CHAPTER-1

1.1ABSTRACT

In the current open society and with the growth of human rights, people are more and more concerned about the privacy of their information and other important data. This study makes use of electrocardiography (ECG) data in order to protect individual information. New technologies in multimedia and communication fields have introduced new ways to transfer and save the medical image data through open networks, which has introduced new risks of inappropriate use of medical information.  Electrocardiograms as personal data are being applied more and more as a biometric and deserve to be protected. In this paper, a wavelet based steg-anography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data. Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems.. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, some distortion measurement metrics have been used: the Percentage Residual Difference (PRD) , the root mean square error(RMSE), peak to peak signal to niose ratio(PSNR) and correlation coeffiecient.It is found that the proposed technique provides high security protection for patients data with low distortion and ECG data remains diagnosable after watermarking (i.e. hiding patient confidential data) and as well as after watermarks (i.e. hidden data) are removed from the watermarked data.

**1.2 PROBLEM STATEMENT**

The ECG signal is popularly used for diagnosis of various cardiovascular diseases. In recent times, the ECG signal is also being used for biometric security systems. As the ECG signals contain private health information, along with personal identification data, it needs to be secured before transmission through various public networks to avoid the data being compromised. Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two sub-categories. Firstly, there are techniques that are based on encryption and cryptographic algorithms. These techniques are used to secure data during the communication and storage. As a result, the final data will be stored in encrypted format. The disadvantage of using encryption based techniques is its large computational overhead. Therefore, encryption based methods are not suitable in resource-constrained mobile environment. Other techniques are called steganography techniques; Steganography is the art of hiding secret information inside another type of data called host data .

**1.3 LITERATURE SURVEY**

* [**V. Sankari**](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.V.%20Sankari.QT.&newsearch=true) **and K. Nandhini**

**Proposed a Steganography technique to secure patient confidential information using ECG signal**.

**ABSTRACT:**

The number of aging population are growing significantly. In accordance with Health Insurance Portability and Accountability Act (HIPAA) the patient's privacy and security is important in the protection of healthcare privacy. Point-Of-care (PoC) is an application used in hospitals widely around the world. The Security Regulations are implemented to provide data integrity, confidentiality, and availability. Therefore, patients ECG signal and other physiological readings such as temperature, blood pressure, glucose reading, position, etc., are collected at homes by using Body Sensor Networks (BSNs) will be transmitted and diagnosed by remote patient monitoring systems. At the same cost that the patient confidentiality is protected against intruders while data traverse in open network and stored in hospital servers. In this project, to fulfill HIPAA act, a Discrete Wavelet Transform based steganography technique has been proposed. DWT technique allow ECG signal to put out of sight the patient confidential data and thus guarantees the patient's privacy and confidentiality. In addition the following mechanism were incorporated in this project: (1) encryption and decryption for data confidentiality and integrity (2) a three-tier security for data (3) ECG based Steganography to exchange data. A degree of high privacy is guaranteed for patient and simultaneously the Stego ECG remains diagnosable. Our scheme also ensures security, scalability, and efficiency.

* **N. Suganya , M.Marimuthu**

Proposed ECG Steganography Based Privacy Protecting Of Medical Data for Telemedicine Application.

**ABSTRACT:**

The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in ECG signals. The proposed encryption technique used to encrypt the confidential data into unreadable form and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After data encryption, the data hider will conceal the secret data into the ECG signal coefficients. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using chaos crypto system. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Here the discrete wavelet transformation is used to decompose an ECG signal to different frequency sub bands. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the high frequency coefficients. In the data extraction module, the secret data will be extracted by using relevant key for choosing the relevant data to extract the data. By using the decryption keys, extracted text data will be decrypted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.

* [**Ayman Ibaida**](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Ayman%20Ibaida.QT.&newsearch=true) **and** [**Ibrahim Khalil**](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Ibrahim%20Khalil.QT.&newsearch=true)

**Proposed a Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems.**

**ABSTRACT:**

With the growing number of aging population and a significant portion of that suffering from cardiac diseases, it is conceivable that remote ECG patient monitoring systems are expected to be widely used as point-of-care (PoC) applications in hospitals around the world. Therefore, huge amount of ECG signal collected by body sensor networks from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level, etc., and diagnosed by those remote patient monitoring systems. It is utterly important that patient confidentiality is protected while data are being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. In this paper, a wavelet-based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference and the wavelet weighted PRD. It is found that the proposed technique provides high-security protection for patients data with low (less than 1%) distortion and ECG data remain diagnosable after watermarking (i.e., hiding patient confidential data) and as well as after watermarks (i.e., hidden data) are removed from the watermarked data.

* **Mekala.R , Vanitha .S**

**PROPOSED A PRIVACY PROTECTION OF MEDICAL DATAS USING ECG STEGANOGRAPHY.**

**ABSTRACT:**

In wireless networks, the bio-medical data may be vulnerable to attacks like tampering, hacking etc.This paper proposes wavelet based steganography technique which is used to provide more security which combines encryption and concealing technique to protect patient confidential data while transmitted over the public network. To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics such as Percentage RMSE Difference (PRD) and the other error performance metrics such as PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error).

* **Ms. Pawar Kshetramala Dilip, Prof. V. B. Raskar**

**Proposed Hiding Patient Confidential Information in ECG Signal Using DWT Technique.**

**ABSTRACT:**

The patient's confidential data should be safe and secure these is Act by Health Insurance Portability and Accountability Act (HIPAA). At the same time, there is a significantly growth in population. Numbers of patient care centers are used usually around the world in a Point - Of - care (PoC) applications. The Security systems are implemented to provide data integrity, privacy, and accessibility. Therefore, ECG signal of the patients and other physiological data of the patient’s like body temperature, glucose level, blood pressure, position, etc., are collected by Body Sensor Networks (BSNs) at home. After that it will transmitted over network and then stored at hospital server. In this paper, it used the steganography method which is depending on discrete wavelet transform to accomplish HIPAA act. DWT technique is applied on the ECG signal to hide confidential information of the patient which provides privacy to confidential information. High degree privacy is provided to patient, also Stego ECG remains diagnosable. In this paper the steganography technique is used to provide the three tire securities to patient’s data. Our system also ensures safety, scalability, and effectiveness.

* **Anish Singh Shekhawat ,Arnav Jain and Dipti Patil.**

**Proposed A Study of ECG Steganography for Securing Patient’s Confidential Data based on Wavelet Transformation.**

**ABSTRACT:**

The ECG signal is popularly used for diagnosis of various cardiovascular diseases. In recent times, the ECG signal is also being used for biometric security systems. As the ECG signals contain private health information, along with personal identification data, it needs to be secured before transmission through various public networks to avoid the data being compromised. This paper discusses various data encryption techniques along with data embedding using signal transformation to ensure that the sanctity of the information.

* **Treesa Joseph, Remya U L**

**Porposed An**  **ECG Steganography based privacy protection of medical datas for telemedicine application**

**ABSTRACT:**

Over 20 million people worldwide have abnormal electrocardiogram (ECG) signals, i.e., arrhythmias, each year. Most of the cardiac patients are elders.And if they increasingly move to nursing homes, it is a necessary tendency to reduce the medical labor cost by deploying self-organized wireless cardiac-monitoring hardware/ software systems in an area with a radius of hundreds of feet. Such medical information networks could allow the doctors to immediately capture the arrhythmia events of any patient without leaving their offices. In this paper, a wavelet based steganography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data.Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems. An added benefit is the freedom of movement for patients due to the wireless networking technologies. To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics, the Percentage Residual Difference (PRD) has been used.