A Secure Crypto based ECG Data Communication using Modified SPHIT and Modified Quasigroup Encryption

S.Sujatha
Associate Professor, School of IT & Science
Dr.G.R.Damodaran College of Science
Coimbatore, Tamilnadu, India.

R.Govindaraju
Research Scholar, School of IT & Science,
Dr.G.R.Damodaran College of Science,
Coimbatore, Tamil Nadu, India.

ABSTRACT
In recent years, wireless body area sensor network is one of the important aspects for the development of the healthcare applications. But, it has several issues based on the security and authentication during the transmission of the data. Because of the influence of the hackers, more importance is been given to security aspect in Wireless Body Area Sensor Networks communication. Cryptographic techniques are observed to provide significant results in protecting data from hackers and attackers. Some of the existing cryptographic algorithms such as selective encryption provide good results. The present research work mainly deals with securing the ECG data in Wireless Body Area Sensor Network (WBASN) before transmission. The existing algorithm is mainly based on the RSA algorithm which is used for data security during the transmission but it has some problems in real time applications and it is more exposure to vulnerable attacks. Therefore, in this paper, improved selective algorithm based on the modified quasigroup encryption is used along with the modified SPHIT compression algorithm. Modified quasi group encryption which uses genetic algorithm for optimization is used in this approach for improving the Quasigroup performance. The optimization based approach provides the optimized Quasigroup for encryption which gives better security for the ECG data. The results obtained are compared with other existing algorithm which is evaluated using the quality measurement parameters.

Keywords
Quasi group Encryption, ECG data, Cryptographic Encryption, Genetic Algorithm, SPHIT Compression

1. INTRODUCTION
In recent years, rapid development of the fields such as agriculture, medical, defense due to the technology development in wireless networking, microelectronics integration and internet. These technological developments are helpful to renovating the healthcare service in such a way that it can be useful for the early detection of the diseases, improving the existing healthcare system for managing the illness [1].

In body area sensor network physiological signals such as Electrocardiographic (ECG) signals are collected using biosensors which are placed inside the human body and it is mainly used for analyzing the diseases such as heart attacks, arterial blockages, and enlarged heart muscle [2]. The BASN consists of signal collector and biosensors. The biosensors are used to evaluate certain parameters in the human body either internally or externally. The server in the network is mainly used to collect the signals from the biosensors and the collected signals are transmitted to the remote networking for diagnosing the diseases. The data received after processing in remote diagnosis is used for planning the treatment [3].

The ECG data are very important because if any loss or distortion is occurred during the transmission of the data for the remote diagnosis. Sometimes the ECG data are unavoidably large because of long period of monitoring [4]. As mentioned above, if the loss occurs, then it will be reflected during the diagnosis of the diseases and it will affect the patient. The transmission of the ECG data in the BASN network is very important. The security issues in the body area sensor network cannot be ignored. As the transmission of ECG data is insecure in networks, encryption and compression have become necessary steps for securing the ECG data.

Cryptographic approaches have been extensively used in the security applications for securing various types of data in variety of applications. The academic attention and interest towards cryptographic techniques have increased in recent years because of its typical mathematical data-manipulation algorithms involving secret keys, encryption algorithms for confidentiality and Message Authentication Codes (MACs) and digital signature algorithms for real-time authentication, data origin authentication, integrity or non-repudiation. Therefore, Cryptography is observed to be the technique that can be incorporated in the software protection technique for improved protection [5].

A novel scheme for compression and encryption is being proposed in this paper. The compression of the ECG data is based on the Modified Set Partitioning in Hierarchical Trees (MSPIHT) algorithm and Modified quasigroup encryption is implemented for encrypting ECG data.

2. RELATED WORKS
A number of cryptographic techniques have been developed in the literature for various security applications. Each of those techniques has their own merits and demerits. This section clearly discusses about some of the most important cryptographic based techniques for security in wireless body sensor networks.

2.1 A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health
A new quasigroup based block encryption system with and without cipher-block-chaining has been presented in [6]. The performance of the Quasigroup approach is compared with Advanced Encryption Standard-256 (AES256) bit algorithm using the NIST statistical test suite (NIST-STS) that is tested

for randomness of a sequence. An efficient encryption algorithm must eliminate any statistical attributes of the input sequence and construct an output close to a true random sequence. It is observed from the results that the proposed algorithm provides significant results in almost all the test suites.

2.2 A two-tiered authentication and encryption scheme in secure healthcare sensor networks

The author uses the two tier authentication for secure communication in healthcare application of wireless sensor networks [7]. The unique key is used to encrypt the data in the first phase and it is generated in a decentralized fashion. It gives the security in non-trusted environment. In the second phase unique key is used as session key which is mainly used for authentication of data aggregation node from sensor nodes. This method gives confidentiality, authorization, and secure communication in wireless sensor networks healthcare applications. This security scheme is compared with the other security scheme and it is observed to provide the robust, prompt and scalable security services.

2.3 A design proposal of security architecture for medical body sensor networks

In wireless personal area networks security is one of the important issues during the real time implementation of body area sensor network because of the some vulnerability [8]. In this approach, the security scheme used in body area sensor network is mainly for high level security as well as light weight protocol. This security architecture has secure transmission of data using the bio-channel and the several secure aspects for physiological data.

2.4 An Integrated Biometric-Based Security Framework Using Wavelet-Domain HMM in Wireless Body Area Networks (WBAN)

A novel security framework based on the biometric approach is used in this research article. The framework has the body sensors which are mainly based on the advantages of the biometric features and sensors are placed inside the human body [9]. The communication between the sensors is very important because the data loss or data can be exposed to security threats easily. In this paper encryption scheme is used in the framework for effective and secure communication. A wavelet based hidden markov model along with the non Gaussian statistics is used for accurate authentication. The author simulated the framework and it is implemented in the real time environment. The performance of the framework is compared with the other security framework.

2.5 A Novel Biometrics Based Security Solution for Body Sensor Networks

The secure communication is always a serious issue in the wireless sensors network and it is one of the important issues in the healthcare systems also [10]. In this approach, the author used a novel scheme in security framework based on cryptography. The encryption scheme, key generation, integrity protection are used in the cryptography. The keys are generated using the ECG signals in the first phases. AES is used for encrypting and protecting the data in second phase. The security scheme is used to satisfy the requirements of the body area sensor network. It outperforms the other approaches in terms of power consumption and memory occupation.

2.6 Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs

Electrocardiographic system is one of the important machines in the medical field and it is mainly based on the wireless body area sensor networks [11]. The energy consumption and data security are two important issues in the ECG system. Many techniques are introduced for the energy consumption and security. In this approach, the author introduces a novel framework for energy consumption and secure communication. The framework is used for secure transmission of the ECG data by using the compression, encryption using RSA. SPHIT is used for compressing the ECG data and the compressed data is encrypted using the selected encryption mechanism which uses RSA. The two rate unequal error protection is used for saving energy in this security scheme. The existing schemes are compared with this security framework and the simulated results are showed improvement of 40% than the other schemes. The quality measurement is used for measuring the framework.

3. METHODOLOGY

As aforementioned in the survey, basic problems such as security issues, error resilient issue, bandwidth issues are discussed in the existing techniques. In this paper, a novel and improved frame work has been proposed for providing security and authentication to the ECG data. The framework consists of the compression, encryption and transmission. In order to obtain high compression with less distortion, in this paper, Modified SPHIT (MSPIHT) is used for the compression and modified quasi group encryption is used for encryption. Figure 1 clearly depicts the framework of the proposed approach which is used to improve the transmission rate and for secure communication of the ECG data.

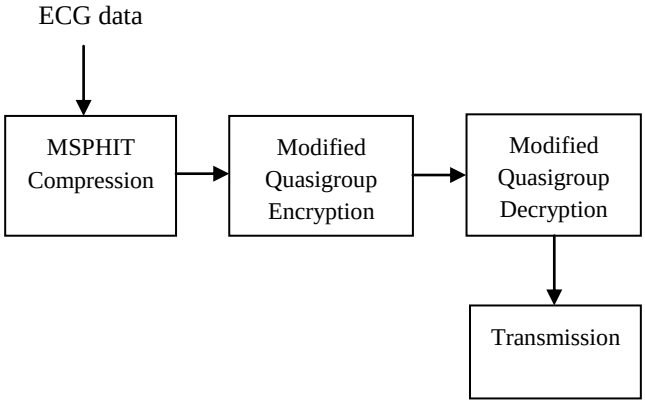

Fig 1: Block Diagram of the Overall Secured ECG

3.1 Modified SPIHT Coder for Compression

Set partitioning in hierarchical tree algorithm is one of the widely used compression algorithm. It is mainly used for improving the codec's efficiency. Although the SPHIT algorithm is used for compression in many fields it has some disadvantages such as memory consumption which affects the performance of the framework and results are not efficient. During the coding time of the SPHIT algorithm the elements

will be inserted or deleted in this list which consumes more time.

In order to overcome aforementioned problems Modified SPHIT is used as a compression algorithm in many fields. In this MSPHIT algorithm two concepts are mainly used for compressing the ECG data along with other parameters in the SPHIT algorithm. They are number of error bits and absolute zero tree [12].

Number of error bits: the most significant bits are used in the transform coefficients in SPHIT coding. The least significant bits are omitted in the decoding and it is called as truncating error.

The number error bits in the MSPHIT technique is represented as a μ_e and it is used for indicating the number of bits during the truncating error. In real time scenarios, after identifying whether $C\,(i,j)$ is insignificant or significant coefficient, its first $(\,n+1-\mu e)$ bits are given as output and it is not stored in the least significant bit of LIS.

Absolute Zero tree: The significant coefficients are mainly focused in the low pass subbands after the wavelet decomposition and the coefficient transform $C\,(i,j)$ magnitude is decreased because of the pyramid level decrement in the coding. The hierarchical trees in the coding are always zero tree and coefficient in the many segments are very small it leads to the compression ratio reached.

In SPIHT coding, zero roots coordinates are stored in the list of insignificance sets and never stored in the LIS. As a result LIS is expanded rapidly. In order to solve these problem absolute zero tree is introduced in modified SPHIT [13]. μ_e is defined as number of errors in truncating bits. If the magnitude of the coefficient transform is lower than the $2^{\mu e}$ then it is called as an absolute tree. The coordinates of the absolute zero tree is not stored in the LIS, length is the shortened, and coding time is also reduced [14]. The $Zero$ in the absolute zero tree is represents the set is absolute or not.

$$Zero\,(X(i,j)) = \begin{cases} 0 & if \ \max_{C(k,l)\in X(i,j)}\{|C(k,l)|\} \geq 2^{\mu_e} \\ 1 & otherwise \end{cases}$$

Where $X(i,j)$ represents $C(i,j), D(i,j) or\ L(i,j)$

As mentioned in Modified SPHIT number of error bits is used before encoding and it is used to represent the number of bits which is going to be omitted. After the wavelet coefficient last significant bits will be omitted. Absolute tree is used for reducing the size of the LIS and least significant bits are not stored in the LIS. These two things are mainly used for overcoming the memory consumption problem. The working of the Modified SPHIT algorithm is explained. The sorting and refinement process are combined together in the Modified SPHIT algorithm for reducing the time. The initial value in the modified SPHIT algorithm is used in the number of error bits for reducing the number of bits before coding. The process of the MSPHIT starts with the adding the coefficients to the LIS and omitting the last error bits [14, 15].

3.1.1 Algorithm Steps

Step 1: Wavelet coefficients are obtained from wavelet transform and initialize with number of error bits
Step 2: Select partitions of coefficients Um
Step 3: For each $n = n_0, n_0 - 1, n_0 - 2, ..$
Step 4: If $S_n\,(Um) = 0$ (the set is insignificant) then disregard bits in Um
Step 5: If $S_n\,(Um) = 1$ (the set is significant) then use recursive algorithm to partition Um
Step 6: Test sets until all significant coefficients found
Step 7: The following sets of coordinates are used to present the new coding method:
$O\,(i,j)$: set of coordinates of all offspring of node (i,j)
D (i, j): set of coordinates of all descendants of node (i, j)
H (i, j): set of coordinates of all spatial orientation tree roots (nodes in the highest pyramid level)
L (i, j): D (i, j) – O (i, j) (all descendents except the offspring)
Step 8: Three Lists
- LIP - list of insignificant coefficients
- LIS - list of tree roots (i, j) of insignificant descendant sets D (i, j) (Type A) or insignificant descendant of offspring sets L (i, j) = D (i, j) - O (i, j) (Type B)
- LSP - list of significant coefficients

Step 9: Number of error bits i.e., least significant bits are omitted.
Step 10: Lists tested in order LIP, LIS, LSP for efficient embedded coding
Step 11: Initialization of Lists
LIP: co-ordinates of all tree roots wavelet example: Coordinates in coarsest scale subband
LSP: empty: The coordinates of the tree roots are not stored in the LIS in MSPHIT algorithm because the memory consumption is more.
Step 12: Sorting and refinement pass
- Output nth bit of all LSP members found significant at thresholds greater than 2n
- Two bit types in stream: significance test bits and refinement bits

Step 13: Quantization Step Update:
- Decrement the value of n by 1 and go to sorting pass if n is not less than 0

MSPIHT compression algorithm has become an essential tool for uniformly quantizing the coefficients attained from the wavelet sub band decomposition of data.

Thus, the ECG data is compressed based on the MSPIHT algorithm.

3.2 ECG Encryption

This section discusses about the cryptographic encryption technique for ECG encryption. Quasigroup encryption technique is observed to provide good results and hence this research work adapts quasi group encryption and certain

modification has also been proposed in Quasigroup encryption for improving the security with less time consumption.

3.2.1. Quasi group Encryption

The compressed ECG data is given as an input to the quasigroup encryption and it is mainly used for the encryption of the ECG data based on the significant data scrambling properties. Even though the input is constant output is improved by using the scrambler. The quasigroup encryption is based on the permutation scrambling based in the basis of the algorithm [16].

In quasi group encryption $a_1, a_2, a_3, \ldots, a_n$ belongs to the quasi group Q. QE is defined as encryption operator in the algorithm and it is represented as defined over the predefined elements [17]. The quasi encryptor are used for mapping the predefined elements in another vector $b_1, b_2, b_3, \ldots, b_n$ and the elements of the resultant vector is also belongs to the same quasi group encryption. The encryption is define as a

$$E(a_1, a_2, a_3, \ldots, a_n) = b_1, b_2, b_3, \ldots, b_n$$

Where $b_1 = a * a_1, b_i = b_{i-1} * a_i, I$- it represents the number of elements that has to be encrypted in the iteration process and a is the hidden key.

The Multi Level Indexed encryptor is defined as

$$QE^{I_r, I_s}_{h_1, h_2, h_3 \ldots, h_n}(a_1, a_2, a_3, \ldots, a_n) = e_1, e_2, e_3, \ldots, e_n$$

Where $a_1, a_2, a_3, \ldots, a_n$ is represented as input data, $e_1, e_2, e_3, \ldots, e_n$ -the output vector and the array of the indices which is mainly used for the quasi group ordering are represented as $I_r, and\ I_s$.The vector $h_1, h_2, h_3 \ldots, h_n$ is the hidden key or the secret key [18].

Encryption Algorithm:

Input: compressed ECG data, Encryption Key

Output: Encrypted data

1. Get the data and store in r and c respectively.
2. Convert ECG data into matrix then it is converted into a vector
3. Obtain all odd position values initially and then even position values.
4. Construct a new data matrix by filling the odd positions values followed by even position values.
5. Convert new matrix into a vector.
6. Convert the decimal key into binary key data.
7. Binary key data is embedded in the vector.
8. Convert the vector into data matrix of size (r,c).

3.2.2. Decryption

The decryption is the process of the constructing the inverse data matrix and it is very similar to the encryption process. The decryption process is defined as a

$$D(a_1, a_2, a_3, \ldots, a_n) = e_1, e_2, e_3, \ldots, e_n$$

Where $e_1 = a/a_1$ and $e_i = a_{i-1}/a_i$

Decryption Algorithm:

Input: *encryption data, decryption Key*

Output: *decrypted data*

1. Convert the encrypted data into the vector.
2. Convert the decimal key into binary key
3. The binary key data is initially used for decryption and stored as a vector.
4. The vector is converted to data matrix of size(r, c).
5. The data matrix is divided into the two vectors
6. The new matrix is formed by filling the odd position and even position from two vectors
7. The resulted decrypted data is obtained.

3.3 Proposed Modified Quasi Group Encryption

This research work proposes a novel modified Quasigroup encryption algorithm using metaheuristic approach. This approach uses a heuristic algorithm called genetic algorithm for quasi group optimization.

Genetic Algorithms (GAs) are one of the most promising metaheuristic optimization algorithms. GA looks for an optimal or sub-optimal solution of a given problem through imitating the natural evolution. The solutions are encoded into chromosomes which are the linear data structures that are appropriate for application of the genetic operators. The genetic operators apply the principles of biological evolution in real time software [19]. The crossover operator is the most essential operator in GA that simulates sexual reproduction of haploid organisms. Alternatively, mutation operator makes random alterations to the genotype. The entire process is improves the significance of the population of candidate solutions. The value of each solution is evaluated using fitness function that assigns higher score to better candidate solutions [20].

GA was initially applied to the quasigroup optimization in [21] and the technique was further extended in [22]. The artificial evolution was utilized to explore superior quasigroups isotopic to the quasigroup of modular subtraction [19]. As the bit permutation was carried out, a huge number of quasigroups could have been discovered without wide memory requirements.

GA for the identification of analytic quasigroup is done through encoding of the candidate solutions and fitness function to assess chromosomes [21].

3.2.3. Fitness function based on products of sequences

A number of fitness functions were already been developed for quasigroup optimization. Fitness functions depending on hashing [21], randomness of generated sequences [22], and the associativity and commutativity [23] were observed to drive the evolutionary optimization of isotopic quasigroups in specific direction.

This paper formulates a new fitness function depending on the latest modelled property of quasigroups, the heterogeneity of products of sequences [24]. This approach aims to identify a quasigroup that would produce heterogeneous products of k elements a ∈ Q i.e. a^k as possible. Moreover, the quasigroup

should generate different sequences of intermediate results $b_1, b_2 \ldots . b_k$ when computing a^k for all a ∈ Q using all possible products elements. In this approach, only the highest power k = n is utilized to calculate heterogeneity (randomness) of products of sequences.

Consider a Quasigroup of modular subtraction (Q, o), where Q = {0,1,...,n − 1} and operation o is defined as $a\ o\ b = (a + n - b)$ mod n. Consider a vector of results of the power operation $\vec{r} = (r_o, r_1, \ldots . , r_{n-1})$, where r_i is the number of cases in which $a^n = i$ for all a ∈ Q and all product elements of n elements of Q. Let $\vec{\imath} = (i_o, i_1 2, \ldots . , i_{n-1})$ be a vector of intermediate results where i_i is the number of times $b_j = 1$ during the evaluation of a^n for all a ∈ Q, 1 ≤ j ≤ n and all product elements. Let $\vec{s} = (s_o, s_1, \ldots . , s_{n-1})$is the vector containing the number of distinct sequences of intermediate results obtained when computing a^n i.e. $s_i$equals to the number of all distinct sequences generated when computing i^n [19].

Tree fitness functions are defined based on the product elements:

$$f_1^{a^n}(\vec{r}, \vec{\imath}) = \frac{1}{2}\left(\frac{\sum_{j,\vec{r}_{j>0}}(1)}{n} + \frac{\sum_{j,\vec{\imath}_{j>0}}(1)}{n}\right)$$

$$f_2^{a^n}(\vec{r}, \vec{\imath}) = \frac{1}{2}\left(\frac{\max(\vec{r}) - \min(\vec{r})}{\max(\vec{r})} + \frac{\max(\vec{\imath}) - \min(\vec{\imath})}{\max(\vec{\imath})}\right)$$

$$f_3^{a^n}(\vec{s}) = \frac{\max(\vec{s}) + \min(\vec{s})}{2C_n}$$

Where C_n denotes the n-th Catalan number.

The fitness function$f_1^{a^n}$assigns large fitness to quasigroups in which it holds: ∀q ∈ Q ∃a: $a^n = q$ and $\forall q \in Q\ \exists a\ \in Q\ \exists l\ \in \{1,2, \ldots , n\}$: $a^l = q$. Alternatively, it chooses quasigroups that generate such sequences that consists of all elements of Q at least once. The fitness function $f_2^{a^n}$assigns large fitness to quasigroups that generate sequences containing all elements of Q with approximately the same frequency. Ultimately, the third fitness function assigns large fitness to quasigroups that generate as different sequences of intermediate results as possible [21].

3.2.4. *Overall Proposed Encryption Approach*

- Phase1: Encryption of ECG data using quasigroup based encryption system.
- Phase2**:** Then optimization of quasi group algorithm is done using genetic algorithm.
    a) Initialization of GA to Quasigroup Optimization
    b) Search of Significant Quasigroup
    c) Identification of analytic Quasigroup
    d) Encoding of fitness function

These two phases are clearly depicted in figure 2.

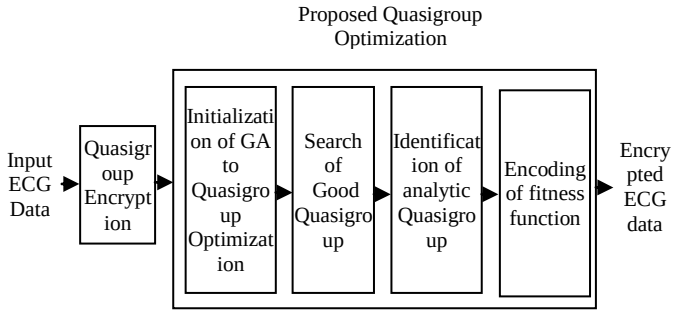

Fig 2: Proposed Encryption Framework

Thus, after attaining the encrypted ECG data, the ECG data are transmitted through WBSN.

The proposed security algorithm for transmitting ECG data as an input data has following advantages

1) The number of bits is reduced in the ECG data by using the compression algorithm. So that the number of bits to be encrypted is also reduced.
2) It is gives more secure communication than the other existing algorithms.

4. EXPERIMENTAL RESULTS

For experimental evaluation of this proposed work, three sample ECG data are taken for consideration. The proposed system for secure communication is evaluated and it is compared with the traditional security algorithm such as RSA. Moreover, for the compression phase, proposed Modified SPIHT compression coder is compared with SPIHT.

The proposed framework for security can be evaluated objectively and subjectively. The quality measures used to compare the performance of the proposed security framework are Mean Square Error (MSE), Peak Signal To Noise Ratio (PSNR) and Encryption and Decryption Time.

4.1 Mean Square Error (MSE)

The mean square error is defined as the cumulative measurement of the proposed algorithm.

$$MSE = \frac{1}{MN}\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(X,Y) - I'(X,Y)]^2$$

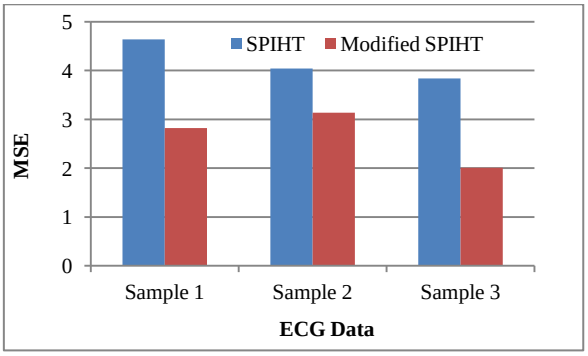

Fig 3: MSE Comparison

Figure 3 clearly depicts the MSE comparison of the proposed Modified SPIHT with SPIHT. It is clearly observed from the figure that the proposed Modified SPIHT approach attains lesser MSE when compared with the SPIHT approach. For all

the three ECG data taken for consideration, the MSE values of the proposed Modified SPIHT approach is very less when compared with the existing SPIHT approach.

4.2 Peak Signal to Noise Ratio

The quality of the data after the decryption is measured using the PSNR ratio

$$PSNR = 10 \log 10 \left(\frac{255^2}{MSE} \right) db$$

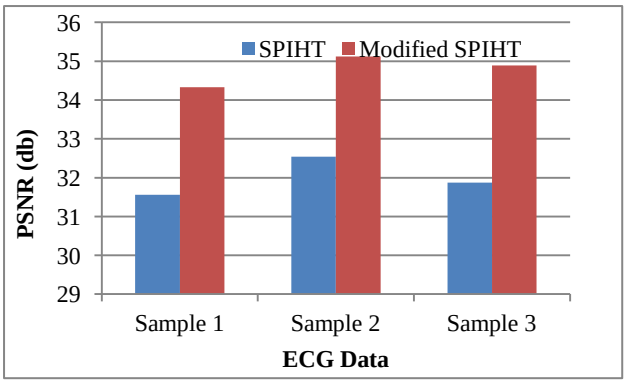

Fig 4: PSNR Comparison

PSNR value comparison of the proposed MSPIHT and existing SPIHT approach is clearly depicted in figure 4. It is clearly observed from the figure that the proposed Modified SPIHT approach outperforms the existing SPIHT approach. For instance, for ECG sample 1, PSNR attained for existing SPIHT is 31.56 db, where as for the proposed Modified SPIHT approach, it is 34.33 db. Similarly, for the other two samples, the PSNR of the proposed approach is higher than the existing approach.

4.3 Encryption and Decryption Time

The speed of the algorithm is directly proportional to size of the data. Encryption time of the existing RSA and quasigroup algorithm is compared with the proposed modified quasi group encryption approach.

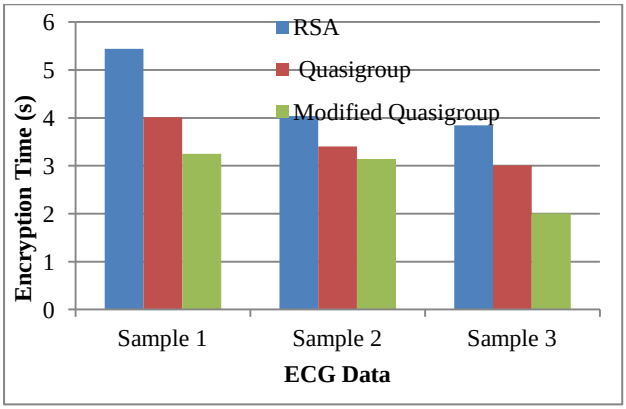

Fig 5: Encryption Time Comparison

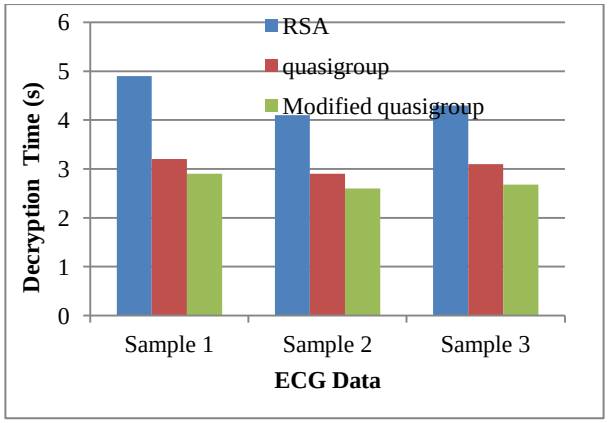

Fig 6: Decryption Time Comparison

Figure 5 and 6 clearly shows the encryption and decryption time comparison between the existing and proposed approach respectively. The proposed modified quasi group approach clearly outperforms the existing approach. The time taken for encryption and decryption of the proposed Modified quasi group encryption is very less when compared with existing RSA and Quasi group encryption approaches.

5. CONCLUSION

ECG data security has become an essential issue to be taken into consideration in the medical analysis. In recent years, due to the improvisation of various attacks, the necessity of efficient security system has taken its own importance. In this paper, an efficient cryptographic security framework has been proposed to provide security to the ECG data in WBSN. This approach includes the encryption and compression algorithm for ECG data. An efficient modified quasigroup encryption algorithm and modified SPHIT compression algorithm is used for encryption and compression of the ECG data respectively in the proposed framework. Quasi group encryption is observed to provide significant results and this paper improves the performance of the Quasigroup algorithm by integrating Genetic Algorithm. The proposed security framework is measured by using the quality measures such as PSNR ratio and mean square error rate. Experiments are conducted with ECG data and the results are compared with the other existing algorithms. The proposed algorithm outperforms the other algorithm and it provides the strong and fast secure communication.

6. REFERENCES

[1] E. Dishman, “Inventing wellness systems for aging in place," *IEEE Computer*, vol. 37, no. 5, pp. 34-41, May 2004.

[2] Khalil, I and Fahim Sufi, “Real-time ECG data Transmission with Wavelet Packet Decomposition over Wireless Networks”, International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Page(s): 267 - 272, 2008.

[3] Yogita L. Kumbhare, Pankaj H. Rangaree, Dr.G.M.Asutkar “Wireless Body Area Sensor Network Authentication using HMAC function” 2nd National Conference on Information and Communication Technology (NCICT) 2011.

[4] Islam, M.R. Ahmad, S. Hirose, K. ; Molla, Md.K.I., “Data adaptive analysis of ECG signals for cardiovascular disease diagnosis”, Proceedings of 2010

IEEE International Symposium on Circuits and Systems (ISCAS), 2010.

[5] DR Stinson, Cryptography, Theory and Practice, 2nd edition, Chapman & Hall, CRC Press, Boca Raton (2002).

[6] Matthew Battey and Abhishek Parakh, "Efficient Quasigroup Block Cipher for Sensor Networks", Cornell University Library, 2012.

[7] Kanjee, M.R. Divi, K. ; Hong Liu, "A two-tiered authentication and encryption scheme in secure healthcare sensor networks", Sixth International Conference on Information Assurance and Security (IAS), 2010.

[8] Ramli, S.N. , Ahmad, R. ; Abdollah, M.F. ; Dutkiewicz, E., "A biometric-based security for data authentication in Wireless Body Area Network (WBAN)"15th International Conference on advanced Communication Technology (ICACT), 2013.

[9] Chol-soon Jang ; Deok-Gyu Lee ; Jong-Wook Han, "A Proposal of Security Framework for Wireless Body Area Network" International Conference on Security Technology, 2008.

[10] Jingwei Liu Zonghua Zhang ; Rong Sun ; Kyung Sup Kwak, "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks" IEEE International Conference on Communications (ICC), 2012.

[11] Shu-Di Bao ; Yuan-Ting Zhang , "A design proposal of security architecture for medical body sensor networks" International Workshop on Wearable and Implantable Body Sensor Networks, 2006.

[12] Yong Sun, Hui Zhang, Guangshu Hu, "Real-time implementation of a new low-memory SPIHT image coding algorithm using DSP chip", IEEE Transactions on Image Processing, vol 11, Issue 9, pp 1112 1116, Sept. 2002 .

[13] M. Akter, M. B. I. Reaz, F. Mohd-Yasin, and F. Choong, "A Modified-Set Partitioning in Hierarchical Trees Algorithm for Real-Time Image Compression", ISSN 1064-2269, Journal of Communications Technology and Electronics, 2008, Vol. 53, No. 6, pp. 642–650. © Pleiades Publishing, Inc., 2008.

[14] Kazi Rafiqul Islam, Md. Anwarul Abedin, Masuma Akter, and Rupam Deb "High Speed ECG Image Compression Using Modified SPIHT" International Journal of Computer and Electrical Engineering, Vol. 3, No. 3, June 2011.

[15] M. Blanco-Velasco, F. Cruz-Roldan, J. Godino-Llorente, and K. Barner, "Wavelet packets feasibility study for the design of an ECG compressor," IEEE Trans. Biomed. Eng., vol. 54, no. 4, pp. 766–769, Apr. 2007.

[16] G.Mohana Priya, P.Vasanthi Kumari,"Compression of Quasi-Group Encrypted Grayscale Images", International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012.

[17] Maruti Venkat Kartik Satti, "Quasi Group based Crypto-System", A Thesis, 2007.

[18] Koscienly, C. 2002. Generating quasi groups for cryptographic applications. Int. J. Appl. Math. Comput. Sci., vol.12, No.4, 559–569.

[19] Eliska Ochodkova, Pavel Kromer, Jin Dvorsky, Jan Platos, Ajith Abraham, Vaclav Snasel, "Genetic Search for Quasigroups with Heterogeneous Power Sequences", Third World Congress on Nature and Biologically Inspired Computing (NaBIC), 2011.

[20] M. Mitchell, An Introduction to Genetic Algorithms. Cambridge, MA: MIT Press, 1996.

[21] V. Snasel, A. Abraham, J. Dvorsky, E. Ochodkova, J. Platos, and P. Kromer, "Searching for quasigroups for hash functions with genetic algorithms," in World Congress on Nature & Biologically Inspired Computing, pp. 367 – 372, IEEE Computer Society, 2009.

[22] V. Snasel, J. Dvorsky, E. Ochodkova, P. Kromer, J. Platos, and A. Abraham, "Genetic algorithms evolving quasigroups with good pseudorandom properties," in ICCSA (3) , vol. 6018 of Lecture Notes in Computer Science, pp. 472–482, Springer, 2010.

[23] V. Snasel, J. Dvorsky, E. Ochodkova, P. Kromer, J. Platos, and A. Abraham, "Evolving quasigroups by genetic algorithms," in DATESO, vol. 567 of CEUR Workshop Proceedings, pp. 108–117, 2010. ISSN 1613-0073.

[24] E. Ochodkova, J. Dvorsky, V. Snasel, and A. Abraham, "Testing quasigroup identities using product of sequence," in DATESO , vol. 567 of CEUR Workshop Proceedings, pp. 155– 162, CEUR-WS.org, 2010.