Steganography Based Authenticated Data Sharing in Health Care

P. Thangaraj, M. Salomi, A. Devipriya
1,2,3 Department of CSE, KPR Institute of Engineering and Technology, India

Abstract - As per Health Insurance Portability and Accountability Act (HIPAA) the patient's protection and protection are significant in assurance of medical care protection. Simultaneously, the quantity of maturing populace is developing essentially. Purpose Of-care in medical clinics utilized generally around the globe. The Security Regulations are represented in order to provide data veracity, privacy, and accessibility. Consequently, patient's ECG along with other physiological signals, for example, temperature, pulse, glucose reading, position, and so forth, were gathered by utilizing Body Sensor Networks (BSNs) and transmitted. At a similar cost, understanding protection is ensured against stalkers while information direct in vulnerable organization and placed in medical clinic workers. Likewise, the accompanying system was consolidated in this venture: (1) encryption and decryption for information classification and trustworthiness (2) ECG based Steganography to trade information. Our plan additionally guarantees security, efficiency, and scalability.

Keywords - Steganography, ECG, Watermarking, Encryption, Wavelet, Confidential

1. Introduction
As per HIPAA guidelines, the patient’s secret data transmitted across the public organization which is ensured and safe. Understanding security is significant that an affected person can control who all can utilize their secret wellbeing data, for example, phone number, address, name, and care number and who all can get to patient's information and who all can't. Simultaneously number of maturing populaces is in-wrinkling essentially; observing affected person at their place can diminish expanding traffic in emergency clinics and clinical focuses. To give secrecy trustworthiness, and accessibility is the essential objective. Steganography includes concealing data. Message hiding diminishes the opportunity of a data being traced. The fundamental point is to shroud affected person's private information and other ECG signal data. ECG signal is utilized be-cause ECG size is enormous contrasted with additional clinical pictures. Consequently, patient's ECG signal readings, for example, temperature, circulatory strain, glucose perusing, position, and so on, are gathered at homes through Body Sensor Networks and it will be sent and analysed by re-bit tolerant observing frameworks. At a similar cost that the patient privacy is secured against third parties when data passed through vulnerable organization and put away in medical clinic workers.

Background
Enormous approaches have been introduced to protect patient private data. However, these approaches are introduced in order to protect data based on steganography techniques which hides secret information within medical images [1]. Previously watermarking approaches are handled to share secret data due to less efficiency and security issues this approach was dropped.

Motivation
- This project is motivated to share confidential files using techniques like steganography and cryptography.
- Investigates the existence of the original data.

Objective
- Protecting patient confidential data from intruders using steganography method.
- Formulate new steganography technique.
- Fast and scalable operation.
- Prevent the unauthorized access.
- The primary goal is to provide confidentiality, integrity and availability.

Scope of The Project
- Main aim is to hide patient's confidential data and other physiological information in ECG signal.
- To prove that both the Host ECG and stego ECG signals can be used for diagnoses. The difference between both the signals are undetectable.

The steganography’s primary objective is to enclose far away the mystery text in the other media. Hence nothing can see the text and the two members are speak covertly way [2].

Limitations
- The upside of steganography deals with planned vulnerable message and it doesn't stand out to itself as an object under examination. Certainly, the noticeable encoded messages too will be monitored regardless of how strong the messages are.
- Steganography integrates the disguise of data located in system files.
- Purely Focuses on both embedding and extraction process.
Important of The Project

- It is utilized here is to diminish the danger of utilizing cryptographic calculations alone.
- Data concealing methods install data into another medium making it vague to other people, aside from those that are intended to get the covered-up data and know about its presence.
- It centers around strategies for concealed information in which cryptographic calculations are joined with the data concealing procedures to build the security of sent information. Least Significant Bit (LSB) calculation used to conceal the mystery message into the picture.
- Triple DES Cryptography calculation is utilized here to encode and decode the mystery message which fortifies the security in better manner.

2. Development Methods

Organization security comprises of the arrangements and strategies received by an organization chairman to forestall and screen unapproved access, abuse, alteration, or forsaking of a PC organization and organization open assets [3]. Some set of experiences of systems administration is incorporated, just as a prologue to TCP/IP and internetworking. We proceed to consider hazard the board, network dangers, firewalls, and more particular reason secure systems administration gadgets [4]. An essential comprehension of PC networks is imperative to comprehend the standards of organization security. In this segment, we'll cover a portion of the establishments of PC organizing, at that point proceed onward to a diagram of some well-known organizations. Following that, we'll take a more top to bottom glance at TCP/IP, advantage of that association with accomplish something shrewd. On the other hand, UUCP typically works by having a system-wide UUCP user account and password [5]. Any framework that has a UUCP association with another must know the proper secret key for the UUCP or NUUCP account. Recognizing a host past that point has generally been minimal in extra of believing that the host is who it professes to be, and that an association is permitted around then. All of the greater as of past due, there has been a further layer of confirmation, whereby the two hosts must have a similar arrangement variety, that could be a number that is augmented on every occasion an association is made [6].

Cryptography

Cryptography is the research of secret (crypto-) composing graph). concerned approximately creating calculations: hide the putting of a few message from all aside from the sender and beneficiary (safety or thriller), in addition to verify the rightness of a message to the beneficiary (validation). From the premise of several mechanical answers for laptop and interchanges safety troubles, Cryptography is the workmanship or technology enveloping the requirements and strategies for changing a comprehensible message into one that is incomprehensible and, in a while, retransforming that message back to its specific shape. Plaintext is the first comprehensible message [9]. Code text is the modified message.

Substitution letters are supplanted by different letters (ii) Transposition: letters are orchestrated in an alternate order.

These codes might be:

- Monoalphabetic: just a single replacement/rendering is utilized.
- Polyalphabetic: where a few replacements/interpretations are utilized. Item figure: a few codes connected together.

Encrypt File

This module encodes the stacked record which is to be inserted utilizing Triple DES encryption algorithm. The encryption calculation scrambles the document utilizing explicit key as shown in Figure 1.

![Encrypt File Diagram](image-url)
Module Description
Embed Secret Data
The encoded record is watermarked or inserted with cover picture utilizing the secret phrase. LSB calculation done this inserting cycle. It replaces the pixel estimations of the cover picture. It lessens the recognize capacity of the stego picture [10].

Host File
This module empowers the client to stack the inserted picture to the worker. Worker will get the stego picture and the key file from the sender. Stores it on explicit area. At that point communicates this stego picture over the organization to the mentioned beneficiary. Advantages and disadvantages of Steganography and Cryptography is shown in Table 1.

Table 1: Advantages and disadvantages

| Steganography | Cryptography |
|---------------|--------------|
| • Obscure message passing. | • Known message passing Common innovation. |
| • Little known innovation. | • Most calculations known to government offices Strong calculation are presently impervious to beast power assault. |
| • Innovation actually being created for specific arrangements. | • Large costly processing power needed for breaking. |
| • Once distinguished message is realized. | • Innovation increment decreases strength. |
| • Many Carrier designs. | • |

Extract File
When the discovery is discovered the beneficiary with key will separate the inserted stego picture. This is accomplished by utilizing the extraction strategy. Extraction is accomplished when the keys are coordinated in any case bombed extraction. Here the encoded text record is isolated out from the stego image.

Decrypt File
Triple DES algorithm of decryption method is used here. Decoding calculation unscrambles the isolated scrambled document. The key which is utilized for encryption is utilized here for unscrambling. At last, the first mystery text record is seen by the beneficiary.

3. Hardware Requirements
System : Pentium(R) Dual-Core
Hard Disk : 160 GB.
Monitor : 14’ Color Monitor.
Mouse : Optical Mouse.
Ram : 1GB.

4. Software Requirements
Operating system : Windows 7, 32 Bit
Front End/GUI Tool : Microsoft Visual studio 2008
Coding Language : C# CODING
Application : Windows Application (C#)
Back End : SQL Server 2005.

5. Conclusion
The proposed work reveals steganography calculations to shroud quite private and physiological information through ECG signal. ECG signal conceals the relating tolerant private information and subsequently ensures the affected person’s security and secrecy. The proposed work results in improved security, productivity and execution.

References
[1]. H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, and A. Khoynazhad, —Resource-aware secure ecg healthcare monitoring through body sensor networks, I Wireless Communications, IEEE, vol. 17, no. 1, pp. 12–19, 2010.
[2]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, —Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 1, pp. 131–143, 2013.
[3]. S. Kaur, R. Singhla, O. Faroq, and B. Ahuja. —Digital Watermarking of ECG Data for Secure Wireless Communication in 2010 International Conference on Recent Trends in Information, Telecommunication and Computing. IEEE, 2010, pp. 140–144
[4]. Arvind Kumar, Km. Pooja —Steganography- A Data Hiding Technique International Journal of Computer Applications (0975 – 8887) Volume 9–No.7, November 2010.
[5]. F. Zhu and S. U. Guan, “Ordered incremental training with genetic algorithms,” International Journal of Intelligent Systems, vol. 19, no. 12, pp. 1239–1256, 2004.
[6]. S. U. Guan and S. Li, “Incremental learning with respect to new incoming input attributes,” Neural Processing Letters, vol. 14, no. 3, pp. 241–260, 2001.
[7]. X. Liu, G. Zhang, Y. Zhan, and E. Zhu, “An incremental feature learning algorithm based on least square support vector machine,” in Proceedings of the 2nd International Frontiers in Algorithmics Workshop (FAW ’08), pp. 330–338, Changsha, China, 2008.
[8]. W. Bai, S. Cheng, E. M. Tadjoudine, and S. U. Guan, “Incremental attribute-based particle swarm optimization,” in Proceedings of the 8th International Conference on Natural Computation (ICNC ’12), pp. 669–674, Chongqing, China, 2012.
[9]. S. U. Guan and J. Liu, “Incremental ordered neural network training,” Journal of Intelligent Systems
[10]. Murugan, S., & Sumithra, M. G. (2020). Big Data-Based Spectrum Sensing for Cognitive Radio Networks Using Artificial Intelligence. In Big Data Analytics for Sustainable Computing (pp. 146-159). IGI Global.
[11]. Senthilkumar, S., Karthic, A., Madavan, R., Moshi, A. A. M., Bharathi, S. S., Saroja, S., & Dhanalakshmi, C. S. (2020). Optimization of transformer oil blended with natural ester oils using Taguchi-based grey relational analysis. Fuel, 119629.