RESEARCH ARTICLE OPEN ACCESS

Confidential Data Hiding Using Wavlet Based Ecg Stegnography

Malashree K S[1],Jagadish K N [2], Suma.M[3]
[1]Student,M.tech, Electronics and communication Department, The a. i. t College of Engineering, chikkamagalore, India
[2]Student, M.tech, Electronics and communication Department, The B.g.s.i.t College of Engineering, BG nagar, Mandya,India
[3]asst.prof, Electronics and communication Department, The a. i. t College of Engineering, chikkamagalore, India

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 (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. It is utterly important that patient confidentiality is protected while data is being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. In this project, 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.

Index Terms—ECG, Steganography, Encryption,Wavelet, Wa-termarking, Confidentiality.

I. INTRODUCTION

The number of elderly patients is increasing dramatically due to the recent medical advancements. Accordingly, to reduce the medical labour cost, the use of remote healthcare monitoring systems and Point-of-Care (PoC) technologies have become popular . Monitoring patients at their home can drastically reduce the increasing traffic at hospitals and medical centres. Moreover, Point-of-Care solutions can provide more reliability in emergency services as patient medical information (ex. for diagnosis) can be sent immediately to doctors and response or appropriate action can be taken without delay. However, Remote health care systems are used in large geographical areas essentially for monitoring channel used to exchange information. Typically, patient biological signals and other physiological readings are collected using body sensors. Next, the collected signals are sent to the patient PDA device for further processing or diagnoses. Finally, the signals and patient confidential information as well as diagnoses report or any urgent alerts are sent to the central hospital servers via the Internet. Doctors can check those biomedical signals and possibly make a decision in case of an emergency from anywhere using any device[3]. Using Internet as main communication channel introduces new security and privacy threats as well as data integration issues. According to the Health Insurance Portability and Accountability Act (HIPAA), information sent through the Internet should be protected and secured. HIPAA mandates that while transmitting information through the internet a patient's privacy and confidentiality be protected as follows:

- Patient privacy: It is of crucial importance that a patient can control who will use his/her confidential health information, such as name, address, telephone number, and Medicare number. As a result, the security protocol should provide further control on who can access patient's data and who cannot.
- Security: The methods of computer software should guarantee the security of the information inside the communication channels as well as the information stored on the hospital server. Accordingly, it is of crucial importance to implement a security protocol which will have powerful communication and storage security.

PROBLEM STATEMENT

Several researchers have proposed various security protocols to secure patient confidential information. Techniques used can be categorized into two subcategories. 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.

PROBLEM FORMULATION

I. Many security techniques are based on hiding its sensitive information inside another insensitive host data without incurring any increase in the host data size and huge computational overhead. These techniques are called steganography techniques. Steganography is the art of hiding secret information inside another type of data called host data. However, steganography techniques alone will not solve the authentication problem and cannot give the patients the required ability to control who can access their personal information as stated by HIPAA.

II. PROPOSED SYSTEM

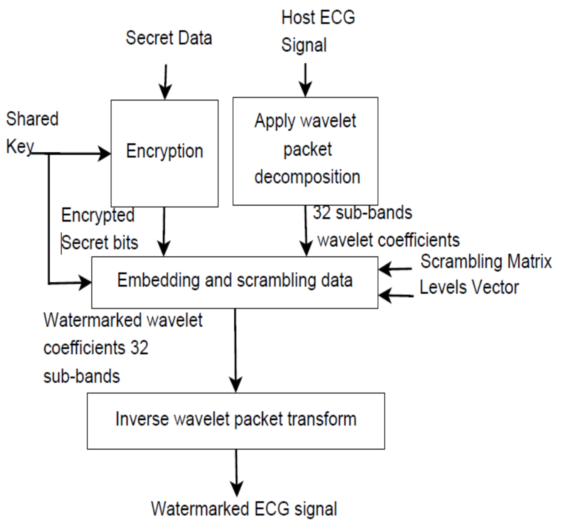

Secret Data
Host ECG Signal
Shared Key
Encryption
Apply wavelet packet decomposition
Encrypted Secret bits
32 sub-bands wavelet coefficients
Scrambling Matrix
Levels Vector
Embedding and scrambling data
Watermarked wavelet coefficients 32 sub-bands
Inverse wavelet packet transform
Watermarked ECG signal

Fig. 1 Block diagram of the sender steganography which includes encryption, wavelet decomposition and secret data embedding.

III. METHODOLOGY

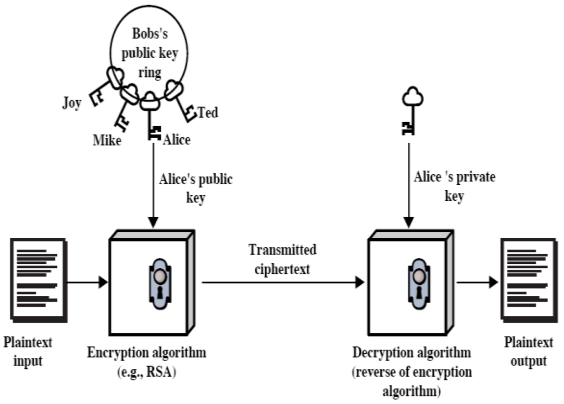
The sender side of the proposed steganography technique consists of four integrated stages as shown in Fig 1. The proposed technique is designed to ensure secure information hiding with minimal distortion of the host signal. Moreover, this technique contains an authentication stage to prevent unauthorized users from extracting the hidden information.

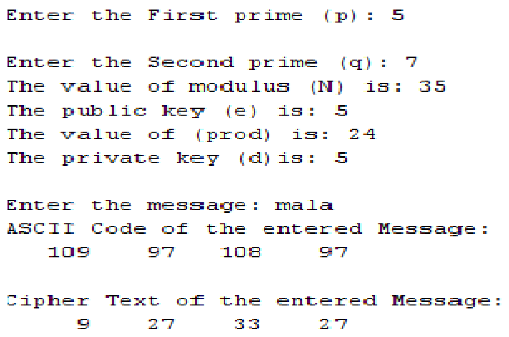
A. Stage 1: Encryption

The aim of this stage is to encrypt the patient confidential information in such a way that prevents unauthorized persons - who does not have the shared key- from accessing patient confidential data. In this stage XOR ciphering technique is used with an ASCII coded shared key which will play the role of the security key. XOR ciphering is selected because of its simplicity. As a result, XOR ciphering can be easily implemented inside a mobile device. Fig 2 shows an example of what information could be stored inside the ECG signal .

RSA ALGORITHM:

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person whocan decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the publickey, this makes the RSA algorithm a very popular choice in data encryption.




```
Enter the First prime (p): 5

Enter the Second prime (q): 7
The value of modulus (N) is: 35
The public key (e) is: 5
The value of (prod) is: 24
The private key (d)is: 5

Enter the message: mala
ASCII Code of the entered Message:
    109    97    108    97

Cipher Text of the entered Message:
      9     27     33     27
```

Fig2 RSA algorithm and result

B. Stage 2: Wavelet Decomposition

Wavelet transform is a process that can decompose the given signal into coefficients representing frequency components of the signal at a given time. Wavelet transform can be defined as shown in time domain with frequency domain in one transform. In most applications discrete signals are used. Therefore, Discrete Wavelet Transform (DWT) must be used instead of continuous wavelet transform. DWT decomposition can be performed by applying wavelet transform to the signal using band filters. The result of the band filtering operation will be two different signals, one will be related to the high frequency componentsand the other related to the low frequency components of the original signal. If this process is repeated multiple times, then it is called multi-level packet wavelet decomposition. Discrete

Wavelet transform can be defined

$$W(i,j) = \sum_{i} \sum_{j} X(i)\Psi_{ij}(n)$$

Where W(i, j) represents the DWT coefficients. i and j arethe scale and shift transform parameters, and ij(n) is the wavelet basis time function with finite energy and fast decay. The wavelet function can be defined

$$\Psi_{ij}(n) = 2^{-i/2}\Psi(2^{-i}n - j)$$

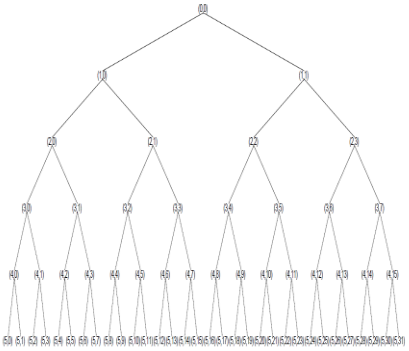


Fig.3 5-level wavelet decomposition tree showing 32 sub-bands of ECG host signal and the secret data will be hidden inside the coefficients of the sub-bands

In this project, 32-level wavelet packet decomposition has been applied to the host signal. Accordingly, 4 sub-bands resulted from this decomposition process as shown in Fig 2. In each decomposition iteration the original signal is divided into two signals. Moreover, the frequency spectrum is distributed on these two signals. Therefore, one of the resulting signals will represent the high frequency component and the other one represents the low frequency component. Most of the important features of the ECG signal are related to the low frequency signal. Therefore, this signal is called the approximation signal (A). On the other hand, the high frequency signal represents mostly the noise part of the ECG signal and is called detail signal (D).

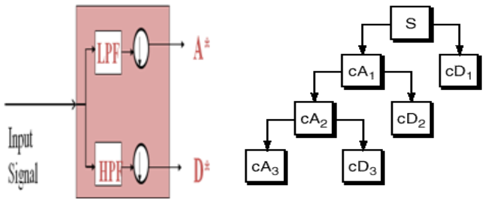
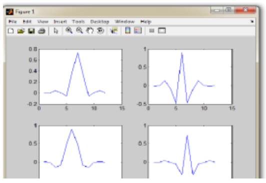
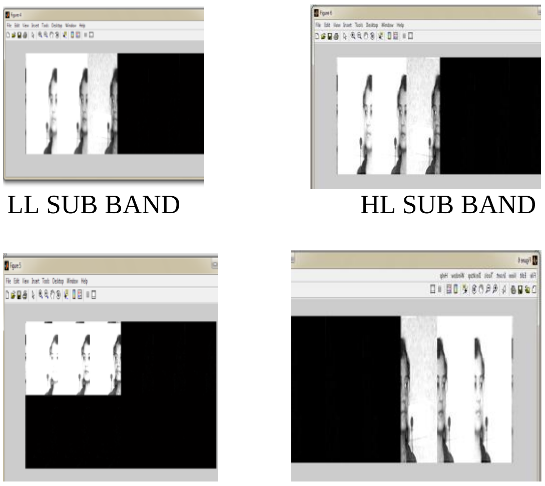


Fig 3 dwt sub bands



LL	HL
LH	HH

GENERAL DWT SUB BAND AND ECG



LL SUB BAND

HL SUB BAND

LH SUB BAND

HH SUB BAND

Fig 4 results of LL,LH.HL.HH sub bands from dwt

C. Stage 3: The embedding operation

At this stage the proposed technique will use a special security implementation to ensure high data security. In this technique a scrambling operation is performed using two parameters. First is the shared key known to both the sender and the receiver. Second is the scrambling matrix, which is stored inside both the transmitter and the receiver. Each transmitter/ receiver pair has a unique scrambling matrix defined by

$$S = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,32} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,32} \\ \vdots & \vdots & \ddots & \vdots \\ s_{128,1} & s_{128,2} & \cdots & s_{128,32} \end{bmatrix}$$

where S represents wavelet function. S and P are positive integers representing transform parameters. C represents the coefficients which is a function of scale and position parameters. Wavelet transform is a powerful tool to combine Where S is a 128 × 32 scrambling matrix. s is a number between 1 and 32. While building the matrix we make sure that the following conditions are met:

- The same row must not contain duplicate elements
- Rows must not be duplicates.

The detailed block diagram for the data embedding process is shown in Fig . The embedding stage starts with converting the shared key into ASCII codes,therefore each character is represented by a number from 1 to 128. For each character code the scrambling sequence fetcher will read the corresponding row from the scrambling matrix. Anexample of a fetched row can be shown in Fig 3.

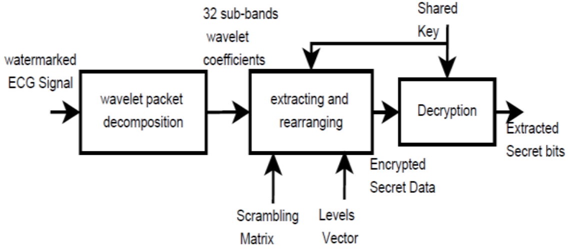


Fig.5 Block diagram of the receiver steganography which includes wavelet decomposition, extraction and decryption

The embedding operation performs the data hiding process in the wavelet coefficients according to the sub-band sequence from the fetched row., the embedding process will start by reading the current wavelet coefficient in sub-band 32 and changing its LSB bits. Then, it will read the current wavelet coefficient in sub-band 22 and changing its LSB bits, and so on. On the other hand, the steganography level is determined according to the level vector which contains the information about how many LSB bits will be changed for each sub-band. For example if the data is embedded in sub-band 32 then 6 bits will be changed per sample, while if it is embedded into wavelet coefficient in sub-band 1 then 5 LSB bits will be changed.

D. Stage 4: Inverse wavelet re-composition

The resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet re-composition. The result of this operation is the new watermarked ECG signal. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain. Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original unwatermarked ECG signal. The detailed embedding algorithm is shown in Algorithm 1. The algorithm starts by initializing the required variables. Next, the coefficient matrix will be shifted and scaled to ensure that all coefficients values are integers. Then, the algorithm will select a node out of 32 nodes in each row of the coefficient matrix. The selection process is based on the value read from the scrambling matrix and the key. The algorithm will be repeated until the end of the coefficient matrix is reached. Finally, the coefficient matrix will be shifted again and re-scaled to return its original range and inverse wavelet transform is applied to produce the watermarked ECG signal.

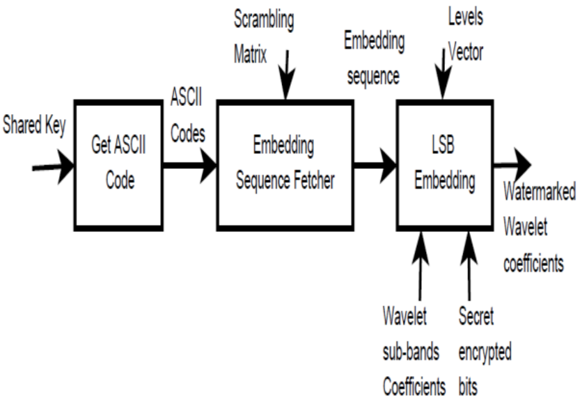


Fig. 4 Block diagram showing the detailed construction of the watermark Embedding operation

FLOWCHART

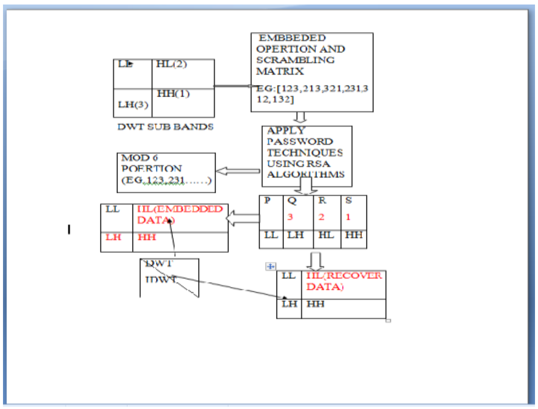
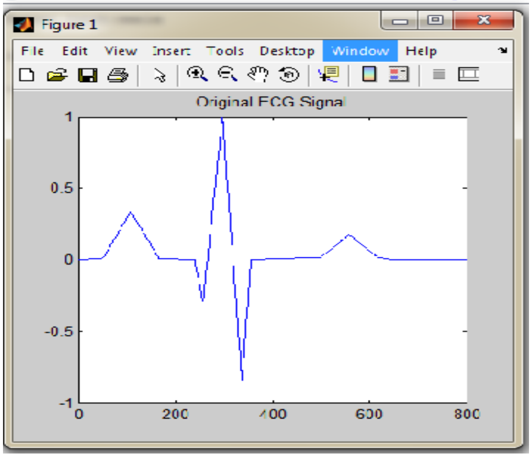
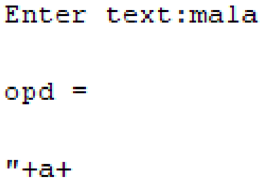

LL
HL(2)
HH(1)
LH(3)
DWT SUB BANDS
EMBBEDED OPERTION AND SCRAMBLING MATRIX
EG:[123,213,321,231,312,132]
APPLY PASSWORD TECHNIQUES USING RSA ALGORITHMS
MOD 6 POERTION (EG,123,231……)
LL
HL(EMBEDDED DATA)
LH
HH
P
Q
R
S
3
2
1
LL
LH
HL
HH
DWT
IDWT
LL
HL(RECOVER DATA)
LH
HH

Fig Flow chart of embedded operation and scrambling matrix opertion

RESULTS:
INPUT:



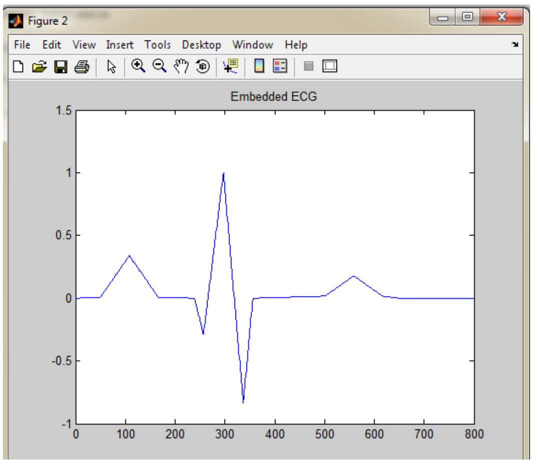
AFTER ENCRYPTION:
OUTPUT



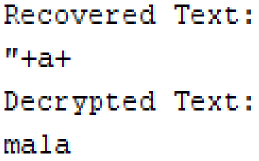
```
Enter text:mala

opd =

"+a+
```



RECOVER AND DECRYPATED DATA



```
Recovered Text:
"+a+
Decrypted Text:
mala
```

IV. CONCLUSION AND FUTURE WORK

A novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. This technique will provide a secured communication and confidentiality in a Point-of-Care system. A 5-level wavelet decomposition is applied. A scrambling matrix is used to find the correct embedding sequence based on the user defined key. Steganography levels (i.e. number of bits to hide in the coefficients of each sub-band) are determined for each sub-band by experimental methods. In this paper we tested the diagnoses quality distortion. It is found that the resultant watermarked ECG can be used for diagnoses andthe hidden data can be totally extracted.

REFERENCES

[1] Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," *IEEE Transactions on information technology in biomedicine*, vol. 8, no. 4, pp. 439–447, 2004.

[2] F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving tele cardiology sensor networks: toward a low-cost portable wireless hardware/ software codesign," *IEEE Transactions on Information Technology in Biomedicine*,, vol. 11, no. 6, pp. 619–627, 2007. patient record using image transform".

[3] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in *5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009*. IEEE, 2010, pp. 207–212.

[4] W. Lee and C. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*,, vol. 12, no. 1, pp. 34–41, 2008.[5] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in *Proceedings.*