RESEARCH ARTICLE OPEN ACCESS

A Study of Techniques on Securing Patient Confidiental Information by Using Ecg Steganography

B.Sivaranjani*, Dr.N.Radha**
**(Research Scholar, Department of Computer Science, PSGR Krishnammal College For Women, Coimbatore, India.)*
***(Assistant Professor, Department of Computer Science, PSGR Krishnammal College For Women, Coimbatore, India.)*

ABSTRACT
Breaches and identity theft of medical data are on the rise. The advancement of electronic medical records has raised new concerns about privacy, balanced, duplication of services and medical errors. Modern issues include the degree of disclosure of information to insurance companies, employers, and other third parties. Medical privacy is the practice of maintaining the security and confidentiality of patient records. Several algorithms and techniques were proposed for the secured transmission of data and to protect user's privacy. Cryptography and steganography are the two major protection mechanisms that are defined for the protection of security issues where biometric form of security is provided using ECG Signal. In this paper, a study of various techniques used for securing data and how biometrics were used for the hiding data are discussed.

Keywords: *Steganography, Cryptography, Wavelet transform, Discrete Cosine transform*.

Date of Submission: 08-11-2017 Date of acceptance: 28-11-2017

I. INTRODUCTION

Many concepts are discussed to provide secure transmission. The patient data is secured by using cryptography and steganography. In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it. The intended information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating a cipher text that can only read if text is decrypted. A specific encryption method is therefore required to protect the information during transmission. However, conventional block cipher algorithms such as data encryption standard (DES), triple data encryption standard (Triple-DES), and international data encryption algorithm (IDEA) are unsuitable for image encryption because of the special storage characteristics of images [2]. Conventional image encryption algorithms are primarily based on the position permutation, such as Arnold transform, magic square matrix, and fractal curve scan [3]. In this paper, RSA Algorithm is used for encryption and decryption.

Steganography Imaging System (SIS) is a system that is capable of hiding the data inside the image. The system is using 2 layers of security in order to maintain data privacy. Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Privacy, on the other hand, is the ability of an individual or group to isolate them or information about themselves and thereby reveal them selectively. Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues.

To provide high data security, an embedding operation is carried out which hides the information in the ECG signal. In order to hide the data, the time domain signal should be converted into the frequency domain. Wavelet Transform decomposes signals as a superposition of simple units from which the original signals can be reconstructed. The Fourier Transform decomposes signals into sine and cosine functions of different frequencies, while the Wavelet Transform decomposes signals into wavelets. Since the Fourier Transform is a global integration transform and there is no time factor in it, it cannot effectively analyze non-stationary signals whose statistical properties change with time. In order to analyze non-stationary signals, we need to decompose signals into units that are localized in both the time and frequency domains. During the past several years, a number of researchers have made efforts on this issue and have attempted to design secure bio-cryptosystems. This paper shows several techniques and discusses their advantages and disadvantages.

II. BACKGROUND STUDY

Jiapu pan et al.,[1] proposed a real-time algorithm for detection of the QRS complexes of ECG signals. It reliably recognizes QRS complexes based upon digital analyses of slope, amplitude, and width. A special digital band pass filter reduces false detections caused by the various types of interference present in ECG signals. This filtering permits use of low thresholds, thereby increasing detection sensitivity. The algorithm automatically adjusts thresholds and parameters periodically to adapt to such ECG changes as QRS morphology and heart rate. Widely used Holter tape recording requires. Holter scanning device that includes a QRS detect to analyze the tapes much faster than real time. Currently under developments are arrhythmia monitors for ambulatory patients which analyze the ECG in real time.

J. Parak et al.,[2] proposed the utilization of digital signal filtering on electrocardiogram (ECG). Designed filters are focused on removing supply network 50 Hz frequency and breathing muscle artefacts. Moreover, this paper contains description of three heart rate frequency detection algorithms from ECG. Algorithms are based on statistical and differential mathematical methods. All of the methods are compared on stress test measurements. All described methods are suitable for next simple implementation to a microprocessor for real-time signal processing and analysing**.** The frequency measurement issued in many medical or sport applications like stress tests or life treating situation prediction. One of possible ways how to get heart rate frequency is compute it from the ECG signal.

Nikhil S. Kale., [3] proposed an electrocardiogram is common bio-signals used to detect the heart activities by non-invasive techniques. A wavelet based de-noising algorithm on ECG signals is used for extracting features such as amplitude of the ECG signal. Signal processing is done by removing high frequencies components using the proposed algorithm. Component analysis is done using moving average filter and first order derivative filter. Simulation shows satisfactory result of ECG signal analysis. It routinely accesses the muscular and electrical behaviour of the heart. In biomedical engineering most commonly used method are digital signal processing and data analysis.

Z. Piotrowski et al.,[4] proposed an algorithm for Heart Rate (HR) detection used in electrocardiogram monitoring system as well as algorithm for Heart Rate Variability (HRV) estimation. During the training dedicated flights, military pilots are monitored for checking their susceptibility to stress and self-control. ECG data-logger as a personal portable device is collecting biological signal during the testing flight. Computed HR values together with Accumulated Reference Pattern PQRST complex (ARP) are estimates of pilot's health. ECG analysis is performed using Short-term Autocorrelation Center Clipping (SACC) method. SACC method dedicated for HR detection and ECG R-pointers analysis is very robust for the noisy environment.HRV parameters estimation is based on advanced spectral analysis of electrocardiogram (tachogram of RR values). HRV estimation is non invasive method of estimation the Sympathetic and Parasympathetic Nervous System influence on the heart rate.

ShikhaKuchhal et al.,[5] proposed that RSA algorithm depends on the decomposition of large prime numbers. In the algorithm, two large prime numbers are used to construct public key and private key. In order to achieve maximum efficiency, the symmetric key algorithm and public key algorithm are always combined together. That is, using a symmetric key algorithm to encrypt the confidential information needed to be sent, while using the RSA algorithm to encrypt the key. This takes advantages of both the kinds of cryptography, namely high speed DES and key management using RSA algorithm which is of convenience and security. Therefore, distribution of the private key and saving both transmission keys are very important. This document briefly introduces the concept of RSA algorithm, and thereby design and analyze the performance of our improved implementation. The authors have developed a program for encrypting and decrypting text files. In addition, the encryption procedure and code implementation is provided.

Ching-Kun Chen et al.[6] proposed a secure communication system, a pair of Lorenz-based synchronized circuits were developed by using operational amplifiers, resistors, capacitors and multipliers. The verification presented in volume numerical simulation and hardware implementation to demonstrate feasibility of the proposed method. High quality randomness in ECG signals results in a widely expanded key space, making it an ideal key generator for personalized data encryption. Lyapunov exponent's spectrum to extract the features of human ECG and use them as a secret key to encrypt images and text messages for secure data transmission. The chaotic synchronization system consists of a driver circuit and a response circuit. This configuration forms an indecipherable scheme that is useful for personalized data transmission, in which extreme security is of primary concern.

Rosziati Ibrahim et al.,[7] proposed an algorithm to hide data inside image using steganography technique. The proposed algorithm uses binary codes and pixels inside the image. The zipped file is used before it is converted in to binary codes to maximize the storage of data inside the image. Various sizes of data are stored inside the images and the PSNR (Peak signal-to-noise ratio) is also captured for each of the images tested. Based on the PSNR value of each images, the stego image has a higher PSNR value. Hence this new steganography algorithm is very efficient to hide the data inside the image.

D. Seetha1 et al.,[8] proposed a technique to hide a text of a secret message in the pixels of the image in such a manner that the human visual system is not able to distinguish between the original and the stego-image, but it can be easily performed by a specialized reader machine. This paper includes the basis of a wavelet-based low-throughput secret key Steganography system that requires the exchange of a secret key (stego-key) prior to communication. And, a new algorithm to hide data inside image using Steganography technique. The proposed algorithm uses binary codes and pixels inside an image. The zipped file is used before it is converted to binary codes to maximize the storage of data inside the image.

Ranjeeta Kaushik et al.,[9] proposed a semi-blind watermarking technique of embedding the color watermark using curvelet coefficient in RGB cover image has been proposed. The technique used the concept of HVS that the human eyes are not much sensitive to blue color. So the blue color plane of the cover image is used as embedding domain. A bit planes method is also used, the most significant bit (MSB) plane of watermark image is used as embedding information. Selected scale and orientation of the curvelet coefficients of the blue channel in the cover image has been used for embedding the watermark information. All other 0-7 bit planes are used as a key at the time of extraction. The results of the watermarking scheme have been analyzed by different quality assessment metric such as PSNR, Correlation Coefficient (CC) and Mean Structure Similarity Index Measure (MSSIM). The experimental results show that the proposed technique gives the good invisibility of watermark, quality of extracted watermark and robustness against different attacks.

Rongrong Ni et al.,[10] proposed a secure semi-blind watermarking technique based on iteration mapping and image features. An image] (gray or color) is divided into blocks of fixed size that are analyzed using fractal dimension to determine their properties. The feature blocks containing edges and textures are used to form a feature label. The watermark is the fusion of image feature label and a binary copyright symbol. Arnold iteration transform is employed for constructing the watermark to increase the security. The secure image adaptive watermark is then embedded in the feature blocks by modifying DCT middle-frequency coefficients. The detection and extraction procedure is a semi-blind, i.e., it does not need the original image. Only those who have the original watermark and the key can detect and extract the right watermark, which makes the approach have high security level.

III. COMPARISON OF DIFFERENT TECHNIQUES

The merits and demerits of different techniques adopted by authors have been analysed and summarized in the following table:

S.NO	TITLE	AUTHORS	METHOD	MERIT	DEMERITS
1	A real-time QRS detection algorithm	Jiapu pan and willis j. Tompkins,	Holter devices,z80 assembly language	Reliability in low pass filtering	Lack in detecting false rate
2	ECG signal processing and heart rate Frequency detection methods	J. Parak, j. Havlik	Digital filters	Saves the computing time	Difficult in applying real-time processing
3	Recognition of various waves from electrocardiogram by using wavelet transform	Nikhil s. Kale, Dr.sunil s. Morade	Denoising, moving filter, DCT, a new r-peak	Reduced amount of computational time	Lack in accuracy
4	Robust algorithm for heart rate (HR) detection And heart rate variability (HRV) estimation	Z.piotrowskiaan dk. Rózanowskib	Accumulated reference pattern (ARP) PQRST complex, heart rate variability (HRV)	Easy computation	Robust
5	Data encryption and transmission based on personal ecg signals	Ching-kun chen, chun-lianglin, shyan-lung linandcheng-tang chiang	Lyapunov exponents, Henon map	Feasibility and effectiveness	Difficult in real time system
6	Data security using RSA algorithm in matlab	Shikhakuchhal, Ishankkuchhal	RSA, encryption, decryption	Enhanced security	Depends more security key
7	Steganography Algorithm to Hide Secret Message inside An Image	Rosziati Ibrahim and TeohSukKuan	Steganography algorithm, secret key, Image processing, data retrieval	Provides layers of security	Feature extraction needs further enhancements
8	A Study on Steganography to Hide Secret Message Inside an Image	D.Seetha, Dr.P.Eswaran	Steganography, Image, steganographic, stego image, hide, Secret Message.	Improves Security and privacy	High computational complexity
9	Semi-blind watermarking scheme For RGB image using curvelet Transform	Ranjeetakaushik , Sanjaysharma and R. Raheja	Digital watermarking, curvelet transform, Bit plane	Good invisibility	Feature extraction needs
10	Secure semi-blind watermarking based on iteration mapping and Image features	Rongrong Nia, Qiuqiruana, H.D. Chengb	Semi-blind watermarking, Fractal dimension, Image features, DCT, Arnold iteration transform, Coefficient relation	Robust	Lacks optimal performance

Table 1: Summary of different techniques used for data security

IV. CONCLUSION

According to this study, above discussed algorithms is used to hide confidential data inside the ECG signal. All suggested methods provide an authentication technique to prevent unauthorized persons from gaining access to the confidential data. This confidential data provide a secure communication in health care systems. This study helps in understanding the QRS Complex detection of heart beat, filtering the signal in heart beat, discussing various encryption techniques like RSA, DES, Triple DES, are used for encryption of patient data over network to secure transmission. Then finally watermarked images are sent and receive to over network which prevent form hacker or unauthorised user in network. Future implementation can be secure using biometric key generation or by using multi biometric recognization of data to secure in network.

REFERENCES

[1] Jiapu Pan And Willis J. Tompkins “*A Real-Time QRS Detection Algorithm”* IEEE Transactions On Biomedical Engineering, Volume:32, Issue:3, March 1985.

[2] J. Parak, J. Havlik *“ECG Signal Processing And Heart Rate Frequency Detection Methods”* Volume: 01, 2006.

[3] Nikhil S. Kale, Dr.Sunil S.Morade *“Recognition Of Various Waves From Electrocardiogram By Using Wavelet Transform”* International Research Journal Of Engineering And Technology, ISSN: 2395 -0056 Volume:3, Issue:6, June-2016.

[4] Z. Piotrowski , K. Rózanowski *“Robust Algorithm For Heart Rate (HR) Detection And Heart Rate Variability (HRV) Estimation”,* Volume:118, 2010.

[5] Ching-Kun Chen, Chun-Liang Lin, Shyan-Lung Lin and Cheng-Tang Chiang*, “Data Encryption And Transmission Based On Personal ECG Signals”*, Sensor Network Data Communication, ISSN:2090-4886, 2015.

[6] Shikha Kuchhal, Ishank Kuchhal *“Data Security Using RSA Algorithm in Mat lab*”,ISSN: 2278 – 0211, Volume:2, Issue:7, 2010.

[7] Rosziati Ibrahim And Teoh Suk Kuan *“Steganography Algorithm To Hide Secret Message Inside An Image”* Computer Technology And Application, ISSN 102-108, 2006.

[8] D. Seetha1, Dr.P.Eswaran *“A Study On Steganography To Hide Secret Message Inside An Image”* International Journal Of P2P Network Trends And Technology (IJPTT), Volume:3, Issue:5, June 2013.

[9] Ranjeeta Kaushik1, Sanjay Sharma2 And L. R. Raheja3 *“A Semi-Blind Watermarking Scheme For RGB Image Using Curvelet Transform*” International Journal In Foundations Of Computer Science & Technology, ISSN:2017.7101, Volume:7, Issue:1, January 2017.

[10] Rongrong Nia, Qiuqi Ruana, H.D. Chengb, *“Secure Semi-Blind watermarking Based On Iteration Mapping And Image Features”,* The Journal Of Pattern Recognition ISSN:357 – 368,2005.

B.Sivaranjani A Study of Techniques on Securing Patient Confidential Information by Using Ecg Steganography.” International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 11, 2017, pp. 75-79.