Secure medical image steganography based on Discrete Wavelet Transformation and ElGamal encryption algorithm

S.Jeevitha [a], N.Amutha Prabha [a,1*]

[a] School of Electronics Engineering, VIT University, Vellore-632014, India
[1] s.jeevita@vit.ac.in, [2] amuthaprabha@vit.ac.in*
* corresponding author

ARTICLE INFO

Article history
Received: 2021-12-17
Revised: 2022-03-21
Accepted: 2022-05-29
Published: 2022-07-20

Keywords
Cryptosystem
Steganography
DWT
ElGamal Encryption
Embedding Capacity

ABSTRACT

The latest development in computing methodologies and related steganography based applications had created a novel practice such as telemedicine where patient diagnosis images or allied information can be used diagnosis practices that are located in remote areas. In order to provide accurate and effective telemedicine the flawless or seamless biomedical information is required from patient. With respect to this the medical data may remain prone to get corrupted by hackers or might get manipulated when transmitted through an insecure channel. The cryptosystems which are available are not efficient enough to solve the above mentioned issues. Hence, in this research work a much efficient and effective image steganography technique has been proposed in order to hide the confidential and important image information. We have incorporated Discrete Wavelet Transformation (DWT) technique instead of wavelet transform techniques to embed the secret message in the required cover images. Also, to assure continuous communication through insecure channel, a new model called ElGamal encryption cryptosystem model has been implemented which contains the steganography scheme which has been proposed and developed. To maintain the content of Region of Interest (ROI), Region of Non- Interest (RONI) is used to embed the secret information. The overall performance analysis reveals that the DWT with ElGamal encryption provides more efficient and also have high embedding capacity, imperceptibility when compared to other methods like Hamming code, Syndrome-Trellis Code (STC) and Rivest-Shamir- Adleman (RSA) based methods.

1. Introduction

The Recent development in technology and related computing techniques increased the implementation steganography applications among which medical image exchange is one of the major one. In present day medical devices, broadcast of biomedical image has become one of the major requirement to maintain the efficient and secure communication of data over insecure channels. Currently, the telemedicine discipline has gained outstanding momentum, which has enabled efficient and well timed analysis remotely. However, the likely challenges on image information/data deviation cannot be ignored. In many instances, the important biomedical image data is transferred quite in a distinctive manner. Such transmission will continue to be prone to the attackers inside channel and consequently there can be compromise toward the secrecy of the affected person's key information. To exchange the biomedical information, Digital Imaging and Communications in Medicine (DICOM) has introduced an efficient standard for biomedical information storage, analysis and

transmission over different channels. At present in many applications it is necessary to share the examined medical image information to different locations through different channels, where the image information might get exposed to attackers. This crucial data may get accessed by the intruders who cannot have right access which would possibly lead the information to get misused. Apparently, in biomedical application making sure those intact photo characteristic and key facts is predictable. In such implementations maintaining entire picture records confidentiality in the course of transmission throughout channel is necessary. Where, many efforts were made to improve information security at the transmission. But, with particular medical image information hiding technique or record embedding methods has received much interest. Numerous data hiding tactics such as Watermarking, Cryptography/Cryptosystems and Steganography were carried out to secure the data. Between those dominant technologies, Steganography is more efficient and appropriate for important information safety over uncertain channel conditions [1]. Steganography is the recent technique which is used to hiding the confidential information onto a cover image and transmitting it through an unsecure channel [2]. With the intention to perform data hiding in cover image or biomedical image, many techniques has been developed [3]. These techniques are mainly categorized into two main categories a) Spatial domain b) Frequency domain [4], in which the spatial technique embeds the secret information directly in to the Least Significant Bit (LSB) of the cover image, where in the frequency domain technique the secret data is embedded within the LSB of the coefficients. Regrettably, while implementing spatial domain method the image quality might get distorted and as a consequence making it vulnerable to get accessed by third-party because of perceptibility issues. However, frequency domain techniques are restrained due to low flexibility towards offensiveness [5].

Perceptibility brought on due to embedding the top motive behind such limitations, and hence to cope with it, researchers [6] recommended Optimal Pixel Adjustment Process (OPAP) based LSB embedding method. This method exhibited higher stego-picture quality with quite lower complexity. Even as thinking about the essential system of medical image safety, especially while imposing steganography, it is crucial to make sure that the techniques have higher embedding potential and least perceptibility. It is vital to achieve improved data transformation at the same time as information embedding. In comparison to different fundamental current techniques, the Discrete Wavelet Transform (DWT) approach has been implemented on this paper, which plays a prominent role to select/retrieve the most appropriate coefficient for information hiding. Additionally, it could enhance the existing problems of the Wavelet Transform (WT) referred as two dimensional (2D) singularity issues [7]. When compared to reversible steganography, Inverse DWT (IDWT) has been implemented for data extraction at the decryption end. Further, another additional use of the proposed work is to provide higher security scheme of encrypting patient's information by implementing ElGamal Encryption Algorithm (EEA).

As a result, in conjunction with ensuring high security of affected person's secret information it also ensures accessibility of the secret information. The most viable aspect of the presented method is the implementation of safety technique together with the improved DWT based steganography. EEA cryptosystem has been implemented to comfy the information access. The effectiveness of the proposed technique has been analyzed along with statistical assault evaluation over stego image. The proposed work gives higher Peak Signal to Noise Ratio (PSNR), low Mean Square Error (MSE), very less or even negligible perceptibility and the required histogram differences.

2. Related Work

There are numerous processes to secure patient's important information. The challenging parts of those methodologies are how much information can be stored, and up to what extent the approach is safe.

Zheng et al. [8] had proposed an efficient reversible method based on WT. Their technique is primarily based on making use of B-spline WT on the initial ECG signal to locate QRS complex. On the original image Haar lifting WT is implemented after detecting the R wave's original ECG signal. Later, by comparing non-QRS high-frequency coefficients are selected and index subscript mapping is applied. Then, the water mark is embedded by shifting one bit of the selected coefficients to the left. Then using reverse Haar lifting WT the original signal is reconstructed.

S.Matey et al. researchers had proposed a real-time information embedding technique by using inverse wavelet transform (IWT), where the output was in integer form so the memory consumption

was relatively less. Also In [10], IWT based steganography has been implemented where multiple images have been converted into single image by using left-flipping and a dummy image was created by using Arnold Transform.

Barton et al. [11] implemented the reversible data hiding technique which uses compressive steganography method. WT technique had been applied to achieve the better data embedding but the efficiency was comparatively less and also the compression rate was less. A low distortion reversible technique has been introduced [12] to increase the compression rate, where a fixed portion of the signal is compressed which contains critical information and the portions which are prone to attacks. Tian et al developed a new approach based on pixel difference in order to increase the embedding efficiency, where an increased reversible data embedding can be observed. But in this approach the authors were not able to address the further consequences which might lead to the vulnerability of attacks.

In order to analyze an image, it is important to consider two major regions in the images that are ROI and RONI [14]. The region that contains most crucial data in radiographic images is termed as ROI. In this region it is difficult to perform any kind of modification in a radiographic image which might cause misdiagnosis. The non essential portion of the medical image referred as RONI [15].For extraction of ROI and RONI in a medical image, both supervised and unsupervised strategies are used. Supervised method compromise the accuracy of segmentation, so automated techniques which are implemented in lots of segmentation strategies [16].

As mentioned, the above researchers have made an analysis on different data encryption techniques by using various steganography methods. These kinds of strategies have been especially focused on either PSNR enhancement or embedding capacity enhancement using WT techniques. The primary requirement like conservation ROI, maximum imperceptibility, minimal or negligible histogram variations, statistical attack resilience, higher PSNR has no longer been considered plenty.

To maintain the quality of image, information hiding algorithm became evolved using statistics coding and edge detection approach. Also, RSA based totally protection key Encryption, Ripplet Transform, LSB embedding has been implemented.

The proposed method overcomes the constraints of existing scientific image data hiding strategies like excessive computational cost, confined embedding rate and also it achieves essential balance among embedding capability and quality of the stego-image

3. Materials and Methods

In this section, the analysis of the implemented methodology including algorithm designs and steganography techniques which are proposed for hiding the secret information has been efficiently explained. EPR were embedded into sharp area using canny edge detection technique. The flowchart of the proposed process is shown in Figure 1.

ElGamal encryption and DWT techniques combined to maintain the quality of stego images. In order to top-up another level of security, an efficient and simple encryption methodology has been introduced to hide the meaning of EPR. This technique possesses higher embedding capacity and imperceptibility by enabling a best solution for biomedical image transmission over public channels.

The encryption of secret information using ElGamal encryption technique has been applied initially and then cipher text data has been embedded into the image. To recover the confidential information, the encrypted data is extracted from the stego image using pre-implemented extraction system. Eventually, the decryption technique is carried out to retrieve the original secret data. The proposed method contains of six foremost procedures as listed: wavelet approach, encryption, edge detection, embedding, extraction, and decryption.

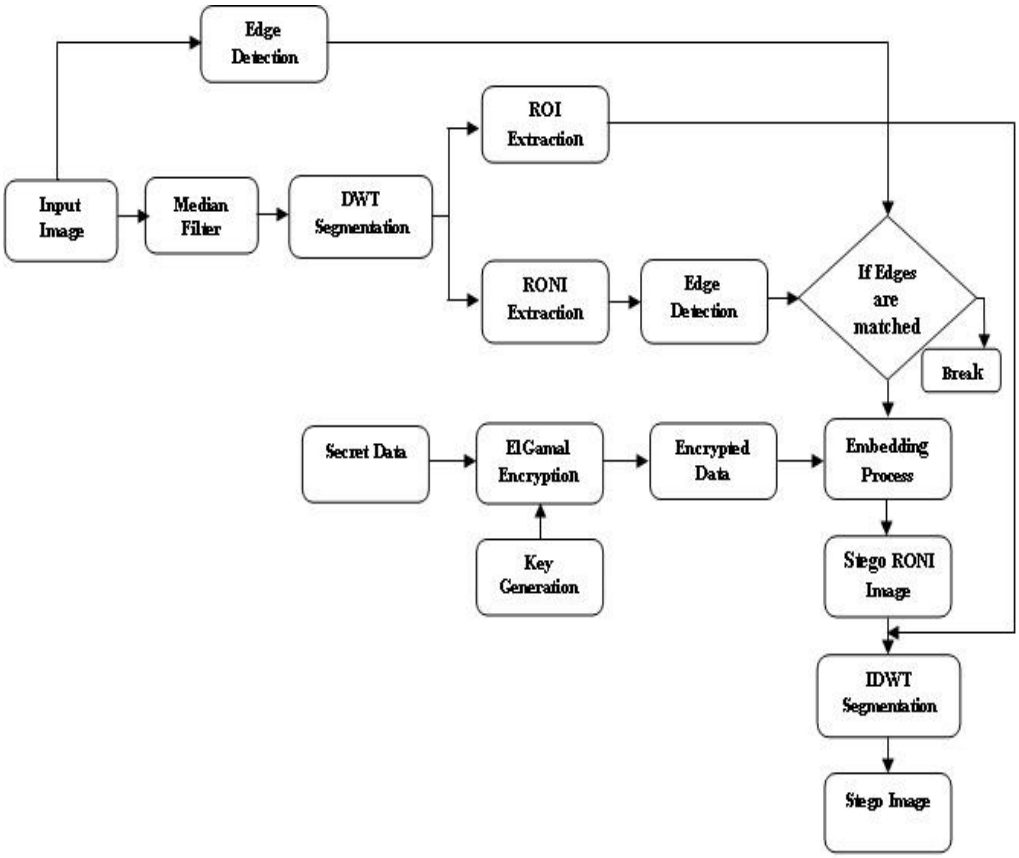

Fig. 1. The block diagram of the proposed embedding process

3.1. Implementation steps

1) Image acquisition process

Image acquisition describe as "the process of recovering an image from the different source, commonly PET, SPECT, CT, MRI and hence it can be flow through any technique which need to occur further". Image Acquisition is the first important step used to perform the workflow sequence in image processing. The image acquired from this stage is completely an unprocessed image and it is the output of hardware which has been used to create it. However, it will contain important data which is necessary in some fields to have a constant baseline from which to process further [17].

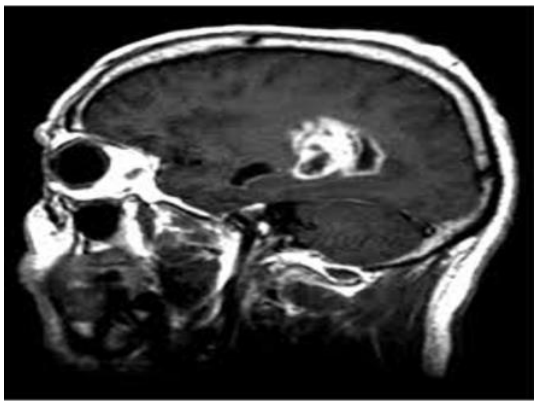

Fig. 2. Input Medical Image

This normally involves recovering images from a particular source which can automatically capture images. It creates a stack of files that can be automatically processed. The input image is shown in **Figure 2.**

2) Median filter

Median filter is a nonlinear filter tool to remove noises in an image. This can be implemented directly from the hardware and does not require many resources. Median filter is traditionally used to eliminate impulse noise as it is one of the popularly used non-linear filters. Usually, standard median filter won't perform well when impulse noise is more than 0.2.

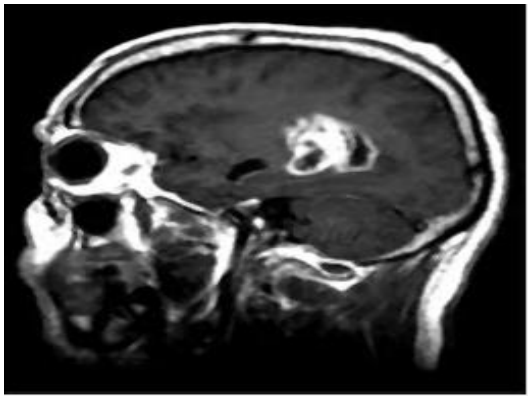

Fig. 3. Pre-processed median filter image

A simple median filter is efficient only when the noise intensity is less than 10-20%. In case, if the noise intensity is increasing, a simple median filter will leave many shots unfiltered. Hence, median filter won't retain details and it also smoothen non-impulsive noise. This is a statistical case where in given sorted list of numbers, the median is the center value of the list. J. W. Tukey [18] implements the median filter in Signal / Image processing. In case, if the count of the list is even, there might be multiple number center values. If the count of list is odd, then there is one single median value. Hence, it is suitable to use odd list sizes while implementing median filter. The Median Filter can be achieved by considering all of the vector's magnitude in a mask and arranging the magnitudes. Then to replace the pixel studied the pixel with the median-magnitude is utilized. When compared to mean filter, simple median filter has more advantages where the result depends on median on behalf of mean valued, where a single noisy pixel is present in an image, it can efficiently skew the mean of a set, but the median of a set is more resistant and effective related with the existence of noise. The pre-processed median filter image is shown in **Figure 3**.

3) Discrete Wavelet Transform

In signal processing WT has been widely used and also in many stages of image compression due to their in-built multi-resolution nature. Wavelet coding methods are efficiently appropriate for applications where scalability and allowable degradation is necessary. In WT signals are decomposed into a set of basic functions. These basic functions are known wavelets. Wavelets can be generated from a unique sample wavelet Ψ (t) known as mother wavelet by shifting and dilations. It can be denoted as Eq. (1) [19]: Where 'p' is the scaling factor and 'q' is the shifting factor.

$$\chi_{p,q}(t) = \frac{1}{\sqrt{p}} \chi(\frac{t-q}{p}) \quad (1)$$

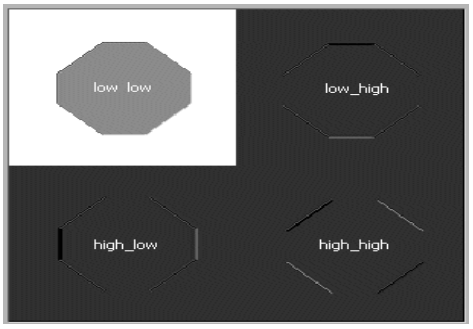

Fig. 4.2D- DWT Image

DWT is an efficient technique for hierarchically disintegrate an image. The input image in DWT is mainly decomposed into four labeled components as LL (Low), HL (Horizontal high), LH (Vertical high) and HH (high) [20] and it is shown in **Figure 4**.

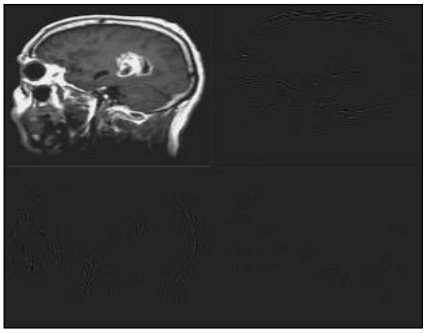

Fig. 5.DWT Image

In DWT, the initial letter responds to either a low pass frequency or high pass frequency process with respect to the rows, and the other letter indicates the respective filter implemented with respect to columns. LL contains of the estimate measure of the original image. The other level contains the in-depth parts and gives the LH, HL and HH frequencies. **Figure 5** represents 2D-wavelet decomposition of an image [21].

4) Region of Interest (ROI)

A ROI is a subdivision of selected element in a dataset considered for a certain purpose. This concept usually implemented in many applications like medical imaging to identify/measure boundaries of a tumor to find the volume or size in an image respectively. Usually, ROI is associated with definite or measureable information, which can be expressed as text or in structured format. In digital images ROI will circumscribe a preferred atomic location.

Where the average statistical value is calculated for all pixels in the ROI and returned to the operator. In many of the E-Learning videos is stated that the information will be available only in the part of blackboard portion, hence in this proposed approach only this part is focused and the resultant ROI and RONI images are represented in **Figure 6** [22].

Fig. 6.ROI and RONI Image

5) Canny edge detection process

Edge detection is the mechanism used to embed the essential information in keen-edged contrast regions of an image in order to produce an efficient and high quality stego image. The normal human eye will be unable to notice the sharpened edges when compared with other areas [23, 24]. The difference between the cover image and stego image is noticeable with the existing edge detection techniques like Sobel, Prewitt, and Roberts. Hence, a simple and efficient algorithm introduced to detect the edge regions on the image by implementing the canny edge detection algorithm as shown in the Figure 7. In this method the edge detection process will use multi-stage algorithm to identify a wide range frequency values at the edges of the images. In Canny edge detection, it will extract important basic information from distinctive vision objects and shorten the amount of information to be processed. This algorithm can be explained in 5 different steps as stated below:

Algorithm 1 The Canny Edge Detection procedure.

- Step1: Initially, to smooth the image and to get rid of the noise, Gaussian filter is applied to the cover image.

- Step2: Further, intensity gradients of the image are identified.
- Step3: False edge detection is removed by applying non maximum suppression.
- Step4: Then dual threshold is applied to diagnose the potential edges.
- Step5: Later edges were tracked by hysteresis method.

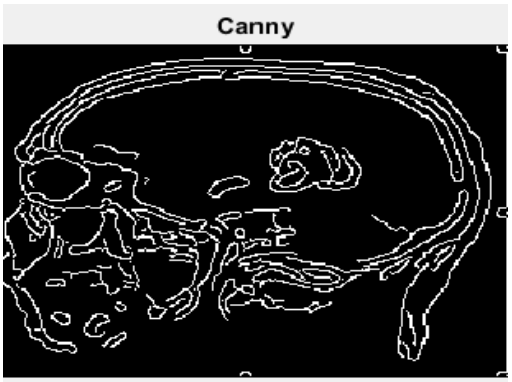

Fig. 7. Canny Edge Detection

6) Encryption and decryption process

To improve the confidentiality of the patient diagnosis data records, top secret data gets encrypted onto the medical image using the different encryption approach. In spite of, the existing encryption techniques have some inefficiency like high computational price. The ElGamal technique implemented to overcome the drawbacks of existing methods. It is one of the leading encryption methods to encrypt the Image/Text for protected transmission.

a) ElGamal cryptosystem

The ElGamal cryptosystem was proposed by T.ElGamal in 1985. The security of this cryptosystem depends on the difficulty of identifying distinct logarithms modules in a large prime numbers. Hence, the modification is made using the ElGamal cryptosystem over a simple root of a large prime number in encrypting and decrypting gray and color images with help of MATLAB program.

The various image encryption techniques implemented to modify the original input image into modified image that will be difficult to understand. In order to keep the image information secret between users and the external factors it is necessary to encrypt the data efficiently so that the content should not be identified without a secret key for decryption [25]. The public key and private key is the pair of key used in Asymmetric Cryptosystem and also called public key cryptosystem. Public key is necessary during the encryption and can be communicated. The private key should be retain only by the recipient of the message and pre-owned at the instance of decryption [26].

The key-generation involves the successive steps [27]

- Choose a large prime p and a positive integer r so that r will be the primitive root of p.
- Choose a positive integer $1< a \leq p-2$.
- Calculate $s \equiv (r)\ a \pmod p$.
- Let the public-key be declared openly→ (r, s, p).
- Let the private key be kept secret → (a)

To encrypt a gray or color image alone the public key (r, s, p) is required, then the cipher image (encrypted image) will be outcome from the plain image (original image). The Processing detail of ElGamal cryptosystem are illustrate in the successive steps.

Algorithm 2 The ElGamal encryption and decryption procedure

b) ElGamal encryption

- Step1: Translate the input image into its corresponding matrix (call it M) using MATLAB such that each element mij in M will not go beyond the prime number p.
- Step 2: The public key is (r, s, p).
- Step 3: For all the element mij in the matrix, select one random integer k with $1 \leq k \leq p-2$.
- Step 4: Calculate $X \equiv r^k \pmod{p}$.
- Step 5: Calculate $yij \equiv (mij * s^k) \pmod{p}$
- Step 6: Display the encrypted image Y.

c) ElGamal decryption

- Step1: Implicate to data (Y) from the encrypted image
- Step 2: Restore the input image M, such that $M \equiv [Y ((X)^a) -1] \pmod{p}$
- Step3: Attain the original image (decrypted image).

7) Embedding process

The embedding system begins by isolating the cover image into ROI and RONI images. To discover the edge area, a high value is primarily assigned to the threshold variable, later modified with respect to the data length and the number of pixels required. An ElGamal is employed to encode the secret information and then embed it into the known edge pixels. The embedding process illustrates in the successive steps.

Algorithm 3 The Embedding procedure

- Step1: Classify the ROI and RONI area in input image.
- Step2: Identification of edges
- Step3: Comparison among the ROI and edge area locations
- Step4: Classification of edge pixels
- Step5: Data Embedding
- Step6: Update the stego image

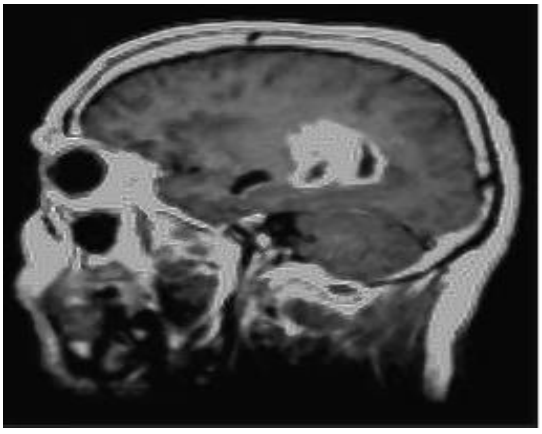

Fig. 8. Stego image.

After implementation of above steps like encrypted data embedding into RONI image using data hiding method and ElGamal encryption process, the stego image is like **Figure 8**.

8) Extraction process

To extract the data securely the stego image is decrypted using two different processes: Initially the data will be extracted from the cover medium and then cover medium is retained. Then to obtain the data the reverse process is performed, it is shown in **Figure 9**.In this process the secret hidden text messages are extracted from encrypted stego image.

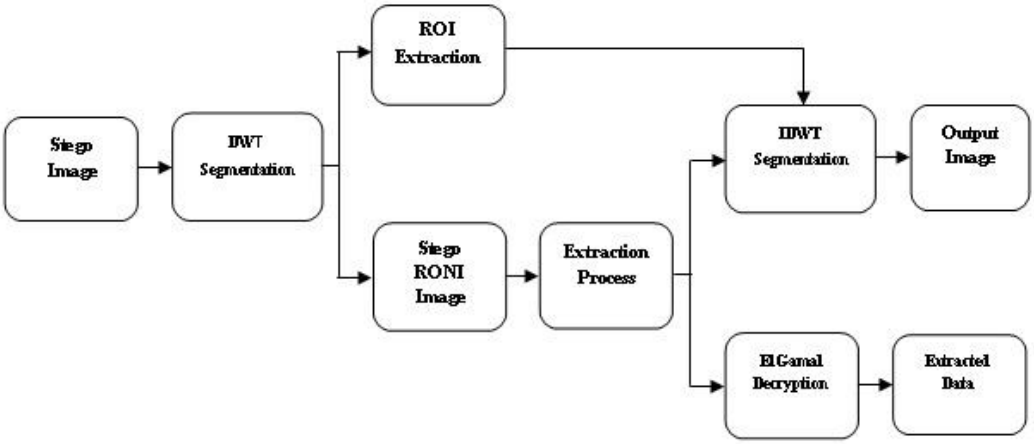

Fig. 9. The Block diagram for data Extraction Process

To subdivide the stego image into the ROI and RONI, coordinates of ROI should be extracted from the first edge blocks using the XOR operations. Hidden text bits are extracted using RDH methods from RONI image. Finally all extracted message characters are applied to ElGamal decryption module to decrypt the information with symmetric keys and restore the original image as in shown in Figure 10.

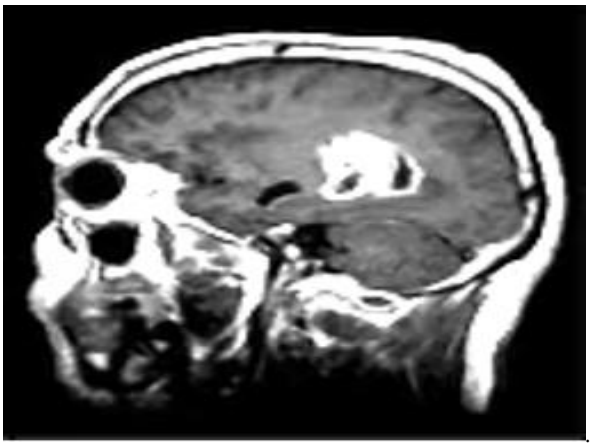

Fig. 10. Restored Output Image

4. Results and Discussion

The proposed methodology performance is calculated using 100MRI cover images (255x255 size of gray level image). In the experiments, stego images are produced using the DWT and ElGamal encryption technique with various levels of embedding rates starting from 5% to 40%. The technique has been established using MATLAB software tool, wherever a well-promoted script file has been implemented to feed the information. The information can be the medical image incorporated with the patient information. The implemented script will let the user to choose the input file, and user defined keys to implement the ElGamal encryption of secret data at the transmitting end and embed the encrypted data in to cover image. Further at the receiver end, the encryption key is required in order to perform extraction of embedded data. Moreover, Inverse DWT and ElGamal decryption methods are used to disintegrate the stego image and recover the secret information from the image.

4.1 Performance analysis

Image quality will be measured using some parameters like PSNR, Weighted PSNR (*w*PSNR), Correlation coefficient (CoC), Structural Similarity (SSIM) and average difference. It also finds the embedding efficiency of the stego image.

1) Mean Square Error (MSE)

MSE is calculated by averaging the squared intensity of the plain (input) image and the resultant (output) image [28] pixels as given by an Eq. (2)

$$MSE = \frac{1}{4MN}\sum_{i=1}^{2M}\sum_{j=1}^{2N}(C_{ij} - S_{ij})^2 \quad (2)$$

where cij and sij denotes the cover and stego pixel values, respectively.

2) Peak Signal-to-Noise Ratio (PSNR)

PSNR is a mathematical measure of image quality based on the pixel variation between the input and output image [28]. The SNR measure is an estimate of quality of reconstructed image compared with input image. PSNR is defined by an Eq. (3)

$$PSNR = 10\,log_{10}\left(\frac{255^2}{MSE}\right) \quad (3)$$

The PSNR is essentially the SNR when all picture element values are equal to the maximum possible value.

3) Embedding capacity

To calculate the performance of the proposed scheme, the length of the key message (capacity of data) is employed in concert of the analysis criteria, that is outlined because the quantity of bits which will be embedded into the cover image. The embedding capacity is given by an Eq. (4)

$$E = \frac{K}{WH}(bpp) \quad (4)$$

where K is the range of information message bits, whereas W and H are the dimension and height of the cover image severally. (Both cover and stego pictures square measure of identical size with W = H = 255).

4) Weighted Peak Signal-to-Noise Ratio (wPSNR)

The *w*PSNR is roughly like PSNR for flat areas as a result of a additional parameter referred to as Noise Visibility Function (NVF) is near one in sleek regions. However, for regions with sharp contrasts, *w*PSNR will be higher than PSNR due to sharp contrast edge region. So the result of NVF is close to zero for advanced regions.

The *w*PSNR is given by an Eq. (5)

$$WPSNR = 10\,\boldsymbol{log}_{10}\left(\frac{\boldsymbol{max}(C)\text{^}2}{||NVF(S-C)||\text{^}2}\right) \quad (5)$$

5) Average difference

The average difference may be an easy and popular image quality analysis criterion. It's computed by averaging absolutely the distinction between the cover and stego images, calculated by an Eq. (6)

$$AverageDifference = \frac{1}{\mathrm{WH}}\sum_{\mathrm{p,q}}(\mathrm{C[p,q]} - \mathrm{S[p,q]}) \quad (6)$$

6) Correlation Coefficient (CoC)

The correlation coefficient of original and encrypted image is analyzed by using two vertical and also horizontal adjacent pixels. The statistical measurement between any two variables which can define that how much they are interrelated to each other is known as correlation. Generally, to reduce the correlation between adjacent pixels a better encryption algorithm is required correlation between adjacent pixels is very high. Correlation co-efficient can be calculated by the following Eqs. (7-10) [29].

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i \quad (7)$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2 \quad (8)$$

$$\sum_{i=1}^{N}(u_i - E(u))(v_i - E(v) \quad (9)$$

$$R_{uv} = \frac{cov(u,v)}{\sqrt{D(u)}}\frac{1}{\sqrt{D(v)}} \quad (10)$$

7) Structural Similarity (SSIM)

The technique of computing the similarity between any two or more images is known as SSIM index. In other words, SSIM index is a method of calculating the quality of image based on the reference of an initial un-compressed image or distortion free image. It is intended to enhance the old techniques like PSNR and MSE, which are recognized to be unpredictable with human eyes sensitivity [30].

As compared to the other techniques which are mentioned previously like PSNR and MSE is that these techniques will estimate apparent errors. In other words it can be stated that SSIM index reflects image degradation as apparent changes in provided structural information. The information when pixel with the strong inter-dependency which is spatially close is known as Structural information. This information covers important data regarding the structure of the objects in the visual scene.

The SSIM index can be calculated on different pixels of an image.

Generally, measurement can be done by using windows of same size like N x N and general Eq. (11) can be given as:

$$SSIM(u,v) = \frac{(2\mu_u\mu_v+c_1)(2\sigma_{uv}+c_2)}{(\mu^2{}_u+\mu^2{}_v+c_1)(\sigma^2{}_u+\sigma^2{}_v+c_2)} \quad (11)$$

The stego images which are created using embedding rates from 5% to 40% using LSB-RSA, STC, Hamming method and DWT with ElGamal encryption techniques are shown in **Figure 11**. As a result it is observe that it is hard to find by the usual human eye to difference between the initial image and processed stego images.

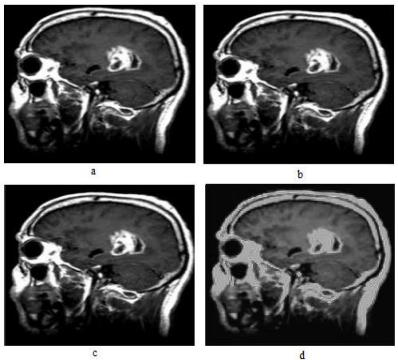

Fig. 11. Stego Images a) RSA method b) STC method and c) Hamming code method and d) DWT with ElGamal Encryption.

In LSB-RSA, tends to introduce the RSA encrypted secret knowledge in the medical image by using the smallest amount important bit and the stego image for RSA is shown in **Figure 11(a**). Canny edge detection technique used to find the sharpest regions in the input image for the embedding

method and data was only hiding in RONI image. The STC stego image and Hamming stego images are shown in **Figure 11(b) and 11(c).** The Stego image of DWT with ElGamal encryption techniques are shown in **Figure 11(d).**

The Histogram of the stego images (represented in Figure 12.) was quite similar to that of the cover images. According to the **Figure 12**, the histograms of the stego images are varying by increasing the embedding efficiency from 5% to 40% with different methods like RSA (**Figure 12(a)),** STC **(Figure. 12(b)**), Hamming code (**Figure 12(c)**), and DWT with ElGamal encryption (**Figure 12(d**)). The embedding rate increases, the embedding efficiency is more and high security of secret data.

It is necessary to say that for a 255 × 255 image, that consist of 65,025 pixels, for 40% embedding rate have (40/100) * 65,025 = 26,010 bits, which is proportionate to 3715 ASCII characters. For a 512 × 512 image, that consist of 2, 62,144 pixels, for 40% embedding rate have (40/100) * 2, 62,144 = 104,757 bits, which is proportionate to 14,979 ASCII characters.

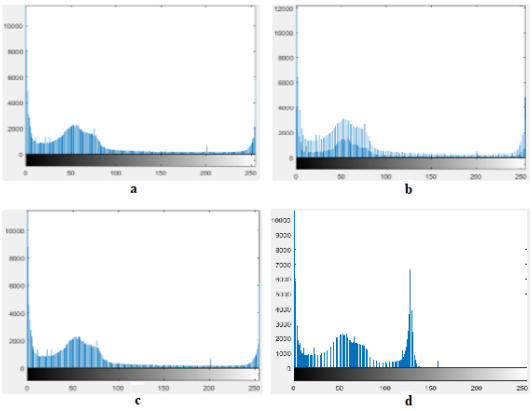

Fig. 12. Histogram of Stego Images a) RSA method b) STC method and c) Hamming code method and d) DWT with ElGamal Encryption.

Table 1 shows the visual quality performance results. It is evident that the proposed technique using DWT along with ElGamal encryption received the great image quality in all metric measurements as compared with different available methodologies, along with Hamming code, STC and RSA implementation. As stated before, our proposed method proved an excessive embedding capacity with an efficient visual quality with respect to PSNR and *w*PSNR.

But, as the ROI size become bigger, the RONI size will become smaller, and for this reason the wide variety of bits that can be embedded will become smaller. Suppose, if the data can be completely embedded using a bigger ROI, it is necessary to embed in the less sharp areas using the algorithm, which eventually affects PSNR, *w*PSNR and MSE.

Similarly, if the embedding rate increases the average difference will also will increases accordingly; however for our proposed technique the usage of DWT with ElGamal encryption along with 40% of embedding rate, 0.1179 average differences is obtained.Second best result is achieved by using Hamming code with 0.2458 average difference using 40% embedding rate. By analyzing the results, it is evident that difference among the cover and stego image developed using our proposed technique is usually small.

A graphical illustration of the PSNR values is shown in Figure 13. The performance of our proposed technique using DWT with ElGamal encryption, compared to the other techniques like Hamming code, STC and RSA, with PSNR values greater than 50 dB, which suggests the hidden data is invisible in step with the human visual perception. From the graph the PSNR values are decreasing when increasing the embedding rate from 5% to 40%.

Table 1. Comparison of the results of proposed method (DWT- ElGamal), STC, Hamming code and RSA

Method	Embedding rate	5%	10%	20%	25%	30%	40%
DWT- ElGamal	***MSE***	0.0023	0.0159	0.0538	0.0746	0.0979	0.1414
	PSNR	74.4772	66.1211	60.8268	59.4054	58.2216	56.6249
	wPSNR	69.3436	61.7243	56.9664	55.9224	54.7592	54.1216
	Average Difference	0.0022	0.0098	0.0419	0.0611	0.0831	0.1179
STC	***MSE***	0.0223	0.059	0.1392	0.1826	0.2218	0.2924
	PSNR	64.6402	60.4241	56.6952	55.5147	54.6721	53.4705
	wPSNR	61.9947	59.598	56.5877	54.1509	53.2097	52.3119
	Average Difference	0.0085	0.0343	0.0938	0.123	0.1497	0.2047
Hamming Code	***MSE***	0.0223	0.0599	0.1443	0.1895	0.2259	0.2974
	PSNR	64.6432	60.3583	56.5381	55.3554	54.5924	53.397
	wPSNR	60.9789	59.598	55.7524	53.6548	53.4906	51.6429
	Average Difference	0.0148	0.0461	0.1192	0.1552	0.1886	0.2458
RSA	***MSE***	0.049	0.0889	0.1495	0.1817	0.2164	0.3105
	PSNR	61.2319	58.6412	56.3833	55.5376	54.7776	53.2104
	wPSNR	61.9947	56.8592	53.1391	53.415	52.1345	50.9624
	Average Difference	0.0406	0.0733	0.1223	0.1482	0.1689	0.3128

The ElGamal with DWT method will produce the higher PSNR values because the ElGamal encryption method implemented over a simple root of a large prime number in encrypting and decrypting gray and color medical images when compared to Hamming code, STC and RSA.

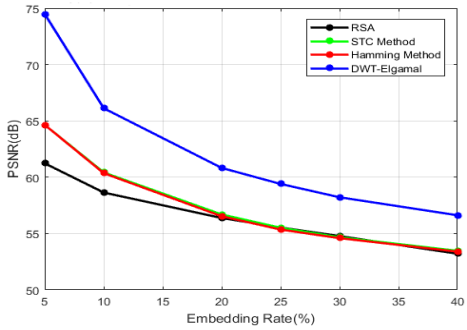

Fig. 13. Performance analyses of PSNR values for different embedding rates.

The performance analysis of the wPSNR values is shown in Figure 14.

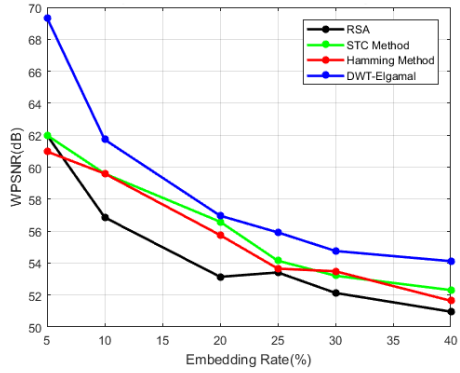

Fig. 14. Performance analysis of *w*PSNR values for embedding rates.

The performance of our proposed technique using DWT with ElGamal encryption, compared with the other methods like Hamming code, STC and RSA, with *w*PSNR values greater than 55dB, which suggests the hidden data is invisible in step with the human visual perception. From the Figure, *w*PSNR values are decreasing when increasing the embedding rate from 5% to 40%. In the diagram *w*PSNR values are decreasing when increasing the embedding rate from 5% to 40%. According to this, the DWT with ElGamal encryption is produce the higher *w*PSNR values when compared to Hamming code, STC and RSA.

Figure 15 shows the performance of Correlation Coefficient (CoC) and SSIM index using DWT with ElGamal encryption system. It is concluded that the performance of CoC and SSIM has been increased with DWT with ElGamal encryption.

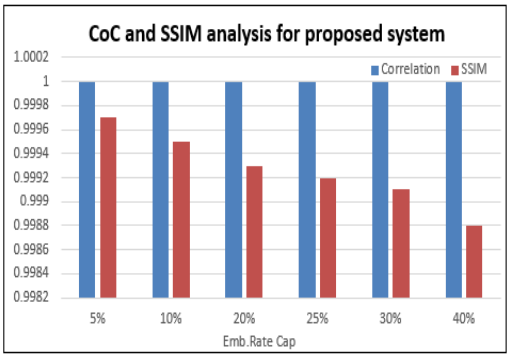

Fig. 15. Performance analysis for CoC and SSIM values for different embedding rates

5. Conclusions

In this paper a completely unique and efficient steganography method for biomedical image steganography has been proposed which can be effectively used in telemedicine applications. At the same time considering scientific image characteristics and associated crucial data, DWT with ElGamal encryption based data embedding technique has been developed. The patient's secret data were embedded into the communication medium (image). As compared to WT approach the efficiency of DWT to cope with singularity issues and image decomposition will increase the efficiency of the proposed technique. The secret information has been encrypted into medical image in the RONI by implemented using DWT with ElGamal encryption technique. Also, it is focused much on encrypting information into the corners of RONI, as it could create less attention for third party about the presence of secret information in the carrier image. However, the ElGamal cryptosystem technique is more invulnerable against attacks than existing encryption technique, which will eventually increase the efficiency using ElGamal encryption and DWT. This paper implements dual model security feature by applying DWT enhanced steganography and ElGamal encryption based secret data encryption which is a combined model which will exhibited better PSNR, embedding capacity, imperceptibility and attack resiliency when compared to other methods and also it provides a good and efficient quality of the stego images. The obtained results from DWT with ElGamal encryption were compared with Hamming code technique, STC algorithm and RSA algorithm.

References

[1] T.Moerland. Steganography and Steganalysis. [Online]. Available: www.liacs.nl/home/tmoerl/privtech.pdf.

[2] M. Mohan and P. R. Anurenjan, "A Novel Data Hiding Method in Image using Contourlet Transform," Recent Advances in Intelligent Computational Systems (RAICS), 2011.

[3] A. Cheddad, J. Condell, K. Curran, and P. Kevitt, "Digital image steganography – survey and analysis of current methods", J. Signal Processing, Vol. 90, No. 3, 2010, pp.752–825.

[4] R. Gonzalez, and R. Woods, "Digital Image Processing," 2nd ed., Prentice Hall, PHI. 2001.

[5] W. Chen, "A comparative study of information hiding schemes using amplitude, frequency and phase embedding," PhD thesis, National Cheng Kung University, Taiwan, May 2003.

[6] C. K. Chan and L. M. Chang, "Hiding data in images by simple LSB substitution," Pattern Recognition, Mar. 2004, pp. 469-474.

[7] J. Xu, L. Yang, and D. Wu, "Ripplet: a new transform for image processing," J. Vis. Commun. Image R, Vol. 21, No. 1, 2010, pp.627–639.

[8] 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.

[9] S. Lavania, P. S. Matey and V. Thanikaiselvan, "Real-time implementation of steganography in medical images using integer wavelet transform," IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-5.

[10] G. Prabakaran, R. Bhavani and P. S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme," International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, 2013, pp. 1188-1193.

[11] J. M. Barton, "Method and Apparatus for Embedding Authentication Information within Digital Data," U.S. Patent 5646997, 1997.

[12] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Reversible data hiding," in Proc. Int. Conf. Image Processing, vol. II, Sept. 2002, pp 157-160.

[13] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug. 2003.

[14] Singh, A.K., Dave, M. and Mohan, A., 2014. Wavelet based image watermarking: futuristic concepts in information security. Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, 84(3), pp.345-359.

[15] Zhang, L. and Zhou, P.P., 2010. Localized affine transform resistant watermarking in region-of-interest. Telecommunication Systems, 44(3-4), pp.205-220.

[16] Rathi, Sonika C., and Vandana S. Inamdar. "Analysis of watermarking techniques for medical images preserving ROI." In Computer Science & Information Technology (CS & IT 05)-open access-Computer Science Conference Proceedings (CSCP), pp. 297-308. 2012.

[17] Jigar Makwana, Dual Steganography, A New Hiding Technique for Digital Communication, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 5 (4), 2016.

[18] J. W. Tukey, (1974). Nonlinear (Nonsuperposable) Methods for Smoothing Data. Conference Record EASCON, p. 673.

[19] Shilpy Mukherjee and Mahajan AR, A Novel Approach for Reversible Data Hiding, International Journal of Advance Research in Computer Science and Management Studies, 2 (5), 2014.

[20] Nikita Kashyap, G. R. SINHA, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", International Journal of Modern Education and Computer Science, 2012, volume 3, pages(50-56).

[21] Y. Licai, L. Xin, and Y. Yucui. Medical image fusion based on wavelet packet transform and self-adaptive operator. In Proceedings of International Conference on Bioinformatics and Biomedical Engineering, pages 2647–2650, 2008.

[22] Gunjal, B.L. and Mali, S.N., 2012. ROI based embedded watermarking of medical images for secured communication in telemedicine. Int. J. Comput. Commun. Eng, 6(48), pp.293-298.

[23] C. Dhaarani, D. Venugopal and A. S. Raja, "Medical Image Compression Using Ripplet Transform," International Conference on Intelligent Computing Applications, Coimbatore, 2014, pp. 233-238.

[24] S. Das and M. K. Kundu, "Ripplet based multimodality Medical Image Fusion using Pulse-Coupled Neural Network and Modified Spatial Frequency," International Conference on Recent Trends in Information Systems, Kolkata, 2011, pp. 229-234.

[25] Hashim, H. R., "H-Rabin Cryptosystem". Journal of Mathematics and Statistics, 2014 10 (3):258-262, 2014 ISSN: 1549-3644.

[26] Abuhaiba I. S. and Hassan M. A. "Image Encryption Using Differential Evolution Approach In Frequency Domain" Signal & Image Processing International Journal (SIPIJ) 2011, Vol.2, No.1.

[27] http://homepages.math.uic.edu/~leon/mcs425-s08/handouts/el-gamal.pdf.

[28] Ulutas, M., Ulutas, G. and Nabiyev, V.V., 2011. Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of Systems and Software, 84(3), pp.341-353.

[29] Vaishali S. Jabade,Dr. Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications (0975 – 8887), Volume 31– No.1, pp. 28-35, October 2011.

[30] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process, vol. 14, no. 2, pp. 253–266, Feb. 2005.