ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 14, April 2017

SECURE DATA TRANSMISSION USING WAVELET BASED STEGANOGRAPHY FOR EHR SYSTEMS

M.S.Nilakshma
Student
Department of CSE
Agni College of Technology
Chennai, India
msnilakshma25@gmail.com

A.Priya
Student
Department of CSE
Agni College of Technology
Chennai, India
priyasweeti225@gmail.com

W.Mercy
Assistant Professor
Department of CSE
Agni College of Technology
Chennai, India
mercy.cse@act.edu.in

Abstract—*As population is growing rapidly every year, the volume of data related to each one in various fields is increasing. Healthcare is a major field, where huge volume of data is handled every day. Healthcare information systems have been developed to handle these big data. Secure storing of patient's data in health care systems is important. Electronic health record (EHR) system offers an efficient way of delivering quality ensured healthcare services. As EHR contains both private health information and personal identification data, it needs to be stored securely before transmission to other networks to avoid the misuse of data. Encryption and steganography are the popular techniques used for data security. In recent times, Electrocardiography (ECG) signal is used for biometric security systems. The ECG signal is an appropriate host signal and provides verifiable secure means to store big EHR data in the cloud. In many EHR systems, encryption is used for privacy and ECG steganography is used for hiding sensitive data. So, secure transmission of this encrypted data can be provided by ECG signal. In this paper, a wavelet based ECG steganography technique is used which involves Multiple Least Significant Bit (MLSB) method to embed the encrypted EHR data into ECG signal to provide confidential storing of patient information. The encrypted data along with the ECG signal can be stored in the file server after compression. A compression stage is introduced in this method to reduce the amount of data so that required storage can be minimized. The proposed method provides less deterioration of signal as well as minimized storage requirements.*

***Keywords-** Electronic Health Record; Electrocardiography; Wavelet; Encryption; Steganography*

I. INTRODUCTION

Various healthcare information systems are used nowadays for maintaining patient's information. Health Information Technology (HIT) in an effort to encourage patient centered care through the assessment of health outcomes [1]. HIT encompasses a collection of technologies to store, share and analyze the health information. It ensures the accessing as well as sharing of data with the patients and their family and doesn't focus on the healthcare providers. For example, doctors can verify as well as access the record of patients without searching for the actual prescription paper. One of the important components of HIT is Electronic Health Record (EHR).

Electronic Health Record is an emerging technology which maintains the entire medical information of a patient [2]. EHR systems offer more efficient means of delivering quality ensured healthcare services and promoting collaborative clinical research. One of the key features of EHR is that data can be accessed, maintained and featured by authorized personals. The advantages of EHR include up-to-date and complete information, less medical errors and reliable prescription [3]. Privacy and security of patient information is a top priority. According to the Health Insurance Portability and Accountability Act (HIPAA), privacy and security regulations are two crucial provisions in the protection of healthcare privacy [4][5][6][7][8][9]. Thus protection of patient information can be achieved by data encryption, private policy, and security. Data encryption ensures security by changing the provided data into an unreadable form. Along with encryption, other techniques can be used which provides confidential storing and transmission. A privacy policy is to be implemented to give authorized and authenticated access of the patient data from the storage. Security ensures integrity, confidentiality and monitoring of the EHR data. It helps in safeguarding and monitoring that helps in identifying the location of storage. This helps in preventing EHR breaching.

Most of the existing systems implemented various security methods for secure transmission of data between two end users over the public network. The existing systems are based on two main techniques. The first technique is the cryptographic technique which is closely related to cryptology as well as cryptanalysis. The process of transforming plain text to an unreadable format using a cipher is called encryption [8][10]. It ensures confidentiality, integrity, non-repudiation, and authentication. The disadvantage of using encryption-based techniques is its large computational overhead.[3][4]. The second technique is the steganographic technique. Steganography is about hidden writing. Thus the data is hidden into another host data, which includes image, audio or video file. Steganography offers more efficient and secure information concealment than traditional cryptography [11]. But encrypted hiding of data provides more security. Watermarking is other data hiding method similar to steganography. Subjecting the signals to transforms results into coefficients which are then modified to hide the secret data. This process is called watermarking [12]. All doctors of hospital can see the watermarked ECG signal, but one certified doctor who has same secret key will extract the secret information by using same key from the host ECG signal [7].The simplest approach to hiding data within a file is called Least Significant Bit (LSB) insertion. In LSB, the data are embedded into the least significant bits in the host data. In case of steganography, it leads to larger host data size and higher computational overhead [5].

In this paper, a hybrid methodology by combining cryptographic and steganographic techniques is used in order to provide protected storage of the patient data. Cryptography enables the encryption of EHR data by using the patient key. This encryption model allows secure access of data by the users due to shared key access for authorized patients and other healthcare system personals. ECG is the graphical representation of electrical signal generated from heart [13]. The ECG signal is used as cover signal, because most of the healthcare systems collect ECG information. Moreover, the size of the ECG signal is large compared to the size of other information [4]. Thus the ECG signal is used as a host file to transmit the patient's data to other end users. As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. The Wavelet transform is a mathematical tool which provides a time-frequency representation of stationary and non-stationary signals [8]. The wavelet coefficient offers an efficient way of storing the data without changing its size. Thus the encrypted data is embedded into the wavelet coefficients of ECG signal. For this embedding process, Multiple LSB (MLSB) method is used. The resulting watermarked ECG signal is then stored in cloud which can be accessed by authorized personals only. Cloud computing, which is composed of many different technologies that already existed, represents a new and more cost effective way of delivering enterprise IT solutions [14]. Cloud delivers data storage server based remote file storage services to the subscriber. Cloud computing provides a required computing infrastructure for the storage of EHR [2]. The subscriber will then be able to process all their files stored on these storage servers and will be able to backup or recover the files. They also provide a new opportunity to share EHRs across different healthcare providers. As a result, all the end users can view the file but only authorized users such as doctors or administrative personals can extract the data from the system.

Rest of the paper is organized as follows. Section II describes about the related research works. Section III illustrates the proposed methodology. Section IV describes implementation of the proposed method. Conclusion and future scope are given in Section V.

II. RELATED WORKS

Uthpala Premarathne and others recently proposed a cryptographic role-based access control model for EHR systems [11], which uses location and biometrics based user authentication and a steganography based technique to embed EHR data in ECG host signals. In their approach, the health authority validates mobile users based on their identity and location attributes. A mobile user consults the domain server, which forwards the request to the health authority on the user's behalf. Based on this validation, the domain server informs the Cloud Service Provider (CSP) to allow the requested information to be transmitted. The ECG is segmented and Haar wavelet transformation is applied on each segment. Then the hash function is applied on EHR data which is encrypted and it is randomly stored in the least significant bits of the ECG data. This watermarked ECG is embedded into the original ECG signal and stored into the cloud servers. The session key, used for encrypting the data, is established only to valid users. Thus this ensures authorized access of data by users.

Shaheen Patel and Sankpal proposed a secure patients data transmission system using XOR ciphering encryption and ECG steganography [16]. In their paper, a hybrid combination of encryption and ECG steganography is used to hide the data. The encryption of data is done by using XOR ciphering method that uses the shared key as the security key. The encrypted data is embedded into the wavelet coefficient of the ECG signal by using ASCII coded shared key in randomized manner.

Eswara Reddy and Gandikota Ramu proposed a Secure Framework for Ensuring EHR's Integrity using Fine-Grained Auditing and Cipher-text Policy Attribute Based Encryption (CP-ABE) [18]. In this paper, the authors aim for integrity of EHR once it is stored in cloud. This scheme provides security of patient data without revealing sensitive data to other users. The file is audited by using CP-ABE. Here, a security key is generated by the data owner from the keys generated from the Key Generating Auditor and the cloud server. This ensures that there is no sharing of master keys between the auditors. Thus this key is used in re-encryption of the cipher-text which ensures that there is integrity of EHR data at the same time. But this paper states that identity privacy and data privacy are the major issues.

Sanjeet Kumar Nayak and Somanath Tripathy proposed a Privacy Preserving Provable Data Possession for Cloud based Electronic Health Record System [3]. In this paper, a privacy preserving provable data possession scheme for cloud based EHR system which also supports blockless verification, data dynamics and batch auditing without using bilinear paring. This system uses Third Party Auditor (TPA) which checks the integrity of EHR data based on the audit response from CSP. The most appealing feature of the proposed scheme is that, it provides lower computation overhead for the TPA as compared to the other existing schemes while enabling all the important requirements including blockless verification, privacy preserving, batch auditing and data dynamics.

Kavya PremChandran and Krishnakumar proposed ECG Steganography using Integer Wavelet Transform [8]. The authors use a technique that combines both steganography and cryptography in order to ensure and guarantee highly secure transmission of patient confidential information over internet. Here Integer Wavelet transform using lifting scheme is used. The data is encrypted using XOR ciphering method. One level of wavelet decomposition is applied on the ECG signal and the encrypted data are embedded into the detail signal using LSB method by using the secret key. The scrambling matrix provides the sequence where the data are embedded. The authors concluded that the distortion caused due to watermarking is less than 1%.

Deepali Awasthi and Swati Madhe proposed evaluation of wavelet based ECG steganography system by using Percentage Residual Difference (PRD) Measurements [7]. In this paper, a wavelet packet decomposition method is proposed for decomposing the host ECG signal. For concealing the patient private information, encryption process is implemented. Patient private information is embedded inside the host ECG signal in form of binary bits. Consequently, encrypted ECG signal is produced by inverse wavelet decomposition. Afterwards, extraction process is implemented which separates the patient private information and host ECG signal.

III. THE PROPOSED METHOD

In the proposed method, there are two phases. The first phase, concerned with the sender, involves encryption, compression and embedding of EHR data in ECG signal. In the second phase, at the receiver end, the extraction, decompression and decryption steps are involved. The stages of the proposed method are given below.

A. EHR Encryption

In this step, the EHR is divided into fixed length blocks of data bits and each block is encrypted separately. For encryption, XOR ciphering method is used with the shared key, which also plays as a security key for the patient. XOR Ciphering is an additive ciphering technique [10]. XOR ciphering technique is selected because of its simplicity. Fig.1 shows the encryption process.

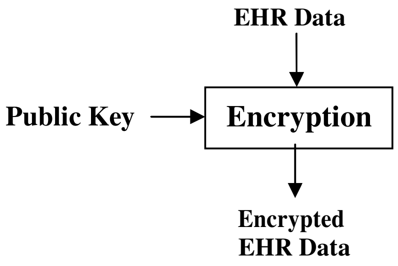


Fig.1 circuit diagram for EHR Encryption

Wavelet Decomposition

Wavelet transform is the mathematical way of performing signal analysis in which the frequency of the signal varies over time. Discrete Wavelet Transformation (DWT) decomposes the signal into coefficients detailed and coefficients approximation. The encrypted EHR data is to be embedded into the detailed component of the signal. In this paper, five level decomposition of wavelet is applied to the ECG signal which gives 32 sub-bands of wavelet coefficients. Fig.2. shows the DWT decomposition process.

B. EHR Data Embedding

In this step, the EHR data is embedded into the wavelet coefficients. Before that, a lossless compression technique is carried out to reduce the number of bits to represent the data. The steganography level is determined by the level vector. The level vector provides the information where the data are embedded into the LSB of the signal by comparing the most significant bit of the host data. This methodology is MLSB technique. The resultant signal is called the watermarked wavelet coefficients. The entire operation is illustrated in Fig.3.

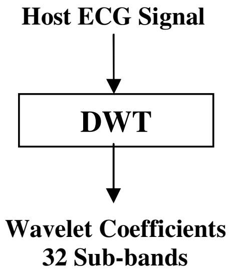


Figure 2 circuit diagram for EHR Data Embedding Process

C. Wavelet Recomposition

In the wavelet recomposition step, the inverse wavelet transformation is applied to the watermarked wavelet coefficients to convert it into watermarked ECG signal. These coefficients are embedded into the original signal according to its index and end described in the ECG signal. The process of recomposition is shown in Fig. 4.

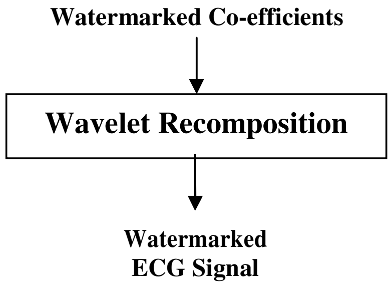


Fig. 3 circuit diagram for wavelet recomposition

File Upload and Download in Cloud

After the encryption and embedding of the ECG signal, the file is uploaded into the cloud server by the health authority. The patient EHR data are securely stored by a cloud provider. The authentication and authorization are verified by the system administrator. The above method suggests secure storing of the data in the cloud. The users such as patients, doctors, nurses, laboratory staff and insurance agents can view the file after downloading it. This requires a shared key between two end users for secure access of data. This prevents unauthorized access of data by others.

D. *Extration of Data*

The extraction of data involves the decryption as well as extraction of data from the ECG signal. Thus this phase includes two stages of implementation. First, five level wavelet decomposition is applied to the resulting ECG signal to get the 32 bit sub-band coefficients, which is shown in Fig.5.

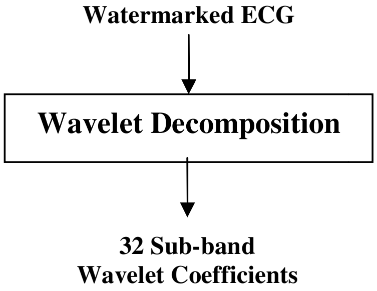


Fig. 4 circuit diagram for. Wavelet Decomposition in Extraction Phase

By using the level vector the data bits are extracted from the watermarked wavelet coefficients. The data are rearranged using the decompression algorithm. The encrypted EHR data are then decrypted using the inverse algorithm with the public key. After that, the resulting data will be used by the authorised users at receiver side. Fig.6. illustrates the process

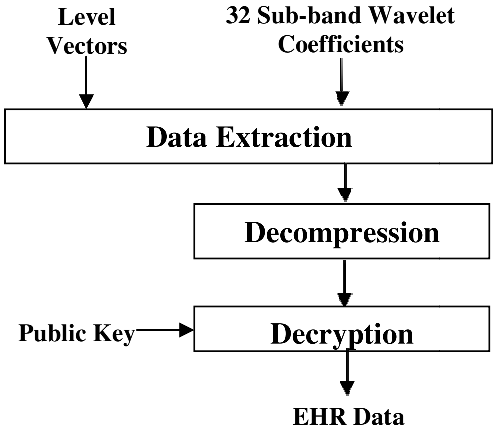


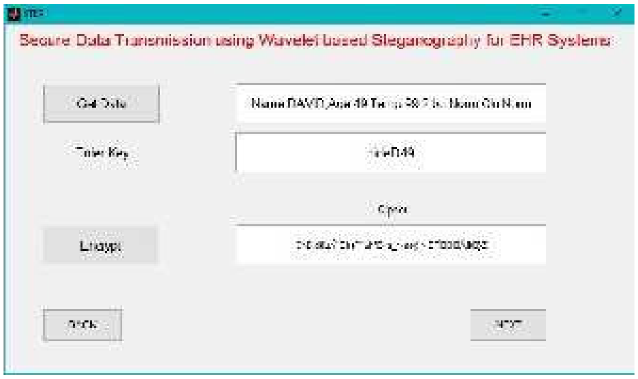
Fig.5 circuit diagram for Decompression and Decryption Process

IV. IMPLEMENTATION

To verify the secure data sharing of EHR, all the stages of the proposed method are implemented. For simplicity, images are not included for the implementation. The host ECG is downloaded from the ECG database Physionet [20]. MATLAB 2014 tool is used to implement the proposed met

hod.

In the first step, EHR data is loaded and using XOR ciphering method the data is encrypted using a public key. Implementation of this step is shown in Fig. 7.


Secure Data Transmission using Wavelet based Steganography for EHR Systems

Name DAVID,Age 49 [illegible]

Fig. 5 circuit diagram for Implementation of EHR Encryption

In the next step, ECG signal is loaded and decomposed into many sections. One section of the signal is selected for the embedding purpose. The index and end point of the section are preserved. Implementation of this step is shown in Fig. 8.

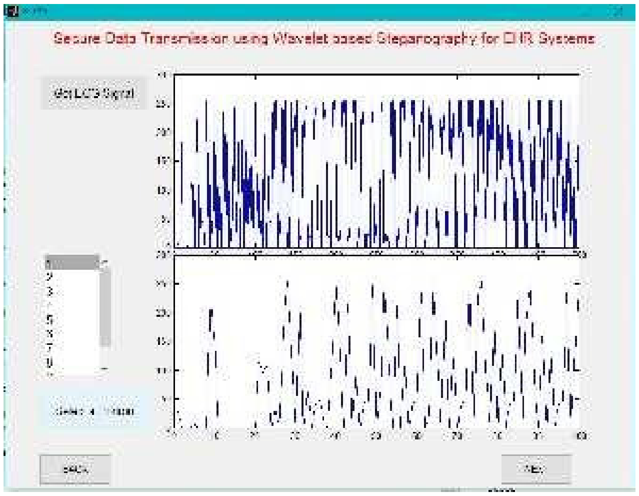
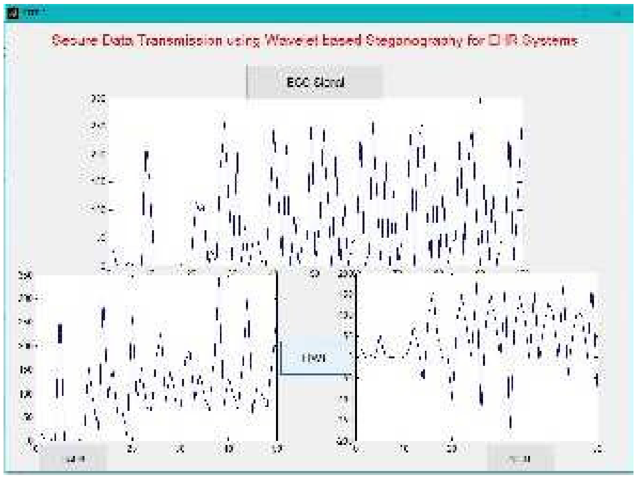

Secure Data Transmission using Wavelet based Steganography for EHR Systems

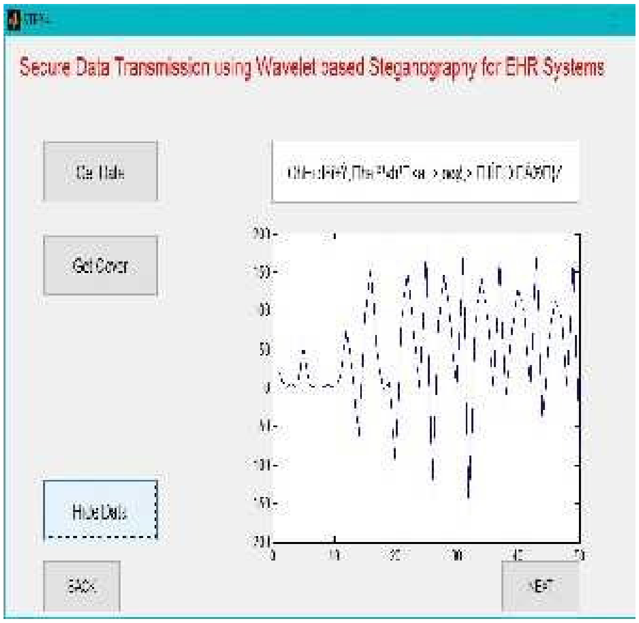
Fig. 6 circuit diagram for Implementation of ECG decomposition

Then, wavelet transform is applied on the selected portion of the ECG signal. This step gives approximation and detail coefficients. Detail coefficients are use to embed the EHR data. Implementation of this step is shown in Fig.9. The Detail coefficients are used as cover to implement data hiding step. The already encrypted EHR data is embedded inside the wavelet transformed ECG signal using the MLSB method. Fig.10 shows the implementation of this step. After embedding the data in the ECG coefficients, inverse wavelet transform is applied on the embedded coefficients. This results into watermarked ECG signal, which is stored in a file.



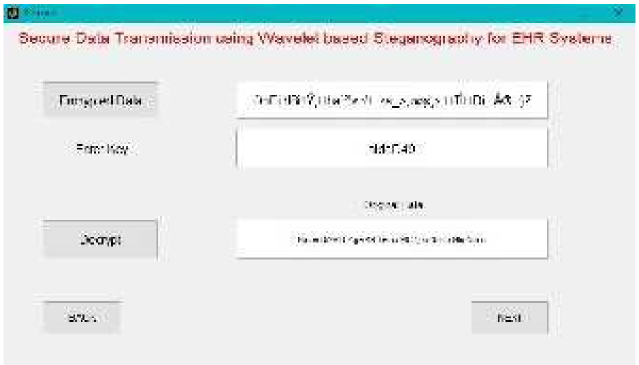
Secure Data Transmission using Wavelet based Steganography for EHR Systems

Fig. 7 circuit diagram for. Implementation Wavelet Transformation



Secure Data Transmission using Wavelet based Steganography for EHR Systems

Fig. 8 circuit diagram for. Implementation of Steganography



Secure Data Transmission using Wavelet based Steganography for EHR Systems

Figure 9 circuit diagram for Implementation of Decryption

In the reverse process, to collect back the original EHR data, wavelet decomposition is applied on the watermarked ECG signal. The data bits are extracted from the ECG signal using MLSB extraction procedure. The resultant data are in encrypted form. To get back the EHR data, decryption step is executed with the same public key used in the encryption stage. The implementation is shown in Fig.11. The original data is reconstructed and now ready for access.

V. CONCLUSION

In this paper, cryptography and steganography based data security method is proposed and implemented. To implement this method, ECG signals are taken from physionet [20]. Wavelet packet decomposition is used for splitting the host ECG signal. The patient private information is protected by the XOR ciphering encryption and lossless compression algorithm. Patient information is then embedded into the ECG signal by using MLSB method. Thus the watermarked ECG signal is formed and stored. In the extraction phase, EHR is reconstructed by decomposition of watermarked ECG signal, decryption and decompression. By implementing the method, it is observed that, the private information can be securely stored and it is hardly possible to access the information by unauthorized persons.

REFERENCES

[1] Sajda Qureshi, Cherie Noteboom and Alice M.Schumaker, “Mobile access for patient centered care: The challenges of activating Knowledge through health information technology”, IEEE International Conference on System Sciences, pp. 3227-3236, 2015.

[2] Preethi and Ranjith Balakrishnan, “Cloud enabled patient-centric EHR management system”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT 2014), pp.1678-1680, 2014.

[3] Sanjeet Kumar Nayak and Somanath Tripathy, “Privacy preserving provable data possession for cloud based electronic health record system”, IEEE TrustCom-BigDataSE-ISPA, pp.860-867, 2016

[4] Deepali Awasthi and Swati Madhe, “Analysis of encrypted ECG signal in steganography using wavelet transforms”, IEEE International Conference on Electronics and Communication Systems (ICECS 2015), pp. 718-723, 2015.

[5] Ayman Ibaida and Ibrahim Khalil, “Wavelet-based ECG steganography for protecting patient confidential information in Point-of-Care systems”, IEEE Transactions on Biomedical Engineering, vol. 60, no. 12, pp.3322-3330, 2013.

[6] V.Sankari and K.Nandhini, “Steganography technique to secure patient confidential information using ECG signal”, IEEE International Conference on Information Communication and Embedded Systems (ICICES2014), pp. 1-7, 2014.

[7] Deepali Awasthi and Swati Madhe, "Evaluation of wavelet based ECG steganography system by using Percentage Residual Difference (PRD) measurements", IEEE ICCSP conference, pp. 559-563, 2015.

[8] Kavya PremChandran and Krishnakumar.K.P, "ECG steganography using integer wavelet transform", International Conference on Computer Communication and Informatics (ICCCI - 2015), pp. 1-5, 2015.

[9] Wei-Bin Lee and Chien-Ding 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, January 2008.

[10] Anish Singh Shekhawat, Arnav Jain and Dipti Patil, "A study of ECG steganography for securing patient's confidential data based on wavelet transformation", IEEE International Journal of Computer Applications, pp. 12-16, November 2014.

[11] Uthpala Premarathne et al., "Hybrid cryptographic access control for cloud-based EHR systems", IEEE cloud computing, pp. 58-64, July/August 2016.

[12] Edward Jero and Ramu, " Curvelets-based ECG steganography for data security", Electronics letters, Vol. 52, No. 4, pp. 283–285, February 2016.

[13] Pallavi.M and Chandrashekar.H.M, "Study and analysis of ECG compression algorithms", IEEE International Conference on Communication and Signal Processing, pp. 2028-2013, 2016.

[14] Ahmed Ibrahim, Baban Mahmood and Mukesh Singhal. "A secure framework for sharing electronic health records over clouds", IEEE International Conference on Serious games and Applications for Health (SeGAH), pp. 1-8, 2016.

[15] Vijendra.V and Meghana Kulkarni, "ECG signal filtering using DWT haar wavelets coefficient techniques", IEEE International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), pp. 1-6, 2016

[16] Shaheen S.Patel and S.V.Sankpal, "Secure patients data transmission using XOR ciphering encryption and ECG steganography", IEEE International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT 2016), pp. 1311-1315, 2016.

[17] Kefei Mao, Jie Chen, Jianwei Liu and, Mengmeng Wang, "Security enhancement on an authentication Scheme for privacy preservation in ubiquitous healthcare system", IEEE International Conference on Computer Science and Network Technology (ICCSNT 2015), pp. 885-892, 2015.

[18] B.Eswara Reddy and Gandikota Ramu, "A secure framework for ensuring EHR's integrity using fine-grained auditing and CP-ABE", IEEE International Conference on Big Data Security on Cloud, pp. 85-89, 2016.

[19] Pei Huang, Borui Li, Linke Guo, Zhanpeng Jin and Yu Chen, " A robust and reusable ECG-based authentication and data encryption scheme for eHealth systems", IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2016.

[20] Goldberger AL et al., "PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals", Circulation 101(23):e215-e220