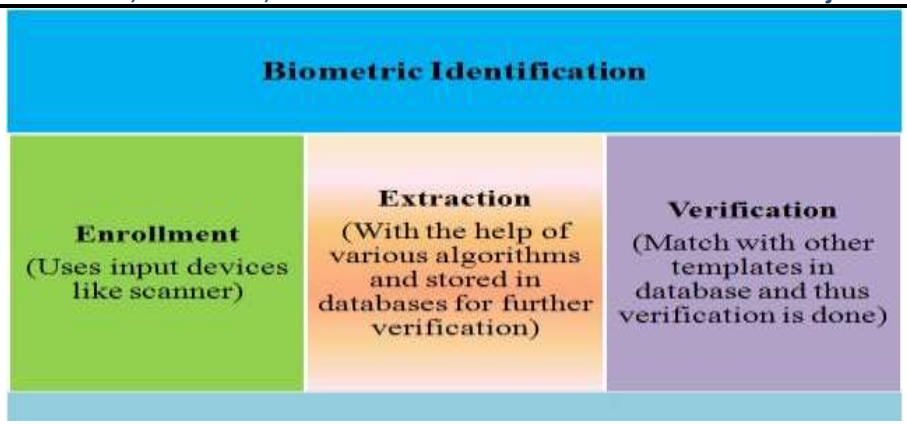

Fig1.Steps included in process of biometric authentication and identification

Various risks involved in the database are:

- Privilege abuse by the users to gain access to data other than what they are authorized to access.
- SQL injection to send unauthorized queries to access the database.
- Denial of service to the users by network flooding, tampering with the access codes or excessive resource consumption.
- Even if the database has a backup, there have been cases, where even backup tapes and hard disks have been compromised.

Even though there are these vulnerabilities associated with the database, the encryption technique will minimize the threats associated with it [22]. The encryption technique is given as follows. Specific biometric characteristics of the client are taken and are asked to generate two keys, public, and secret keys. Secret key will be used to encrypt the plain text into cipher text. The public key will be used by the server to compute on this cipher text using any specific function. These encrypted data can be decrypted by the client just using a secret key, and the client will get original data [24]. An encryption algorithm is proposed in which both additions, as well as multiplication operations, can be used on floating numbers. Before uploading an image in the cloud, the image is encrypted and then stored in the server, because if anyone gets access to the stored image, it would still be in an encrypted form so. Thus, whenever a user wants to access that image, it is only decrypted using that key used to encrypt in encryption, as shown in Figure 2.

Fig 2. Schematic of proposed data authentication and decryption technique

The finger print extraction and verification is done using modified minutae algorithm. This is the feature extraction stage where the minutiae points from the binarized image are extracted as these minutiae points are the basis for matching the two fingerprints. A minutia point can be of either type be a termination type or bifurcation type. Both of them have their own importance while using two minutiae sets for matching. Generally, a minutiae point which exists at the end of a ridge is known as termination minutia and the minutia points which exist at the cutting point or joining point of two ridges is known as bifurcation type of minutiae. These minutiae points are the basis of the analysis in which alignment and matching operations are performed. Fingerprint Image extraction and verification includes,

1. Pre-processing the test Fingerprint.
2. Extract the minutiae points.
3. Matching test Fingerprint with the database.

Table 1 gives the algorithm for fingerprint verification, in which input test fingerprint image is compared with template fingerprint image, for recognition.

Modified minutiae algorithm consists of following steps. The input is gray-scale finger print image and output is verified fingerprint image.

1. Fingerprint is binarized.
2. Thinning on binarized image.
3. Minutiae points are extracted.
4. Data matrix is generated to get the position, orientation and type of minutiae.
5. Matching of test fingerprint with template.
6. Matching score of two images is computed, if matching score is 1,images are matched and if it is 0, images are mismatched.

Generally, a typical biometric system comprises four modules, namely, sensor module, feature extraction module, template database, and matching module. Specifically, the sensor module acquires the biometric image. A set of global or local features are extracted from the acquired biometric image by the feature extraction module [25,26]. Structured feature representations are stored in the template database as template data. The matching module is responsible for comparing the query and template data to reach a match or non-match verdict. A typical biometric system carries out authentication in two stages [11,12]; the enrolment stage and verification stage, as shown in Figure 1. Take fingerprint recognition as an example. In the stage of enrolment, a user presents their finger to the fingerprint sensor and a fingerprint image is acquired by the sensor module. Certain features of the acquired fingerprint image are extracted, and further adapted or transformed to generate template data for the purpose of comparison in the verification stage. In the verification stage, the fingerprint image of a query is collected by the sensor module. The feature representations of the query fingerprint image go through the same process as in the enrolment stage, so as to obtain query data. The query data are then compared with the template data so that a matching outcome is attained.

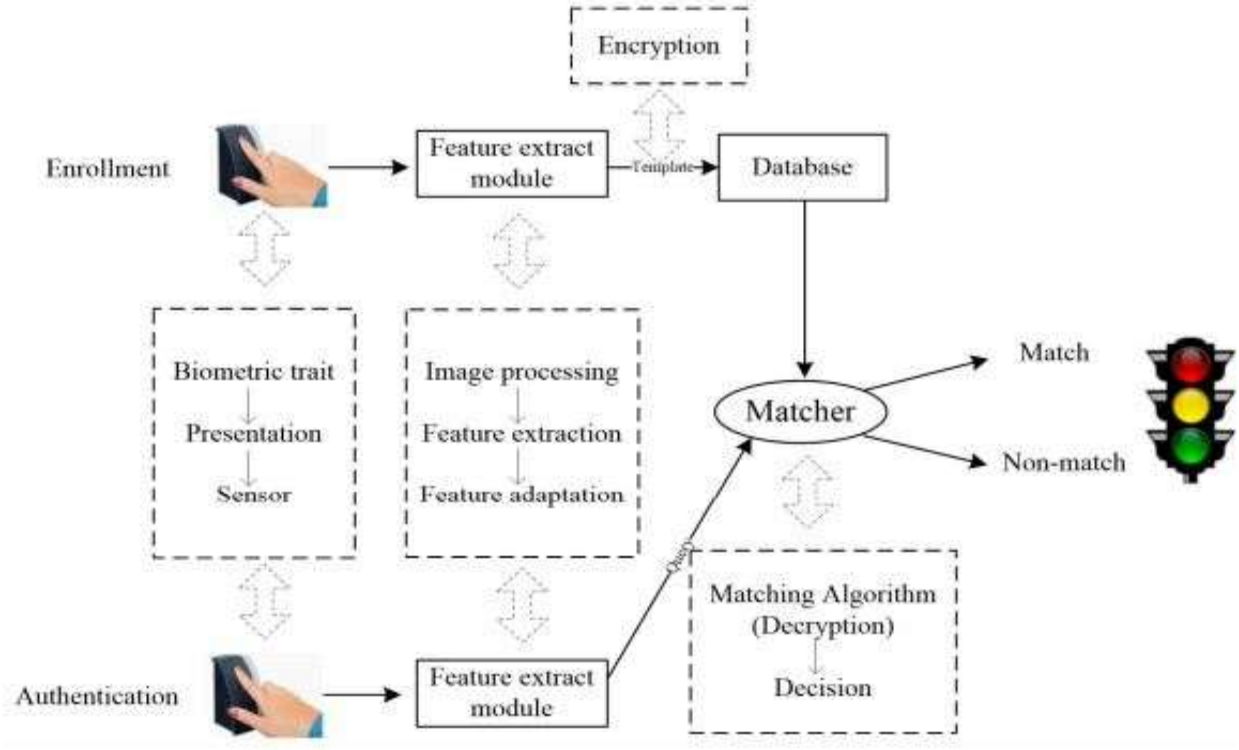

Fig 3.Fingerprint Image extraction and verification using modified minutae algorithm.

3.2 Proposed Algorithm : Modified Pan-Tompkins Algorithm

The new method called Modified Pan-Tompkins algorithm based on the slope and amplitude of ECG signal. The QRS complex detection algorithmuses optimized Bandpass-filtering to reduce false detection. The purpose of filtering is to reduce various noise components in order to achieve improved detection reliability. A schematic flow of the proposed QRS detecting system is shown in Figure 4. In general, the overall detection process can be divided into four stages: (I) Filtering, (2) Derivative, (3) Squaring and (4) R-Peak.

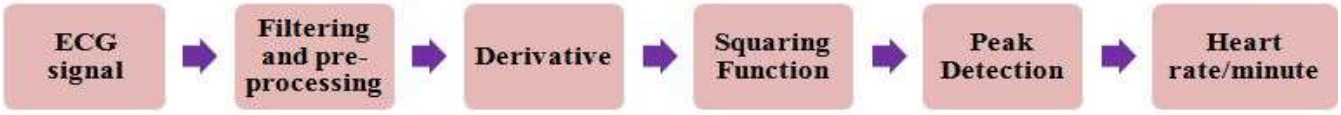

Fig 4. QRS detection

A. Filtering

When the raw ECG signal enters the system, it is first preprocessed by band pass filtering to reduce the influence of baseline wander, muscle noise, 60Hz interference, and interference in T- wave. The desirable range of pass-band 4-15 Hz which is to maximize the QRS complex energy is [I]. The low-pass and high-pass filters are cascaded to form Band-pass filter where the low frequency interference and higher frequency artifacts removed automatically. Thus bandpass allows particular frequencies to analysis the nature of a QRS complex while lower and higher frequency signals gets attenuated.

B. Derivative

To acquire the slope of QRS complex the noise free ECG signal is given to derivative block. The amplitude threshold is applied before any differentiation to the signal in order to cut horizontally the ECG signal to reduce the P and T waves influence compared to the R wave. In the presence of random signal distortion in real world signal will cause many false peak detection with higher peak distortion, peak width and height of the wave gets maximized . This can be avoided by, smoothing the derivative output of the signal, smoothing technique determines the position of the wave appearance, amplitude of the peak, and width of each peak with the particular interval of time.

C. Squaring function

After derivative the output signal is squared sequentially. All data points become positive, the derivative output is amplified nonlinearly, and the QRS complexes are emphasized as y (nT) = [x (nT)]2 (I) where, x (nT) = Input ECG signal y (nT) = Squared input signal It shows the higher frequencies m the signal, which are mainly due to the QRS complex.

D. Peak Detection

A common need for processing the signal is to identify peaks in a signal and to determine their positions, heights, and width. It detects the peak in the signal and comes after extracting the ECG features that contain QRS complex that is more emphasized compared to the noise. A peak is determined when the signal changes direction within the certain time interval. It must able to detect a large number of different QRS morphologies to be clinical useful and must be able to follow sudden changes and gradual changes. QRS complex temporal location is marked from the rising edge point of the integrated ECG Squared waveform. In the last step, two thresholds are varied according to the detection reliability. The value with higher threshold is marked as peak of the signal. Through the peak prediction algorithm the peak is detected which is effective than the amplitude thresholding technique.
Three steps to detect a QRS peak are

1. Select the value and store it to temp local maximum.
2. If newer point value is greater than temp local maximum, then store it to temp local maximum.
3. If newer point value is smaller than half of temp local max, a peak is identified and detected. Otherwise go to step 2.

Then, it is distinguished as QRS complex or noise, or for later diagnose the signal is saved.

1. Neglect all peaks which precedes larger peaks by a refractory blanking of less than 200ms [I] to ignore T waves and multiple detection of QRS complex waves.
2. If the peak is greater than the adaptive detection threshold then it is identified as a QRS complex instead of noise. DT is the detection threshold, where TC is the threshold coefficient.

NPL is the level of noise peak and QRSPL is the QRS complex peak level. To detect the true peak in ECG signal and to neglect the peaks which are too wider, too smaller or too narrow, the parameter such as slope width and threshold amplitude helps for it. This technique is used for measuring positions of peak and heights accurately, but the analysis of peak widths and areas is accurate only if the peaks are Gaussian in shape. So, this cannot be applicable for ECG signal and this becomes the main flaw of modified Pan-Tompkins algorithm.

3.3 Modified Pan-Tompkins Algorithm

The Modified Pan-Tompkins Algorithm (MPTA) consists of derivative, moving average, squaring and threshold operations as shown in figure. MPTA follow these steps: first of all there is a band-pass filter which is composed of a band pass filter and it reduces noise. After this a derivative filter is used in order to get the slope information. After that an amplitude squaring is done and then the signal is passed to a moving- window integrator. Then threshold process is done to locate R-peaks. Figure 1 shows the steps of MPTA to remove different kinds of artifacts and noise.

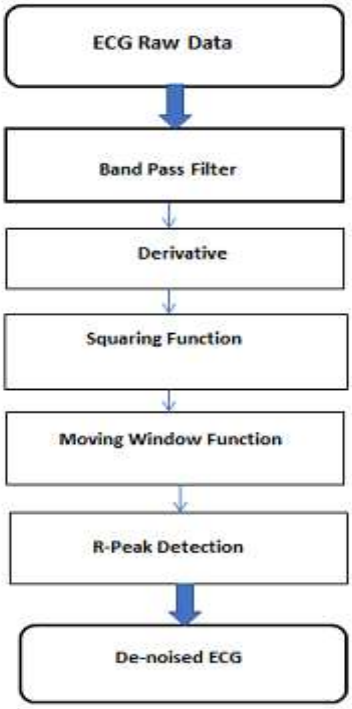

Fig 5.Modified Pan-Tompkins Algorithm

3.4 ECG data classification using modified C4.5 Algorithm

The Decision Support Server (DSS) classifies the individual heartbeats in the ECG based on decision tree learning, which is one of the most widely-employed classification techniques [27]. Its classification accuracy is competitive with other learning methods, and it is considerably efficient. The learned classification model is represented as a tree, called a decision tree. We trained the decision tree based on the modified C4.5 algorithm, which can provide prominent results, readability, flexibility and efficiency [23]. The Iterative Dichotomiser 3 (ID3) algorithm is mostly used for training the decision tree. This makes statistical-based decisions and is therefore less sensitive to errors in individual training examples. Although the ID3 algorithm is used in various domains, it is not applied to our server, because the discrete-valued target function domain cannot be applied to the ID3 algorithm. Therefore, our server uses the C4.5 algorithm, which is an extension of the basic ID3 algorithm.

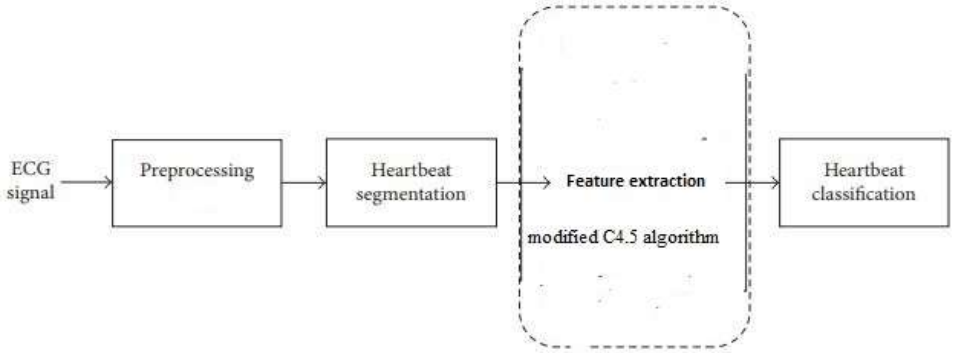

Fig 6 ECG data classification

The DSS classifies the individual heartbeats in the ECG using a decision tree learned by the C4.5algorithm, as mentioned above, and then sends the anonymous ID (AID) and analysis results to the monitoring station (MS). Each of the ECG records from the MIT-BIH arrhythmia database can contain a maximum of 11 heartbeat types, consisting of a normal beat (N) and 10 abnormal beats: left bundle branch block beat (L), right bundle branch block beat (R), atrial premature beat (A), aberrated atrial premature beat (a), premature ventricular contraction beat (V), fusion of ventricular and normal beat (F), ventricular flutter wave beat (I), atrial escape beat (e), ventricular escape beat (E) and paced beat (P).

3.5 Biometrics based security solution for ECG data

A novel and improved frame work has been proposed for providing security and authentication to the ECG data. The framework consists of the compression, encryption , biometric authentication and transmission [28]. In order to obtain high compression with less distortion, Modified SPIHT (MSPIHT) is used for the compression and modified quasi group encryption is used for encryption [13,14]. Figure clearly depicts the framework of the proposed approach which is used to improve the transmission rate and for secure communication of the ECG data.

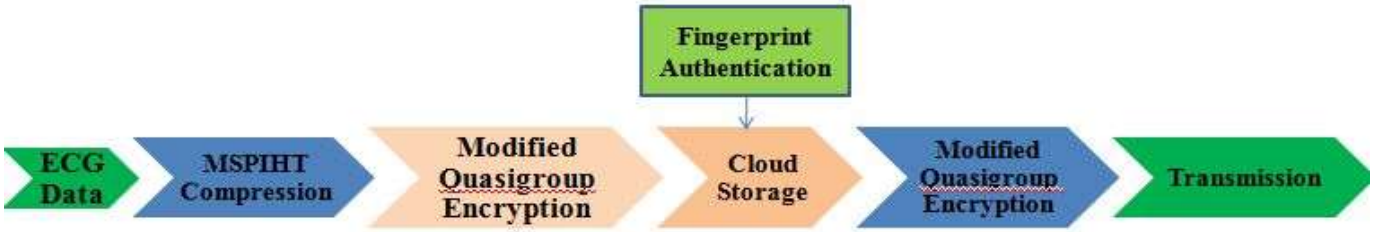

Fig 7 Security implementation in ECG data

3.6 Modified SPIHT Coder for Compression

In this MSPIHT algorithm, two concepts are mainly used for compressing the ECG data along with other parameters in the SPIHT algorithm. They are number of error bits and absolute zero tree. The insignificant or significant coefficient is used in the transform coefficients in SPIHT coding. MSPIHT compression algorithm has become an essential tool for uniformly quantizing the coefficients attained from the wavelet sub band decomposition of data. Thus, the ECG data is compressed based on the MSPIHT algorithm, as shown below.

Step 1: Wavelet coefficients are obtained from wavelet transform and initialize with number of error bits
Step 2: Select partitions of Coefficients Um
Step 3: For each $n=n_0,n_{0-1}, n_{0-2}...$
Step 4: If S_n (Um) = 0(the set is insignificant) then disregard bits in Um
Step 5:If S_0 (Um) =1 (the set is significant) then perform recursive algorithm to partition Um.
Step 6: Test sets until all significant coefficients are found.
Step 7: New coding method uses the following set of coefficients.
O (i,j) : set of coordinates for all off springs of node (i,j)
D (i,j): set of coordinates for all descendants of node (i,j)
H (i,j): set of all coordinates of spatial orientation of the highest peak of tree roots
Step 8: The lists used are
LIP: List of Insignificant Coordinates
LIS: (TYPE A) List of tree roots (i, j) of insignificant descendants D (i,j)
Or
(TYPE B) List of insignificant descendants of offspring sets L(i, j) = D (i,j) - O(i,j)
LSP: List of Significant coefficients
Step 9: Number of error bits (least significant bits) are omitted.
Step 10: List tested in order LIP, LIS,LSP for efficient embedded coding
Step 11: Initialization of Lists
LIP: coordinates of all tree roots
LSP empty: the coordinates of the tree roots are not stored in the LIS in MSPHIT algorithm because the memory consumption is more.
Step 12: Sorting And Refinement Pass
Output nth bit of all LSP members found.
Significant bits at thresholds greater than 2n.
Two bit types in stream: significant test bits, refinement bits.
Step 13: Quantization Step Update
Decrement the value of n and go to sorting pass if n is not less than 0.

3.7 ECG Encryption

Quasigroup encryption technique is observed to provide good results and hence this research work adapts quasi group encryption and certain modification has also been proposed in Quasigroup encryption for improving the security with less time consumption [29, 30].

3.7.1 Modified Quasi group Encryption: The compressed ECG data is given as an input to the quasigroup encryption and it is mainly used for the encryption of the ECG data based on the significant data scrambling properties [32]. Even though the input is constant output is improved by using the scrambler. The quasigroup encryption is based on the permutation scrambling based in the basis of the algorithm.

3.7.2 Encryption Algorithm:

Input: compressed ECG data, Encryption Key
Output: Encrypted data
1. Get the data and store in r and c respectively.
2. Convert ECG data into matrix then it is converted into a vector
3. Obtain all odd position values initially and then even position values.
4. Construct a new data matrix by filling the odd positions values followed by even position values.
5. Convert new matrix into a vector.
6. Convert the decimal key into binary key data.
7. Binary key data is embedded in the vector.
8. Convert the vector into data matrix of size (r,c).

3.8 Decryption

The decryption is the process of the constructing the inverse data matrix and it is very similar to the encryption process.

3.8.1 Decryption Algorithm:

Input: encryption data, finger print features
Output: decrypted data
1. Convert the encrypted data into the vector.
2. Convert the finger print features into binary key
3. The binary key data is initially used for decryption and stored as a vector.
4. The vector is converted to data matrix of size .
5. The data matrix is divided into the two vectors
6. The new matrix is formed by filling the odd position and even position from two vectors
7. The resulted decrypted data is obtained.

This research work proposes a novel modified Quasigroup encryption algorithm using met heuristic approach. This approach uses a heuristic algorithm called genetic algorithm for quasi group optimization. Genetic Algorithms (GAs) are one of the most promising met heuristic optimization algorithms [33]. GA looks for an optimal or sub-optimal solution of a given problem through imitating the natural evolution. The proposed security algorithm for transmitting ECG data as an input data has following advantages

1) The number of bits is reduced in the ECG data by using the compression algorithm so that the number of bits to be encrypted is also reduced.
2) It is gives more secure communication than the other existing algorithms.

IV. Results and Discussion

Before In this research, ECG signal recognition is done by performing the fingerprint authentication. Input of the system is ECG signal and output of will be result of ECG analysis. At the beginning, we will check the fingerprint authentication, if the fingerprint is belongs to the recognized person then only system will be authorized.

1. By using C# Application, Download the Dataset presented in the server (Here we are using Microsoft Default Cloud Server MYASP.NET.
2. From the Cloud, We have to download the Database. We can download all the dataset in one click or we can download the dataset one by one.

Fig 8 Dataset Download

3. After download the mat lab is run and the system will ask fingerprint for authentication process. The fingerprint image will be given as Input image.

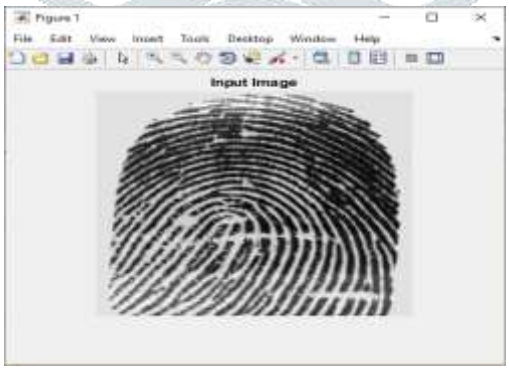

Fig 9 Input image.

4. Once the system confirmed the authorization, The ECG Raw data process begins.

Figure 10 Orientation image will give the direction of the image

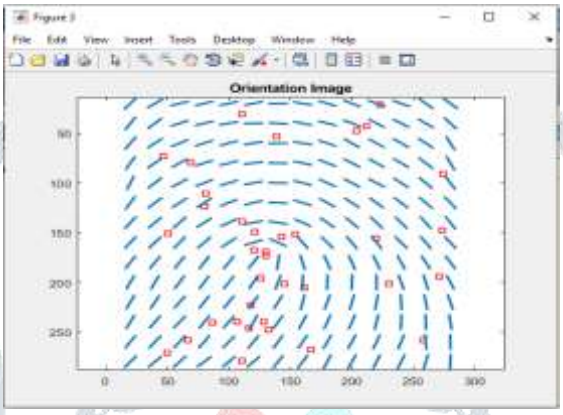

Fig 11 Orientation Image

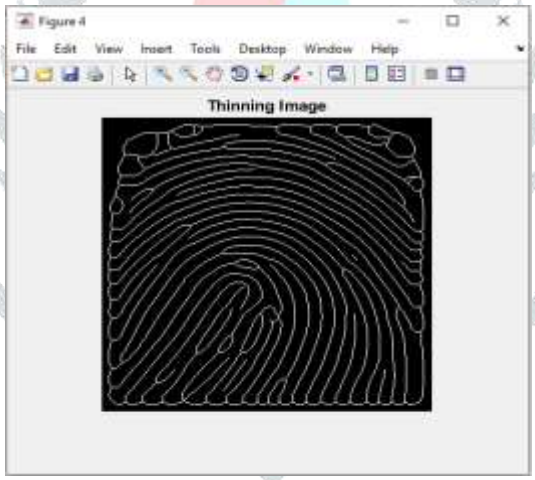

Fig 12 Thinning Image

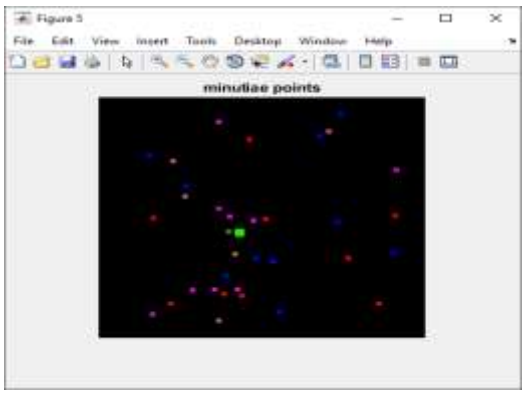

Fig 13 Minutae points

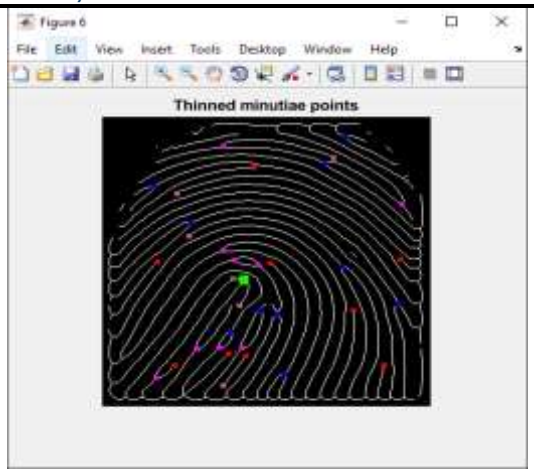

Fig 14 Thinned minutiae points

From the overlayed display of fingerprint with extracted feature of fingerprint minutiae point, we canrecognize a person is authorized or not.

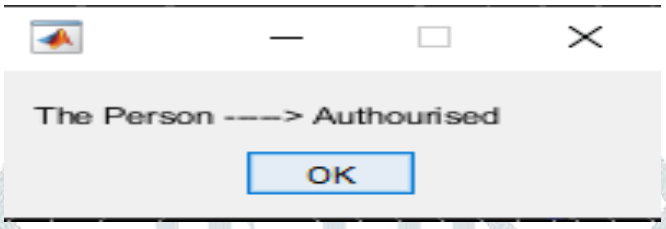

Fig 15 User Authorization

5. Finishing all the steps in the algorithm, the final result will be available the same drive where we stored the input data (new output folder).

Figure 16 represents the ECG signal. 6 plots are used. The first plot represents the raw signal, which will perform the signal acquisition from the signal input folder. Then low pass filter and high pass filter are executed . The low pass filter and high pass filter are combined as band pass filter. These are the first stage of Pan Tompkins Algorithm. In the second stage there is a derivative filter, Squared and adaptive threshold is received as the output.

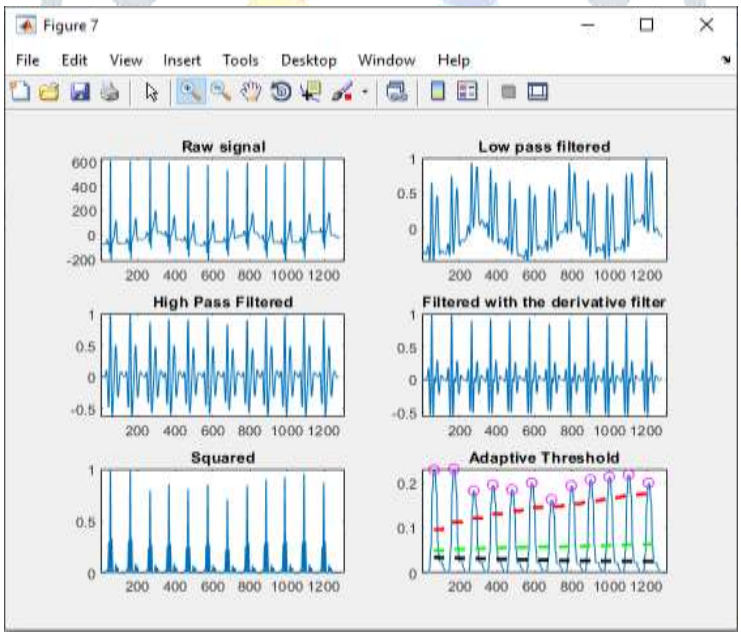

Figure 16 Raw Signal Transformation

The QRS deduction or R peak deduction is identified After that the R peak deduction will be represented as filtered signal. This means the R peak will be overlaid in the given ECG signal. Then we are having the QRS signal will be in the MVI signal. Then we are having the pulse train, that means particular location of the R peak variable and that will be represent in the ECG location. Finally we will get the Output results which will show Normal or abnormal.

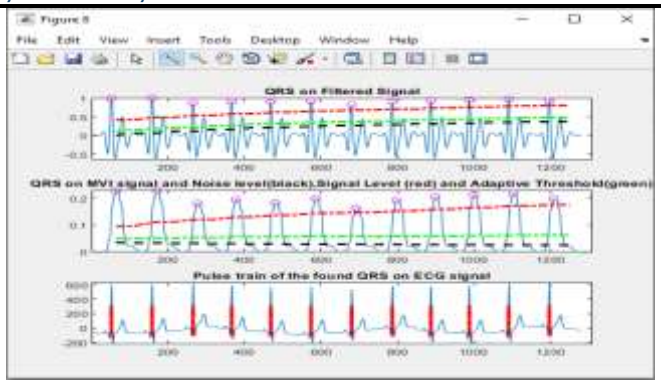

Fig 17 QRS detection

7. Finally, the output data will be uploaded once we click the upload button on the GUI.

8. The processed data will be encrypted and pushed it into the cloud server (MYASP.NET).

We proposed and applied a scheme for P-wave detection, along with the modified Pan–Tompkins algorithm, to enhance the accuracy of heartbeat detection at the first step. Second, this enhanced accuracy in the heartbeat detection naturally has a positive influence on the subsequent feature extraction process. Third, we introduced a classifier based on a decision tree and trained it using a modified C4.5 algorithm, by considering various combinations of ECG features. We rigorously investigated the security of ECG data in the cloud storage and decryption only possible with matching of fingerprint features. As a result, we achieved an average accuracy of 97.03% in recognizing arrhythmia for nine example records from the MIT-BIH arrhythmia database that we considered for our experiments, we designed a simple and effective sensing data scrambling scheme to ensure the security of streamed sensing data and adopted biometrics to preserve user privacy. Using our proposed system, medical experts can capture the intermittent ECG waveforms that may reveal or lead to a more serious problem. An accurate diagnosis of arrhythmia based on a heartbeat detection and classification algorithm can be achieved in real time, which is beneficial for remote medical care. This system represents a low-cost solution, which could be affordable across medical environments.

V. CONCLUSION

ECG data security has become an essential issue to be taken into consideration in the medical analysis. In recent years, due to the improvisation of various attacks, the necessity of efficient security system has taken its own importance. In this research, an efficient cryptographic security framework has been proposed to provide security to the ECG data. This approach includes the encryption and compression algorithm for ECG data along with fingerprint authentication. An efficient modified quasi group encryption algorithm and modified SPHIT compression algorithm is used for encryption and compression of the ECG data respectively in the proposed framework. Quasi group encryption is observed to provide significant results and improves the performance of the Quasi group algorithm by integrating Genetic Algorithm. The proposed algorithm outperforms the other algorithms and it provides the strong and fast secure communication..

REFERENCES

[1] Arteaga-Falconi, J. S., Al Osman, H., & El Saddik, A. (2018). ECG and fingerprint bimodal authentication. *Sustainable cities and society*, *40*, 274-283.

[2] Choi, G. H., Lim, K., & Pan, S. B. (2021). Driver Identification System Using Normalized Electrocardiogram Based on Adaptive Threshold Filter for Intelligent Vehicles. *Sensors*, *21*(1), 202.

[3] Cunha, J. P. T. D. S., & Paiva, J. I. S. (2021). *U.S. Patent No. 10,885,361*. Washington, DC: U.S. Patent and Trademark Office.

[4] Das A, Pal U, Ferrer MA, Blumenstein M. A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics. Pattern Recognit Lett. 2016;82:232–41.

[5] Gomez-Barrero M, Galbally J, Fierrez J. Efcient software attack to multimodal biometric systems and its application to face and iris fusion. Pattern Recognit Lett. 2014;36:243–53.

[6] Hammad, M., & Wang, K. (2019). Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. *Computers & Security*, *81*, 107-122.

[7] Hammad, M., Liu, Y., & Wang, K. (2018). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE Access*, *7*, 26527-26542.

[8] Huang, P., Guo, L., Li, M., & Fang, Y. (2019). Practical privacy-preserving ECG-based authentication for IoT-based healthcare. *IEEE Internet of Things Journal*, *6*(5), 9200-9210.

[9] Huang, Y., Yang, G., Wang, K., & Yin, Y. (2021). Multi-view discriminant analysis with sample diversity for ECG biometric recognition. *Pattern Recognition Letters*.

[10] Husain, K., Mohd Zahid, M. S., Ul Hassan, S., Hasbullah, S., & Mandala, S. (2021). Advances of ECG Sensors from Hardware, Software and Format Interoperability Perspectives. *Electronics*, *10*(2), 105.

[11] Husain, K., Zahid, M. S. M., Hassan, S. U., Hasbullah, S., & Mandala, S. (2021). Advances of ECG Sensors from Hardware, Software and Format Interoperability Perspectives. Electronics 2021, 10, 105.

[12] Izharuddin, Farooq, O., & Rafiq, M. Q. (2015). Partial encryption of ECG with reduced complexity and its FPGA implementation. *International Journal of Biomedical Engineering and Technology*, *17*(4), 398-417.

[13] Jati, G., Rachmasari, A. R., Jatmiko, W., Mursanto, P., & Sediono, W. (2017). An efficient secure ECG compression based on 2D-SPIHT and SIT algorithm. In *2017 International Workshop on Big Data and Information Security (IWBIS)* (pp. 155-160). IEEE.

[14] Jiang RM, Sadka AH, Crookes D. Multimodal biometric human recognition for perceptual human–computer interaction. IEEE Trans Syst Man Cybern Part C Appl Rev. 2010;40:676–81.

[15] Kaul, A., Arora, A. S., & Chauhan, S. (2021). 6 AI-Based Approach for Person Identification Using ECG Biometric. *AI and Deep Learning in Biometric Security: Trends, Potential, and Challenges*, 133.

[16] Kavitha P, Vijaya K. Optimal feature-level fusion and layered k-support vector machine for spoofng face detection. Multimed Tools Appl. 2018;77:26509–43.

[17] Khan, F. H., Shams, R., Rizvi, H. H., & Qazi, F. (2018). A secure crypto base authentication and communication suite in Wireless Body Area Network (WBAN) for IoT applications. *Wireless Personal Communications*, *103*(4), 2877-2890.

[18] Lynn, H. M., Kim, P., & Pan, S. B. (2021). Data Independent Acquisition Based Bi-Directional Deep Networks for Biometric ECG Authentication. *Applied Sciences*, *11*(3), 1125.

[19] Masdari, M., Ahmadzadeh, S., & Bidaki, M. (2017). I ssues, Journal of Network and Computer Applications.

[20] Manishaben Jaiswal, "CYBERCRIME CATEGORIES AND PREVENTION", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.7, Issue 1, pp.526-536, February 2019, Available at: http://www.ijcrt.org/papers/IJCRT1134229.pdf

[21] Odinaka, I., Lai, P. H., Kaplan, A. D., O'Sullivan, J. A., Sirevaag, E. J., & Rohrbaugh, J. W. (2012). ECG biometric recognition: A comparative analysis. *IEEE Transactions on Information Forensics and Security*, *7*(6), 1812-1824.

[22] Rodrigues RN, Ling LL, Govindaraju V. Robustness of multimodal biometric fusion methods against spoof attacks. J Vis Lang Comput. 2009;20:169–79.

[23] Safie, S. I., Soraghan, J. J., & Petropoulakis, L. (2011). Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR). *IEEE Transactions on Information Forensics and Security*, *6*(4), 1315-1322.

[24] Shahin MK, Badawi AM, Rasmy ME. A multimodal hand vein, hand geometry, and fngerprint prototype design for high security biometrics. In: Proceedings of the 2008 Cairo international biomedical engineering conference. IEEE; 2008. p. 1–6.

[25] Singh K, Vishwakarma DK, Walia GS. Blind image deblurring via gradient orientation-based clustered coupled sparse dictionaries. Pattern Anal Appl. 2019;22:549–58.

[26] Söllinger D, Trung P, Uhl A. Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofng. IET Biom. 2018;7:314–24.

[27] Sufi, F., Khalil, I., & Hu, J. (2010). ECG-based authentication. In *Handbook of information and communication security* (pp. 309-331). Springer, Berlin, Heidelberg.

[28] Sujatha, S., & Govindaraju, R. (2013). A secure crypto based ECG data communication using modified SPHIT and modified quasigroup encryption. *International Journal of Computer Applications*, *78*(6).

[29] Tan, R., & Perkowski, M. (2017). Toward improving electrocardiogram (ECG) biometric verification using mobile sensors: A two-stage classifier approach. *Sensors*, *17*(2), 410.

[30] Wati, V., Kusrini, K., Al Fatta, H., & Kapoor, N. (2021). Security of facial biometric authentication for attendance system. *Multimedia Tools and Applications*, 1-22.

[31] Wild P, Radu P, Chen L, Ferryman J. Robust multimodal face and fngerprint fusion in the presence of spoofng attacks. Pattern Recognit. 2016;50:17–25.

[32] Zanddizari, H., Rajan, S., Rabah, H., & Zarrabi, H. (2021). Privacy Assured Recovery of Compressively Sensed ECG signals. *arXiv preprint arXiv:2101.09416*.

[33] Zhao, C. X., Wysocki, T., Agrafioti, F., & Hatzinakos, D. (2012, September). Securing handheld devices and fingerprint readers with ECG biometrics. In *2012 IEEE fifth international conference on biometrics: theory, applications and systems (BTAS)* (pp. 150-155).