DATA SECURITY FOR HIGHLY SECURE MESSAGES WITH THE CONCEPT OF STEGANOGRAPHY AND CRYPTOGRAPHY

S.PRIYADHARSHINI [1] , SANDHYA [2]
[1]Assistant Professor, Department of ECE,
[2]Assistant Professor, Department of CSE,
[1,2] Dhanalakshmi Sirinvasan College of Engineering and Technology, Chennai

ABSTRACT

To transmit secret data over the internet, the information should be sent in a way attacker finds it difficult to read the secret data. In this paper patient's secret information is hidden in the bio-medical signal like ECG/EEG/PPG. The transmitted information generally contains biomedical -signals patient data. Main concerns include privacy and authenticity of the data being transmitted. A secret key is used which is known to sender and receiver. This paper introduces a novel steganography technique that guarantees protection of private data utilizing a key and originality of the bio-medical-signals. To maximize embedding, Fast-Walsh-Hadamard Transform is used to convert the signals into a set of coefficients. The proposed technique can be applied on three bio-medical signals like ECG/EEG/PPG unlike any other technique which uses only one bio-medical signal. To achieve least distortion, coefficients of least significant bit is considered. The algorithm has less impact on the bio-medical signal and the signal at the transmitting side can be recovered with lessdistortion.

INTRODUCTION

In public health-care scheme, physical presence of the patient is required to monitor, which is not appropriate for the current generation for various reasons like crowding of patients in the hospitals and shortage of expertize in rural areas. Thus, a new model so-called "Point-Of-Care" has emerged recently and monitors patient by gathering their samples for a short period of time with the help of Smart Sensor and the information is transmitted to the health authorities. The main interest is saving patient‟s lives and reducing the infrastructural cost in the hospitals.

Inspiteofdistinctbenefits,P-O-Chasfewthreatsrelatedtosecuritysuchas,its availabilityinisolatedareasmakinguseofpublicwebfortransmittinghighlysensitive patient‟s data. However, few countries like US and Australia have set strict rules on clinics commanding protection of patient‟s data from illegal access specially whileperforming off-site work by health authorities. However, there is few concerns from patientspoint-of-viewisprotectionoftheirprivatedataandlegitimacyofthesamples transmittedandresultofdoctordecision(whetherdoctors‟decisionisvalidfor specific sample transferred). Primary concern from Health-Care viewpoint is guarantying efficient and robust method that protects sensitive information of the patient.

OBJECTIVES

To transmit secret data over the internet, the information should be sent in a way attacker finds it difficult to read the secret data.

patient's secret information is hidden in the bio-medical signal like ECG/EEG/PPG.

The transmitted information generally contains biomedical-signals patient data.

Main concerns include privacy and authenticity of the data being transmitted.

A secret key is used which is known to sender and receiver.

This paper introduces a novel steganography technique that guarantees protection of private data utilizing a key and originality of the bio-medical-signals are preserved.

PROBLEM STATEMENT

Many steganography methods are based on the least significant bit (LSB) method of data hiding and extracting.

LSB requires the binary version of the character, and each bit of this version can be inserted in the least bit of the selected byte of the holding image

OVERVIEW

EarlierModelswhichusedtosolvetheseproblemswherebyapplyingclassical cryptography.Eventhoughhavingfewconvenientfunctionalities,theyarenotutilized in this domain as a resultof:

MobileequipmentusedinPOCareresourcelimitedmakingitdifficulttoinstall classic cryptography approach due to overhanging, by performing mathematical procedures that assures high security. Homomorphic encryption method is used to solve these above issues. The advantage of homomorphic method over classical cryptography is cipher-text is utilized as it satisfies patients concern by guaranteeing end to end security and allowing health authorities for direct service to the web since the content is not revealedinbothcases.However,researchersarelookingforwardtosolvethreatsfaced by health authorities and patients: ensuring end to end security for patients sensitive informationthatistransmittedlikepersonaldata(details,id),diagnosingdata(glucose Level), biometric data (Fingerprint and Iris) along with authenticity of normal biomedical signal collected (EEG,ECG,PPG), be suitable for existing POC capacity like memory, electricity consumption and bandwidth, and to avoid delaying the performance of the doctors at health authorities. Another technique called "steganography" is utilized to protect sensitive information along with secret key embedded within transmitted data and only legitimate users can access it. Advantages of steganography are its performance requires lower power and memory, and guaranties originality of the data without manipulatingit.

PROPOSED METHODOLOGY

In this paper, the technique can be applied on three bio-medical signals like ECG/EEG/PPG unlike any other technique which uses only one bio-medicalsignal. To maximize embedding, Fast-Walsh-Hadamard Transform is used to convert the signals into a set of coefficients. To achieve least distortion, coefficients of least significant bit is considered. The algorithm has less impact on the bio-medical signal and the signal at the transmitting side can be recovered with less distortion. The transmitted information mainly contains patient‟s data and the bio-medical signal. Patient data such as name, ID, details, temperature, blood pressure, and glucose value are manuallyentered

ADVANTAGES OF PROPOSED SYSTEM:

- This method provides good efficiency parameters and high securitylevel.
- Proposed technique assures high quality of the cover signal which is calculated by PSNR and the same can be used for diagnosis as the PRD achieved in the proposed method is low or almost equal to zero.

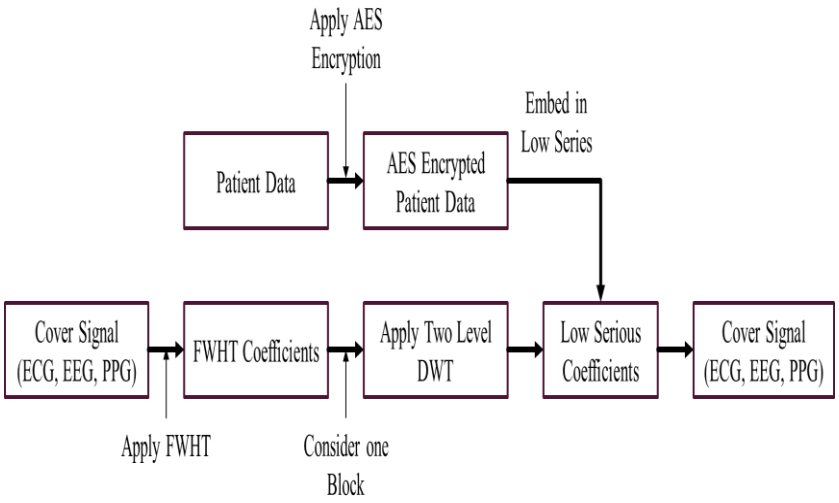
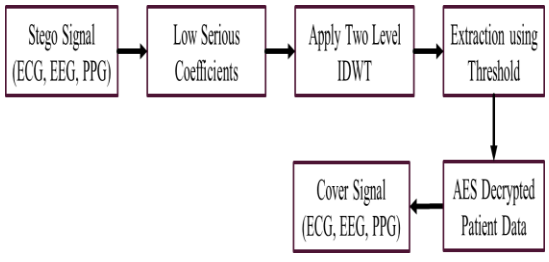


Fig 1:System Architecture

AES Encryption:

Patient‟s data like name, ID, details along with diagnosis and biometric information is encrypted using the AES algorithm. And a secret key is used, which is known only to the authorized person such as the patient and the doctor. Here 16- byte secret key is utilized which is used in the encryption process. This secret key length will decide how many rounds to be performed in AES encryption process. Each byte is converted into its corresponding bits and these bits are againconverted into its equivalent string which can be 0 or 1.



Applying FWHT on the Bio-Medical Signal:

The bio-medical signal can be ECG/EEG/PPG. FWHT is applied on any one of the signals, where the signal can be obtained in a set of coefficients. These coefficients can be divided into high and low series coefficients. Depending on the algorithm, any one of the coefficients can be selected to hide the patient‟s data. In this method, low series coefficients are used since it has a larger impact for reconstruction the bio-medical signal.

Embedding Using Haar DWT:

In this step, the obtained coefficients are considered in blocks of 8. Here 2 Level DWT is applied to the signal and the result obtained after the level 2 DWT is used for embedding. In embedding, energy value and signal value iscalculated. Depending on the AES result obtained which is 0 or 1, these signal value and energy value is embedded into the signal. If string value is 0, then the energy value and signal value is embedded into the signal, if the string value is 1, the same signal is retained which is the obtained FWHT Signal. The same process isrepeated foreach value and the energy and signal values are embedded according to the patient‟s string data value which is 0 or 1.The result of this process results in a signal called stego signal.

EXTRACTION PROCESS

Fig 2:Extraction process block

Extraction Using Haar DWT:

Obtained stego signal is considered in blocks of 3.2 Level IDWT is applied for each block which is the low series coefficient. In this stage patient data is decrypted using the threshold value. Threshold value from 0 to 10 is normally chosen.Threshold value of 5 is considered in this paper.If theobtainedenergyvalue and signal value is less than the threshold value 5, then the patient data is considered to be 1. If the energy value and signal value is greater than the threshold value 5, then the patient data is considered as 0. For each blockof the signal the energy value and signal value are compared with the threshold of 5, to completely obtain the patient data.

Applying IFWHT:

The obtained stego signal is applied with IFWHT. To convert the signal from set of coefficients to its time domain. Hence original bio-medical signal is obtained by applying IFWHT.

AES Decryption:

AES decryption process will return the patient data which is name, identity, details and their diagnosis measure and biometric information. Same rounds of operation is performed as done in AES encryption which is 10 rounds in this paper

EXPERIMENTAL RESULTS

Fig 3: Fetching PatientDetails

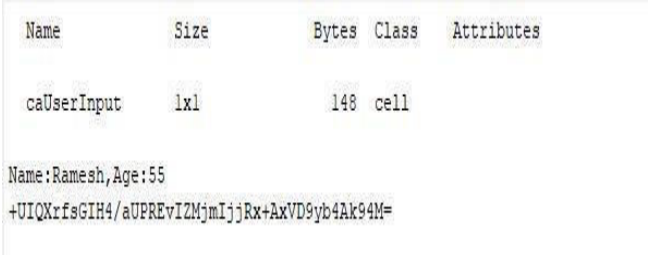


Fig 4: AES Encoded String

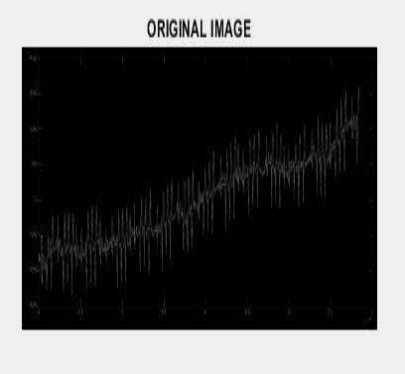


Fig 5: Original image

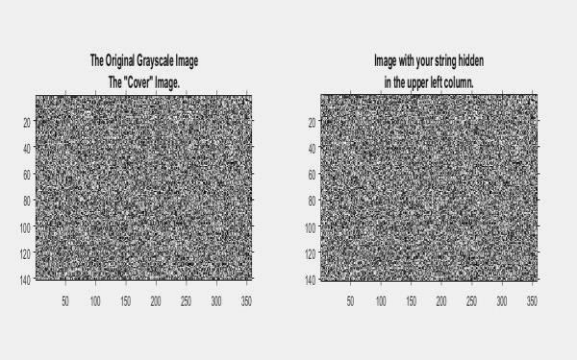


Fig 6: Encoded Image with string

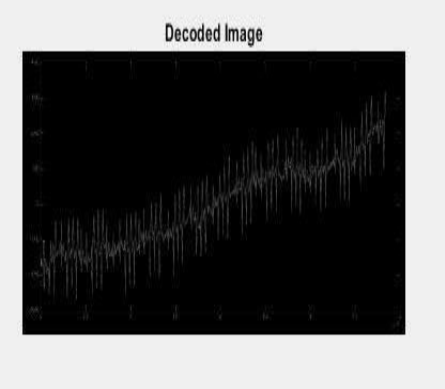


Fig 7: Decoded Image

```
The recovered string =
Name:Ramesh,Age:55
```

Fig 8: Recovered String

Conclusion and Future Enhancement

This paper aim is to hide patient data along with diagnostic data inside the bio- medical signal. Proposed technique assures high quality of the cover signal which is calculated by PSNR and the same can be used for diagnosis as the PRD achieved in theproposed method is low or almost qual to zero.Comparisonof proposed method with the existing state of art papers cited as, the value of PRD is observed to be higher than our proposed algorithm, leading to a secure and imperceptible stegaographic method to hide and transmit medical data for telemedicine. From obtain result, it is clear that the proposed system achieved minimum PRD and high PSNR for all the three bio-medical signals. The security of the proposed algorithm is accomplished with the method of AES encryption which ensures anybody involved in the communication system can receive the message, but only the authorized or intended recipient can decrypt and know the patient‟s data. The proposedmethodcanbeusedinpoint-of-care(POC)systemtodiagnosethepatients at the bed side and for emergency purpose POC is considered as the mainsource.

References

[1] "Curvelets-based ECG steganography for data security"; S. Edward Jero; P. Ramu; Electronics Letters; Year:2016.

[2] "Reversible data hiding in ecg signals based on histogram shifting and thresholding"; Wenchao Wu; Bin Liu; Weiming Zhang; Changwen Chen; 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech); Year:2015.

[3] "Steganography technique to secure patient confidential information usingECG signal"; V. Sankari; K. Nandhini; International Conference on Information Communication and Embedded Systems (ICICES2014); Year:2014.

[4] "Adaptive steganography technique to secure patient confidential information using ECG signal"; Liem Dao Duy; Thy Nguyen Thi Minh; Tu Huynh Thanh; 4th NAFOSTED Conference on Information and Computer Science; Year:2017.

[5] "Securely data hiding and transmission in an ECG signal usingDWT";Sumedha Awasarmol; Shweta Ashtekar ; Amruta Chintawar; International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS); Year: 2017.

[6] "Novel Audio Steganography Technique for ECG Signals in Point of Care Systems (NASTPOCS)"; Anitha Devi; K.B. ShivaKumar; IEEE International Conference on Cloud Computing in Emerging Markets (CCEM); Year:2016.

[7] "Reversible Data Hiding for Electrocardiogram Signal Based on

Wavelet Transforms"; Kai-mei Zheng; Xu Qian; International Conference onComputational Intelligence and Security; Year:2008.

[8] "Reversible blind watermarking for medical images based on wavelethistogram shifting"; Hêmin Golpîra; Habibollah Danyali; IEEE International Symposiumon