International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-3, Issue-2, May 2014

Secured ECG Distribution using Compression and RSA Algorithm for Telemedicine Application

Vithya KP, Premkumar R

Abstract*: The detailed condition of a cardiac patient can be better understood from his ECG. For treatment of the patient over the internet both the security and the bandwidth issues plays a very vital role. A new approach which combines RSA for transmission and SPHIT (Set Partioning in Hierarchical Trees) for image compression which enables uploading of important coefficients of ECG signal. This technique not only provides security but also provides doctor to patient interaction. The simulation results indicate that the proposed method enhances the security for data transmission over the internet with a compression ratio of 2.5. The idea for choosing the SPHIT is it is lossless algorithm and much of importance is to be given to the patient details to provide perfect treatment by all means.

Index Terms: Image compression, Image encryption, discrete wavelet transform, RSA Encryption, SPHIT, ECG.

I. INTRODUCTION

Today, the network users demand audio, images and video along with the text this necessity has become the convergence of computers, networks, communications, and multimedia applications. The information revolution is projecting a new area where medical aspects will combine the functions of various devices [10]. The presence of a network has prompted new problems with security and privacy. The main requirement in order to communicate with images and video is a secured and reliable means. Present situation demands highly secured details of patients. ECG signal is supposed to contain sensitive health information of the patient. In recent developments network security and data encryption have become vital and high profile issues [11]. New approaches in encryption techniques are required to be developed for effective data encryption and multimedia applications. For future internet applications on wireless networks, besides source coding and channel coding techniques, cryptographic coding techniques for multimedia applications need to be developed [1]. Therefore in this paper architecture based on wavelet decomposition of ECG is proposed after the wavelet decomposition the important parts of the coefficients which are represent the P,Q,R,S,T signature decomposition of ECG signal, are segregated leaving the base line are iso-electric both the parts are compressed unimportant part is uploaded to the public repository without encryption[4]. A novel scheme for image compression and image encryption is being proposed in this paper. The concept is based on image compression and secured data transmission.

The approach of this method is based on the SET PARTITIONING IN HIERACHICAL TREES (SPIHT) and RSA Encryption is implemented for encrypting ECG data.

Revised Manuscript Received on 30 May 2014.
* Correspondence Author
Vithya KP*, PG Scholar, Mount Zion College of Engineering and Technology, Pudukkottai – 622507, Tamil Nadu, India.
Premkumar R, Assistant Professor, Mount Zion College of Engineering and Technology, Pudukkottai – 622507, Tamil Nadu, India.

II. BLOCK DIAGRAM

From the error description three basic problems for image transmission over Internet. They are bandwidth issue, error resilient issue, and security issue. The novel approach that is proposed in this the scheme is a combination of image compression and encryption techniques. This is to achieve a low bit-rate in the digital representation of an image with a minimum perceived loss in picture quality by image compression. To obtain high compression ratio with less distortion. For the security problem, DES algorithm is implemented, as this is the current encryption standard. The combination of compression and encryption techniques not only enhances the security for image transmission but also improves the transmission rate.

Determination of the Heart Rate and Rhythm

Normally, the heart of an adult is depolarized 60 to 90 times per minute. A depolarization rate lower than this is called sinus bradycardia, while one that is higher is called sinus tachycardia. The heart rate of the normal newborn is much higher than that of an adult. The heart rate can be calculated by dividing the R-R interval into 60. This number is denoted BPM (Beats Per Minute) [8],[12].

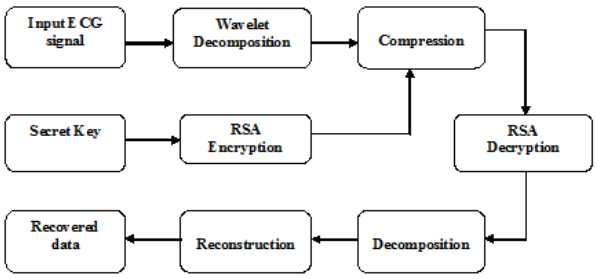

Fig 1. Block Diagram for ECG Distribution

The Duration of the Complexes and Intervals

After determining the heart rate and rhythm, the clinician should measure the duration of the waves and intervals on the electrocardiogram.

The Duration of the QRS Complex

The duration of the QRS complex represents the amount of time required for the depolarization of the ventricular to the Musculature. It is measured from the beginning of the Q wave to the end of the S wave.

In normal adults, the QRS duration is usually 0.10 second or less and in children, it is usually less than 0.08 second. When the QRS duration is greater than 0.10 second in adults, it is proper to consider the presence of some type of ventricular conduction defect.

The TQ Interval

The TQ interval is measured from the end of the T wave to the beginning of the next Q wave. During this period the ventricles are polarized and waiting for the stimulation that initiates depolarization.

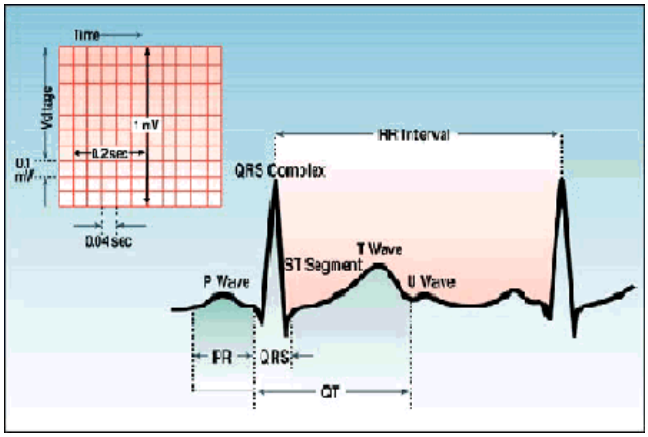

Fig 2. Wave Pattern of ECG Signal

Amplitude P-wave — 0.25 mV
R-wave — 1.60 mV
Q-wave — 25% R wave
T-wave — 0.1 to 0.5 mV

Duration P-R interval : 0.12 to 0.20 s
Q-T interval : 0.35 to 0.44 s
S-T interval : 0.05 to 0.15 s
P-wave interval : 0.11 s
QRS interval : 0.09 s

The normal value of heart beat lies in the range of 60 to 100 beats/minute. A slower rate than this is called bradycardia (Slow heart) and a higher rate is called tachycardia (Fast heart). If the cycles are not evenly spaced, an arrhythmia may be indicated. If the P-R interval is greater than 0.2 seconds, it may suggest blockage of the AV node. Certain disorders, involving heart valves cannot be diagnosed from ECG.

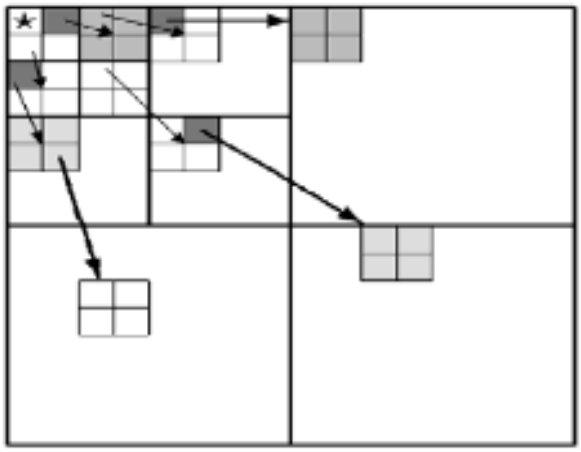

Fig 3. The Process of Compression and Decomposition

Other diagnostic techniques such as angiography and echocardiography can provide information not available in ECG. Each action potential in the heart originates near the top of the right atrium at a point called the pacemaker or sinoatrial (SA) node. The wave generated by action potential, terminates at a point near the center of the heart, called the atrioventricular (AV) node.

III. SIMULATION RESULTS AND DISCUSSION

In the implementation process SPIHT transformation is used for faster transmission and achieved a compression ratio of up to 2.66832. This faster transmission is greatly appreciated for remote telemonitoring, since ECG file are generally enormous in their size. At the same time confidentiality to the data transmitted to the receiver end is achieved as defined below:

Before Compression Size of ECG Signal: 64000B
Computation time for
Encoding time: 0.074 seconds
Encoding time: 0.017 seconds
Encoding time: 0.017 seconds
Encoding time: 0.020 seconds
After Compression size of ECG Signal: 30943B
Compression Ratio: 2.66832
PSNR: 23.5016

Below shown is the obtained GUI representation of the status of the patients ECG conditions to determine the normal and abnormal status. And hence secured ECG distribution is achieved by SPIHT and RSA algorithms.

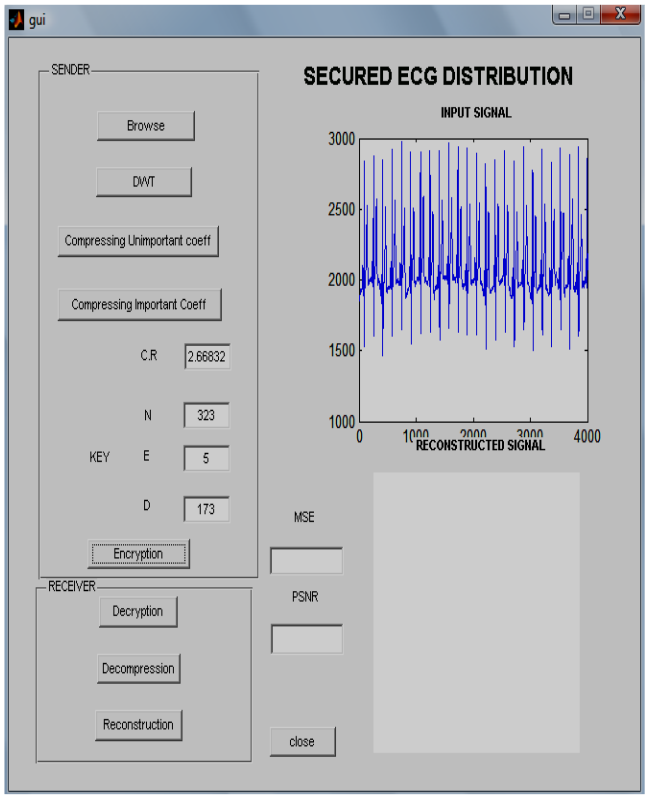

Fig. 4 Secured ECG Distribution

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Based on the approach a software was developed to compress and encrypt images. PSNR which gives the values of pixels in the original and the recovered images, respectively.

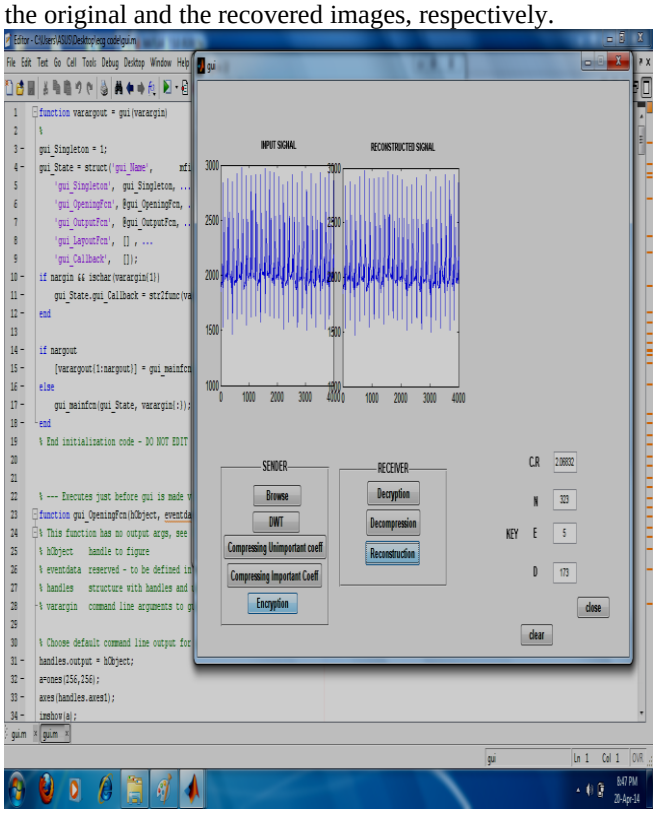

Fig 6. Reconstructed Original ECG

As discussed earlier in the proposed scheme SPIHT [3]and RSA[2] can also be used to have higher compression ratio and highly secured for transmission for patients centric International Journal of Wisdom Based Computing, Vol. 1 (3), December 2011 application and also for quality reconstructed of the ECG [8].

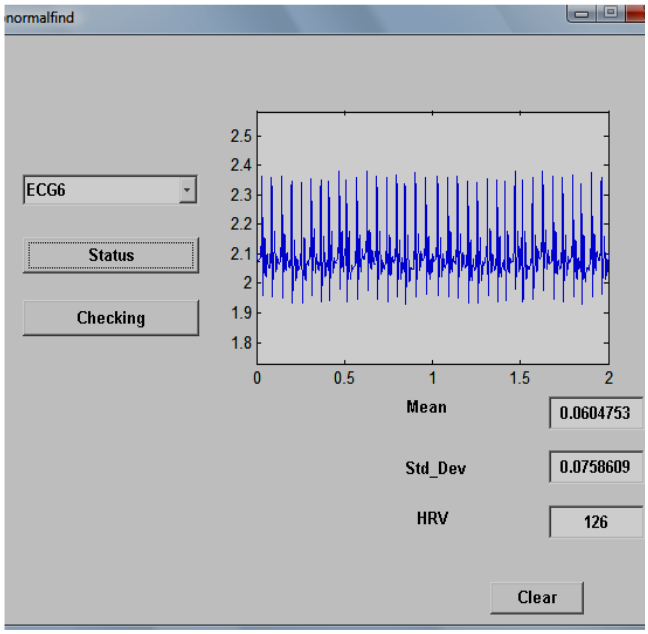

Fig.5 Status of the Patients ECG Normal/Abnormal

```
Input text:
Name:xxxxx

Age:45

Id:hd4352

status:normal
Encrypted text:
°Fé ;~b% :É¾ õ /yi ôIg7\ÃÒjÝ`Óz yUÓ )Ó!µ  al
Decrypted text:
Name:xxxxx

Age:45

Id:hd4352

status:normal
Percentage Residual Difference(%):
    0.1903

>>
```

Fig 7. Performance Analysis

IV. CONCLUSION

In this paper, a joint image compression encryption scheme for Internet health applications is presented. The SPHIT and RSA for image compression and image encryption allows high compression ratio and the security of transmission process is enhanced. Experimental results show that the ECG details are in comprehensible and the reconstructed images have acceptable quality. The timing measurements, shows that software simulation of compression and encryption scheme may be efficient to encrypt various health insurance portability and accountability in real time.

REFERENCES

1. Biel L, Peterson O, Philips on L,Wide P. Ecg analysis: a new approach in human identification. IEEE Transaction on Instrumentation and measurement at 2001.
2. W. Lee and C. Lee, “A cryptographic key management solution for hipaa privacy/security regulations,” IEEE Transactions on InformationTechnology in Biomedicine,, vol. 12, no. 1, pp. 34–41, 2008.
3. Shashikala Channalli et al, “Steganography An Art of Hiding Data”, International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141 137.
4. Chunlin Song, Sud Sudirman, Madjid Merabti, “Recent Advances and Classification of WatermarkingTechniques in Digital Images”,International Conference, Oct. 2009.
5. Ayman Ibaida, Ibrahim Khalil “Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Sys-tems” IEEE Transactions On Biomedical Engineering.
6. Ibaida, A. ; Sch. of Comput. Sci. & IT, RMIT Univ., Melbourne, VIC, Australia ; Khalil, I. Al-Shammary, D. , “Embedding patients confidential data in ECG signal for healthcare information systems”, Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE.
7. M. Engin, Y. Yamaner, E. Z. Engin, “A biotelemetric system for human ECG measurements”, Elsevier Measurement, Article in Press, accepted 7 April, 2005.
8. Chiaraluce F, Ciccarelli L, et al. A new RSA algorithm for video encryption. IEEE Trans Consum Electron 2002; 48:838–43.
9. Sufi F, Khalil I. A new feature detection mechanism and its application in secured ecg transmission with noise Masking. Journal of Medical Systems 2009; 33(3):121–132.
10. S. Jayaraman, S. Esakkirajan, and T. Veerakumar. Digital Image Processing. McGraw-Hill, 2009.
11. K. Zheng and X. Qian, “Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms,” in International Conference on Computational Intelligence and Security, 2008. CIS’08, vol. 1, 2008.
12. A. Al-Fahoum, “Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure,” IEEE Transactions on Information Technology in Biomedicine, vol. 10, no. 1, 2006.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)