IJERT
ISSN : 2278-0181
International Journal of Engineering Research & Technology
Publish & Find Papers @ www.ijert.org
BROWSE
OPEN ACCESS
Call for Papers

Enhanced Audio Steganography using Triple DES and DWT Transformation

Chetan M.D
M.Tech Student,
Digital electronics ,Dept. of ECE,SSIT,
Tumakuru, India, 572105.

Anitadevi M.D,
Assistant Professor,
Dept. of ECE, SSIT, Tumakuru,
India, 572105.

***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 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 are being transmitted over the public network as well as when they are stored in hospital servers used by remote monitoring systems. In this paper, 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. To evaluate the effectiveness of the proposed technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference and the wavelet weighted PRD. It is found that the proposed technique provides high-security protection for patients data with low (less than 1%) distortion and ECG data remain diagnosable after watermarking (i.e., hiding patient confidential data) and as well as after watermarks (i.e., hidden data) are removed from the watermarked data.**

Keywords— Steganography, DWT, ECG, Triple DES.

I. INTRODUCTION

To attain a progressive sustainable development in all regions of the world, attention should be diverted to the health of a population. All sciences contribute to the maintenance of human health and the practice of medicine. Medical physicists and biomedical engineers are the professionals who develop and support the effective utilization of this medical science and technology as their responsibilities to enhance human health care with the new development of the medical tools such as electrocardiogram (ECG). Heart disease is a broad term that includes several more specific heart conditions which are Coronary Heart Disease, Heart Attack, Acute Coronary Syndrome, Aortic Aneurysm and Dissection, Ischemia, Arrhythmias, Cardiomyopathy, Congenital Heart Disease, Peripheral Arterial Disease (PAD).The most common heart condition is coronary heart disease, which can lead to heart attack and other serious conditions and the Myocardial Ischemia is the most common cause of death in the industrialized countries . The electrocardiogram (ECG) is a noninvasive and the record of variation of the bio potential signal of the human heartbeats. The noninvasive technique meaning that this signal can be measured without entering the body at all. Electrodes are placed on the users skin to detect the bioelectric potentials given off by the heart that reach the skins surface. The ECG detection which shows the information of the heart and cardiovascular condition is essential to enhance the patient living quality and appropriate treatment. It is valuable and an important tool in the diagnosing the condition of the heart diseases. POCT is well established worldwide and play a vital role in public health monitoring. It is one of the standards of care in disastrous situation. Major benefits of POCT include more quick decision making and triage, rapidly reducing operating times, with greater reduction in high dependency, post operative care time, reduction in emergency room time, reduce number of outpatient clinic visits and ensure medical

- A five level discrete wavelet decomposition technique for data hiding in ECG signals.
- Triple DES cryptographic algorithm and scrambling matrix based asymmetric encryption and decryption for protecting data confidentiality and integrity.

To weigh up the effectiveness of proposed algorithm on the ECG signal, various distortion measurement metrics like percentage mean square error difference (PRD) for different scrambling matrix combination and the other evaluation metrics such as peak signal to noise ratio for various embedding capacity.

II. RELATED WORK

AymanIbaida and Ibrahim khadil[1] proposed a wavelet based steganography for ECG signals to hide patient information as well as diagnostic information inside ECG signals with XOR ciphering technique to encrypt the patient confidential information. The challenging task here was to retain originality of ECG signal data to remain diagnosable after retrieving patient secret information from ECG signal.

PawanKshetramaladilip and V.B.Raskar[2] have suggested an algorithm to hide patient data inside ECG signals using discrete wavelet transform . But encryption is carried through less secure XOR ciphering and is only tested for text information being the secret data.

Anusha T. Karthikkumar B, ThilakaK[3] have proposed an algorithm for secret data communication through ECG signals. The data hiding technique uses the LSB replacement algorithm for concealing secret message bits into high frequency coefficients. But algorithm is verified for single

wavelet decomposition technique as well as single scrambling matrix combination and only text data being the secret information.

M.SabarimalaiManikandan and S. Dandapat[4] have put forward an objective distortion measure for compressed electrocardiogram signals, with less security being the major limitation , since even unauthorized person can view the medical records sent via network.

NilanjanDey, sayantan et.al[5] have proposed a watermarking technique within ECG for authentication , but fails to retain the originality of ECG signal due to strong security aspects. But major concern in point of care system is to retain the important information in ECG signal for it to be diagonasable.

Hamid.A.Jalad, A.A.Zaidan et.al [6] have discussed a new design for hiding information hiding (data file) within image page of Execution file(EXE file) to ensure that the changes made to the file will not be detected by hackers. But the hiding technique is applied for general information rather than medical data, where lossless retrieval of cover data information is not mandatory.

Mohamed A. Seif At el [7] proposed the ECC based DES algorithm. The DES is a symmetric key Cipher algorithm. The ECC technique is used to generate the required key. The ECC based DES method is applied for different image files for both encryption and decryption with large key space to resist brute force attack. The parameters considered are histogram analysis, correlation, PSNR, MSE and key sensitivity analysis.

Blessy Joy A et al, [8] proposed the cryptographic technique, ECC technique is used to encrypt the RGB image to protect the data from unauthorized access. The image undergoes pixel wise xor operation and encrypted by ECC. Required number of bit planes are encrypted to achieve different levels of security. Parameters like processing power, energy, bandwidth limited for ECC are considered. It is used in multimedia communication.

Chuanmu Li et al, [9] proposed the image watermarking in DWT domain. The binary watermark is generated by a Chaotic map using secret key. The sub bands of 3 level DWT are selected to embedding the watermark by adjusting the coefficients order in different orientation. Parameter such as PSNR, MSE are considered.

Aayushi Verma et al , [10] proposed steganography technique, that is Discrete Wavelet Transform (DWT). The complexity of hidden image has been decreased through DWT technique. The DWT algorithm is used for embedding and extracting the secret image embedded behind the cover gray scale image. Parameters such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), secure, robust and embedding capacity, less distortion are considered.

Nikita Gupta et al, [11] proposed the ECC technique for color image. NIST curves are used for ciphering the color images. The ECC technique key size is compared with RSA method depending on the strength and speed .Parameters such as timing analysis, size are considered.

Pallavi H. Dixit et al, [12] proposed the cryptography and steganography techniques for data security on open network. BLOWFISH method is used for data encryption and Steganography uses List significant Bit (LSB) for hiding the encrypted data. Iris image of authorized person is used to hide encrypted data for the security purpose. The secret key is generated from same iris image which is required for encryption using BLOWFISH algorithm. On 32 bit ARM 7 the algorithms are implemented. Parameters such as memory utilization, processing time for encryption and decryption, security for embedded systems are considered. it is used in mobile, smart card, ATM etc.

Melad J. Saeed et al, [13] proposed the cryptography and steganography techniques in which chaotic method is used for data encryption and Discrete Cosine Transform (DCT) domain to hide encrypted color image. The original image in spatial domain is transformed to frequency domain using DCT. The cover image is embedded in DCT. Parameters such as MSE, PSNR and normalized correlation (NC), to phase and capacity are considered.

III. PROPOSED MODEL

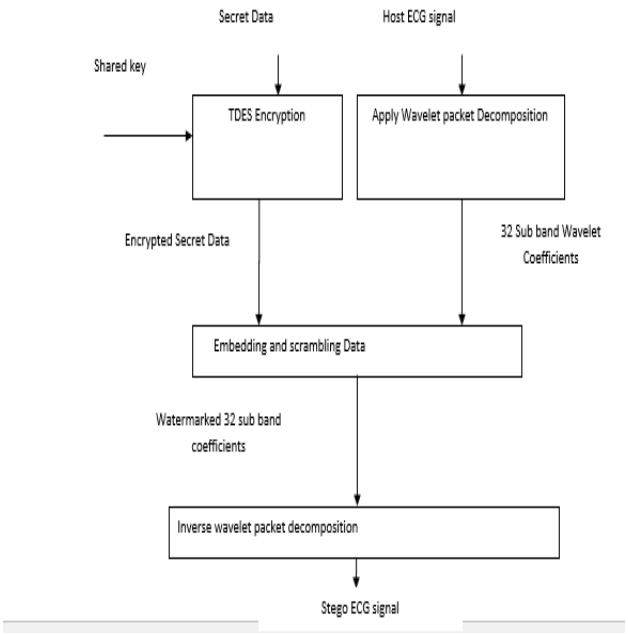

Fig. 1. basic model of the proposed system.

The source side of proposed steganography algorithm consists of four unified stages

- Encryption of secret information
- Wavelet decomposition of host ECG signals
- Embedding and scrambling of secret data
- Inverse wavelet recomposition.

Figure 1 shows the basic model of the system. Assume that the host ECG signal is a one dimensional array of coefficients having 7200 samples sampled at a rate of 360Hz. The host ECG is first decomposed into 32 sub bands by applying 5 level wavelet packet decomposition as shown in fig(2). Then the text information is encrypted using RSA technique, finally the encrypted text is embed into the wavelet sub bands.

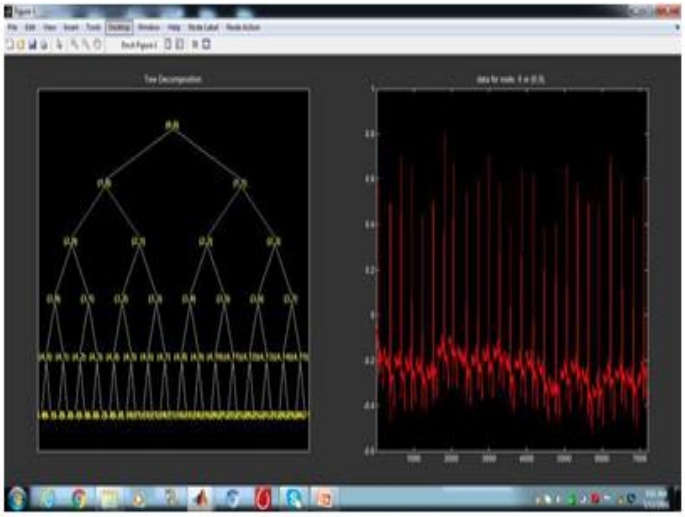

Fig. 2. A Five level Wavelet Decomposition of ECG Signal

IV. SYSTEM IMPLEMENTATION

A. *Triple DES Algorithm*

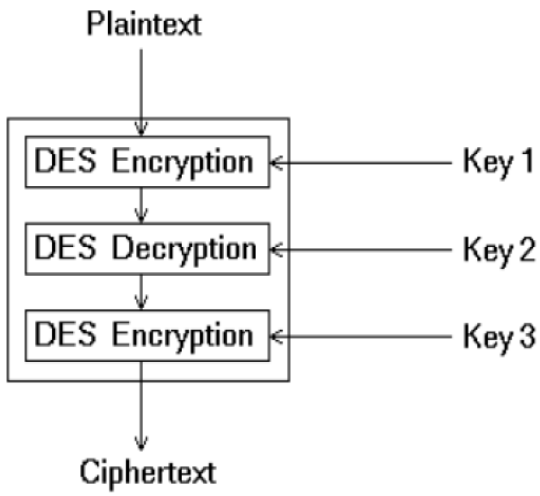

Fig. 3. Triple DES Algorithm

The main aim of this stage is to encrypt the patient confidential information in such a way that it prevents unauthorized persons who does not have the shared key from accessing patient confidential information.

- As a first step, we need to choose two large distinct prime numbers p and q.
- The product of p and q, we call n as a component of the "public key". It must be big enough such that the numbers p and q cannot be extracted from it - 512 bits minimum i.e. numbers greater than 10. ^154.
- Later we generate the encryption key e which should be co-prime to the number m = f (n) = (p -1) (q -1).
- We will then create the decryption key d such that demod m = 1. Now we have both public and privatekeys.
- let y = E(x) be the encryption parameter where x is an integer and y is the encrypted form of x

y = x. ^e mod n

- let X = D(y) be the decryption parameter where y is an encrypted integer and X is the decrypted form of y

X = y. ^d mod n

B. *Embedding Algorithm*

After generation of cipher text by using Triple DES algorithm, we embed the encrypted secrete information in the sub bands obtained after decomposing the ECG signal.

- Convert the cipher text into stream of binary digits.
- The shared key known to both the sender and the receiver.
- Second is the scrambling matrix as shown in fig (2) which is stored at both the sender and the receiver side. Each sender/receiver pair has a same scrambling matrix.
- Scrambling matrix is of 128X32 dimension and the elements of matrix should lie between 1 and 32, with following conditions being met
- Duplicate elements should not be present in the same row. The same row must not be duplicated.
- Apply the scaling operation on each coefficient in the sub bands.
- Access each coefficient from the sub band depending on the sub band number obtained from scrambling matrix .Embed the information bits into the LSB's of sub band coefficients.
- The steganography level selected for bands from one to seventeen is 5 bits. Since more information is carried in these bits.
- The steganography level selected for rest of the bands is 6 bits
- Apply the inverse scaling operation on each stego coefficients in the sub bands.
- Apply the inverse wavelet recomposition on watermarked sub band to obtain the watermarked ECG Signal.

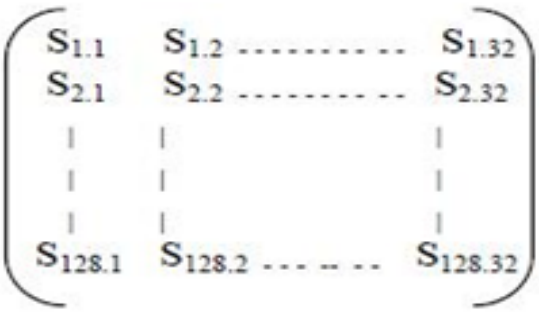

Fig. 4. Scrambling Matrix

After generation of cipher image by using T-DES algorithm convert into stream of binary digits. we embed these bits streams into the sub bands obtained after decomposing the ECG signal. The shared key known to both the sender and the receiver. Second is the scrambling matrix, which is stored at both the sender and the receiver side. Each sender/receiver pair has a same scrambling matrix.

C. Features Extraction using DWT

The Wavelet Transform (WT) is designed to address the problem of non-stationary ECG signals. It derived from a single generating function called the mother wavelet by translation and dilation operations. The main advantage of the WT is that it has a varying window size, being broad at low frequencies and narrow at high frequencies, thus leading to an optimal time-frequency resolution in all frequency ranges. The WT of a signal is the decomposition of the signal over a set of functions obtained after dilation and translation of an analysing wavelet . The ECG signals which consisting of many data points, can be compressed into a few features by performing spectral analysis of the signals with the WT. These features characterize the behavior of the ECG signals. Using a smaller number of features to represent the ECG signals is particularly important for recognition and diagnostic purposes. The ECG signals were decomposed into time-frequency representations using Discrete Wavelet Transform (DWT). The DWT technique has been widely used in signal processing tasks in recent years. The major advantage of the DWT is that it provides good time resolution. Good resolution at high frequency and good frequency resolution at low frequency. Because of its great time and frequency localization ability, the DWT can reveal the local characteristics of the input signal. The DWT represents a 1-Decompodition signal s(t) in terms of shifted versions of a low pass scaling function φ(t) and shifted and dilated versions of a prototype band pass wavelet function ψ(t).

D. Extraction Algorithm

- Apply wavelet decomposition on Stego ECG signal.
- Perform the scaling operation on each coefficient in the sub bands.
- Access each coefficient from the sub band depending on the sub band number obtained from scrambling matrix.
- Extract the information bits into the LSB's of sub band coefficients.
- Perform Triple DES decryption to obtain the original information.

V. PERFORMANCE EVALUATION OF PROPOSED METHOD WITH RESPECT TO TEXT DATA BEING THE SECRET INFORMATION.

Case No	PRD (WESPCIP)[1]	PRD
1	0.326605	0.000230
2	0.326308	0.000244
3	0.32775	0.000147
4	0.327904	0.000223
5	0.326824	0.000350

$$\Psi_{j,k}(t) = 2^{(-j/2)}\,\psi\,(2^{-j}\,t - k) \quad (1)$$

$$\varphi_{j,k}(t) = 2^{-j}\,\varphi\,(2^{-j}\,t - k) \quad (2)$$

Where: j controls the dilation

k denotes the position of the wavelet function

TABLE1: PRD COMPARISON OF PROPOSED METHOD WITH EXISTINGTECHNIQUE

TABLE II: ENERGY COMPARISON OF ORIGINAL ECG SIGNAL WITH WATERMARKED ECG SIGNAL FOR THREE DIFFERENT WAVELETS

Energy of original Signal	Energy (bior 6.8)	Energy (coif5)	Energy (sym4)
2292.611390	2292.647231	2292.639145	2292.701158
298.031456	298.127262	298.120742	298.104580
937.885150	937.882490	937.897849	937.845577
522.558325	522.577383	522.473382	522.504598

In Table 1: The PRD in percentage for the proposed algorithm is tabulated for different combination of Scrambling matrix and is compared with existing technique(WESPCIP)[1]. Proposed algorithm is found to be more efficient resulting in less distortion, so that ECG signal remains diagnosable even after retrieval of secret information.

In Table 2: The energy of different ECG signals is compared with watermarked ECG signal(with text data being the hidden information) is compared by using Coiflet, Bioorthogonal and symlet wavelets. It is found from the tabulated results that Coiflet wavelet based decomposition method results with less distortion as compared with rest two.

In Table3: PSNR for various capacities of text data being the secret information is being tabulated. It shows that as the number of secret data bits increases , the variations in ECG signal also increases, which results in decrease in peak signal to noise ratio(PSNR).

TABLE III: CAPACITY IN BITS VERSUS PSNR

Capacity in bits	PSNR (dB)
1632	57.0790
2416	51.3008
3200	49.1874
3984	47.0587

VI. PERFORMANCE EVALUATION OF PROPOSEDMETHOD WITH RESPECT TO IMAGE DATA BEING THE SECRET INFORMATION.

TABLE IV: ENERGY COMPARISON OF ORIGINAL ECG SIGNAL WITHWATERMARKED ECG SIGNAL WITH IMAGE DATA BEING SECRET INFORMATION FOR THREE DIFFERENT WAVELETS.

Energy of original Signal	Energy (bior 6.8)	Energy (coif5)	Energy (sym4)
298.031456	298.031462	298.031457	298.039118
2292.611390	2292.611425	2292.611390	2292.609555

TABLE V: PRD IN % FOR DIFFERENT COMBINATION OF SCRAMBLING MATRIX

Case No	PRD Proposed
1	0.548048
2	0.553667
3	0.547663
4	0.550826
5	0.557623

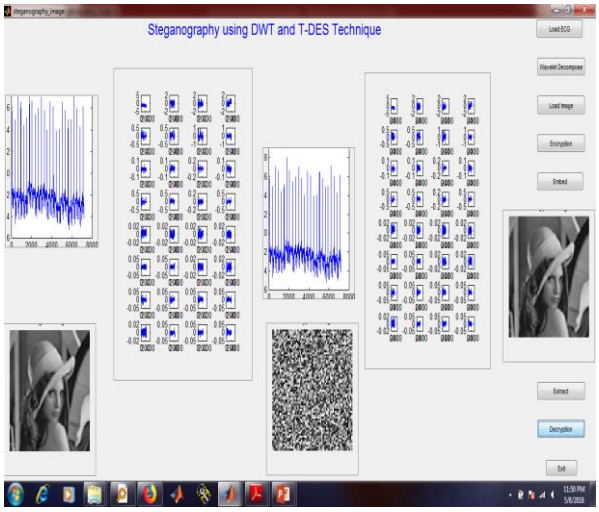

Fig. 5. final obtained results.

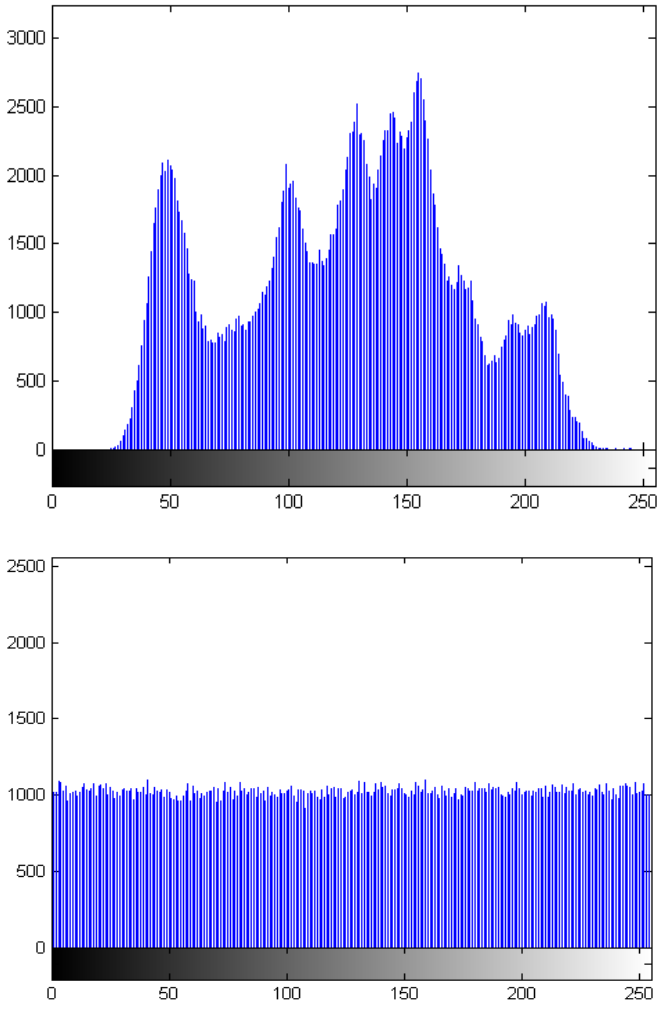

Fig. 6. Histogram of Plain and Cipher Image

VII. CONCLUSIONS

The proposed algorithm allows ECG signal of the cardiac patient to hide corresponding patient confidential data(both text and image) and other various physiological information, thus assuring the integration between ECG and the rest of the parameters. In order to evaluate the effectiveness of the proposed technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference and the wavelet weighted PRD. It is found that the novel proposed technique provides high security protection for patient data with very less distortion and ECG data will remain diagnosable even after retrieving secret information from watermarked data.

REFERENCES

[1] AymanIbaida and Ibrahim Khalil," Wavelet based ECG steganography for protecting patient confidentialinformation in point of care systems," IEEE Trans.Biomedical Engineering, vol. 60, no. 12, December 2013.

[2] Ms. PawarKshetramalaDilip, Prof. V. B. Raskar " Hiding Patient Confidential Information in ECG Signal Using DWT Technique"

[3] International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015

[4] Anusha.T, Karthikkumar.B, Thilaka.K "DWT Based Secured Patient Monitoring System" International Journal of Engineering Trends and Technology (IJETT) – Vol 9 Number 14 - Mar 2014

[5] M. SabarimalaiManikandan, Student Member, IEEE, and S. Dandapat, Member, IEEE "Multiscale Entropy-Based Weighted DistortionMeasure for ECG Coding" IEEE SIGNAL PROCESSING LETTERS, VOL. 15, 2008 page no:829

[6] NilanjanDey, SayantanMukhopadhyay, Achintya, and Sheli Sinha Chaudhari, "Analysis of P-QRS-T components modified by blind watermarking technique within the ECGsignal for authentication in wireless telecardiology using DWT".International Journal of Image, Graphics, SignalProcessing, vol. 4, no 7, July 2012.

[7] Moamed A. Seif Eldeen, Adbellatif A. Elkouny, Salwa Elramly "DES algorithm security fortification using elliptic curve cryptography", IEEE issue 2 Dec 2015

[8] Blessy Joy A,R. Girish, "RGB image encryption based on bitplanes using Elliptic Curve Cryptography", vol. 5, Issue 2, February 2015.

[9] Chuannu li, Haiming sing," A novel watermarking scheme for image authenticaton in DWT domian", vol 61, issue 20 Oct 2013.

[10] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique", 2014.

[11] [12]. Nikita Gupta, Vikas Kundu, Neha Kurra, Shivani Sharma, Bhagyashree Pal, "Elliptic curve cryptography for ciphering image", IEEE issue 25 Jan 2015

[12] Pallavi H. Dixit, Kamalesh B. Waskar, Uttam L. Bombale, "Multilevel Network Security Combining Cryptography and Steganography on ARM Platform", Vol. 3, No. 1, 2015

[13] Melad J. Saeed, "A new technique based on Chaotic Steganography and Encryption text in DCT domain for color image", Vol. 8, No. 5, 2013.