Steganography Technique Based on WPT and ElGamal Encryption with Confusion for Robust Medical Image

Sivakumar Karuppan, Revathy Ondimuthu, N S Nithya

Abstract*—For delivering effective health medical images and Electronic Patient Record (EPR) play an important role and these are stored in cloud, remote medical care and tele medicine service. For health care system, all the medical image data are stored in third party a server that is cloud. So, there is more chance to process or change the medical images as well as patient's records which leads to health-related issues. To prevent the medical details from the hackers, many techniques are proposed and analyzed by the researchers. Anyway, data corruption is done by the attackers till now. In order to improve the security for data, this paper proposes a steganography technique which embed the important details into the medical image by using Wavelet Packet Transform (WPT) without affecting Region of Interest (ROI) which is useful for further diagnosis. Before embedding the patient's record, these data are encrypted by using ElGamal Encryption technique which provides more security to the data. It is observed from the simulation results that the proposed technique produces better performance in terms of MSE, PSNR and WPSNR values. The PSNR value of the proposed system can increase 8.8%, 6.2%, 12.5%, 9.6%, 6.7% and 6.9% for embedding rate 5%, 10%, 20%, 25%, 30% and 40% respectively from the existing (DWT-ElGamal) technique.

Key Words -- Wavelet Packet Transform (WPT), Mean Square Error (MSE), Weighted Peak Signal to Noise Ratio (WPSNR), Electronic Patient Record (EPR), Region of Non-Interest (RONI), Region of Interest (ROI).

I. INTRODUCTION

Nowadays, transmitting information from one place to another through the channel is very essential for many fields such as industries, medical fields, government sectors and etc. This communication must be a secured and it can understand only by the receiver not by the hackers.

Medical providers and insurance companies implement the policies and procedures for protecting medical information of patients which is required by Health Insurance Portability and Accountability Act (HIPAA) [1]. The major part of diagnostic procedure is done with the help of medical images obtained from x-rays, CT scan, ultra sound and etc. [2]. The medical image can be stored, exchange and send medical images by using Digital Imaging and Communication in Medicine (DICOM) standard. This standard contains protocols for the imaging methods such as Magnetic Resonance Imaging (MRI), Radiation therapy, Computed Tomography (CT), radiography and etc. Another medical imaging technology named as Picture Achieving and Communication System (PACS) which provides the storage and access of medical image very easily [4]. When the technology grows up this PACS can be migrated to Cloud. Cloud storage can be implemented in various fields where the image or data are remotely managed, backup and maintained. This gives many advantages such as high speed, reduced cost, data recovery and etc. But it has some disadvantages mainly when storing the valuable and important data remotely in cloud is that the security or privacy related issues. This is because the images are given to the third-party cloud service providers. Also, the internet is not fully secured. Hence, there are more possibilities to hack the medical information of individual patients. To avoid this situation Steganography is used. This method can be used for many applications such as Personal Communication and store data secretly, gives protection against alteration of information, Access control system for digital content distribution, Media Database Systems and etc. The information can be secured by various techniques such as watermarking, cryptosystems or cryptography and steganography. Watermarking is a technique used to embed the secret information in a particular position of an image, audio or video. The location in which the information embedded is only known by the receiver and sender. So, the intruder can see the cover image, audio or video and not the secret text. Cryptography is used to encrypt the secret information and convert into another format using the cryptographic key. This encrypted information can be decrypted by the receiver who knows the correct cryptographic key. Steganography is similar to watermarking technique but it changes the image property. Among these techniques, steganography is the one which secured the data more efficiently [3]. This method can change the image property by inserting the required information into a cover image so that only the transmitter and the receiver can detect the information. When compared to watermarking technique, steganography method provides more security in communication network. In this paper, the steganography method is used to hide the personal information of individual patients in their medical image.

Revised Version Manuscript Received on 10 September, 2019.

SivakumarKaruppan, Assistant Professor , Department of CSE, JCT College of Engineering and Technology, Coimbatore, Tamil Nadu, India

RevathyOndimuthu, Assistant Professor, Department of ECE, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India.

Dr N S Nithya, Associate Professor, Department of CSE, KSR College of Engineering ,Tiruchengode, Tamil Nadu, India.

II. RELATED WORKS

A popular standard known as DICOM used for storing, maintaining and transmitting the medical image. In this standard there is no method are present for preserving the sensitive data that are used for further diagnosis for individual patients. To preserve the data, three methods are proposed in [5]. They are Division into blocks, Least Significant Bit Insertion (LSB), Mean Change Modified Method (MCMM). Among these three methods, integrating DICOM with MCMM is the more effective method to hide the information within the pixel of an image without any degradation of the medical image. For authentication, the key can be shared between sender and receiver. This adds more security to the medical image. Same way, to improve the security three different steganography method is proposed in [6]. First Least Significant Bit algorithm which is used to divide the 24-bit image into triplet (RGB) model and the last bit of the image is changed for hiding the required secret information. Next, segment into blocks which divides the image into several blocks and finally mean change modified method. This method increases the security and reduces block effect. This combined method prevents the stego images from various attacks during the transmission of medical image. For improving security paper [7] presented the methods named as Steganography which is for hiding the required information to the image pixels. The hided information can be extracted by using conventional template matching. The steganographical method proposed in [7], the required data can be embedded into the mean value of number of pixel. In this method, many modifications in image pixel produces degradation in image so number of modification can be limited by mean modification algorithm.

One of the information hiding methodology is present in [8] for protecting the data of patients in medical image is RSA encryption algorithm and hiding technique based on Discrete Cosine Transform (DCT). This method used to hide the information of patients in a medical image except Region of Interest (ROI) and this image has to be transferred through electronically that is mail, fax and etc. RSA encryption algorithm is used in this system because of its simplicity but it has some drawbacks that is, it takes more time to run the algorithm and some large amount of data cannot be handled by this RSA encryption algorithm. This degrades the performance of the system. For noiseless and secure transmission of medical image a new method is presented in [9] which combine cryptography, hiding information techniques and steganography methods. The original image is encrypted using encryption algorithm then the information of patients is embedding in their medical image. This method produces less security and more noise. To achieve higher security and less noise another technique is added which is known as steganography. From the receiver side, the inverse and reverse transforms and techniques applied to extract the embedded secret information from the medical image.

Another steganography method that hide the patient's information inside the digital medical image by the use of dynamic key that can be generated by graph three coloring problem which can be presented in [10]. This method first to segment the given the image into ROI and RONI parts. The hash value and graph of medical image can be obtained by the pixels in the ROI image. ROI is different for each medical image so different graphs are obtained and distinguish one image from other. Three colored graphs can be solved by obtaining the system by using dynamic key, tough key and unpredictable key. This system is not tested with human observers during the experiments. To further improve security in digital medical image, a new steganography method is proposed in [11] with high imperceptibility. Using edge detection, the secret information is embedded in sharp region of image. Also, hamming code is used to embed 3 secret data bits into 4 bit cover image which enhance the quality of the image after reconstruction.

The hybrid method is proposed in [12] which combine cryptography and steganography to enhance the security of medical image. In this paper, the embedding process is based on DCT with Singular Value Decomposition (SVD). The information is encrypted by using the cryptography and this will insert the singular value of DCT coefficient to produce stego image. This method gives more imperceptibility of the stego image. More effective method, to increase security for digital medical images in e-health services, a steganography method is proposed in [13] which combine the integer Wavelet Transform and Edge Detection technique. In this paper [13], Otsu's method is used for divide the original image into two parts that is Region of Interest (ROI) and Region of Non-Interest (RONI). ROI part having the image required for diagnosis. So, RONI part is used for embedding the secret information of patients so that the image as well as the information are secured and does not know by the hackers. The RONI part is transformed by using wavelet transform and the Electronic Patient Record (EPR) (secret information) is embedded in the higher frequency region of RONI region and to detect the edge of image, edge detection is used. This improves the security but the quality of an image is reduced because wavelet transform used in this method concentrate only on higher frequency region.

III. PROPOSED METHOD

All the medical images and patient's records are kept in cloud storage. These are remotely accessed whenever and/or wherever it needed. But the security of these images and records are less because these are stored in the third party servers. To enhance the security by embedding secrete information into the medical image without disturbing Region of Interest (ROI) (region that can be used for further diagnosis). This paper proposes a method Steganography with Wavelet Packet Transform (WPT) techniques. Fig. 1 shows the proposed Steganography system with WPT and edge detection technique. In this system, Canny Edge Detection technique is used because compared to other techniques canny edge detection technique provides better performance.

Initially, the medical image is taken as input and it is given to the adaptive median filter. This filter is used for removing the noise present in the input image and after removal of noise the image can be divided as ROI and RONI. The region having important information for further diagnosis is taken as ROI and the region except ROI is taken as RONI. It is

necessary for embedding the patient's records in a RONI region. So that it cannot affect the ROI region. The edges of RONI region is detected by using Canny Edge Detection Technique which extract the important structural information. If the edges of ROI and RONI are matched then WPT transform is applied for the RONI region. It divides the RONI part and finds the energy of each sub band. The sub band having minimum energy is the sub band where the records can be embedded. The secret information that is the patient's records are encrypted first in such a way that the intruders cannot attack or change the important data present in the records. ElGamal encryption technique is used to encrypt the record data using a key. Then these encrypted data can be sent to the confusion block which adds more security to the record data against intruder attacks. Then embed the encrypted record data to the RONI region where the sub band having minimum energy. After embedding, stego RONI image is obtained and then this image is combined with ROI region. This image is given to IWPT in which the reverse process of WPT is done and finally stego image is obtained.

A. Image Acquisition

Image Acquisition is purely based on hardware dependent process in which the image can be obtained by the reflection of light energy from the object. In every vision system, image acquisition is an initial step which is used to capture the image from the source like camera. Different kinds of sources (camera) can be used for different applications [14]. The main goal of Image Acquisition is to convert the optical image into the array of numerical data which can be modified on computer based on the application. Image Acquisition consists of three steps. They are:

1) The energy can be focused by optical system
2) Energy can be reflected from object of interest
3) The amount of energy can be measured by using a sensor

The camera initially needs some amount of energy for capturing the image. The energy is light or electromagnetic waves. This can capture the image and stored in memory for further processing. Fig. 2 shows that the input medical images from this the secret data can be embedded.

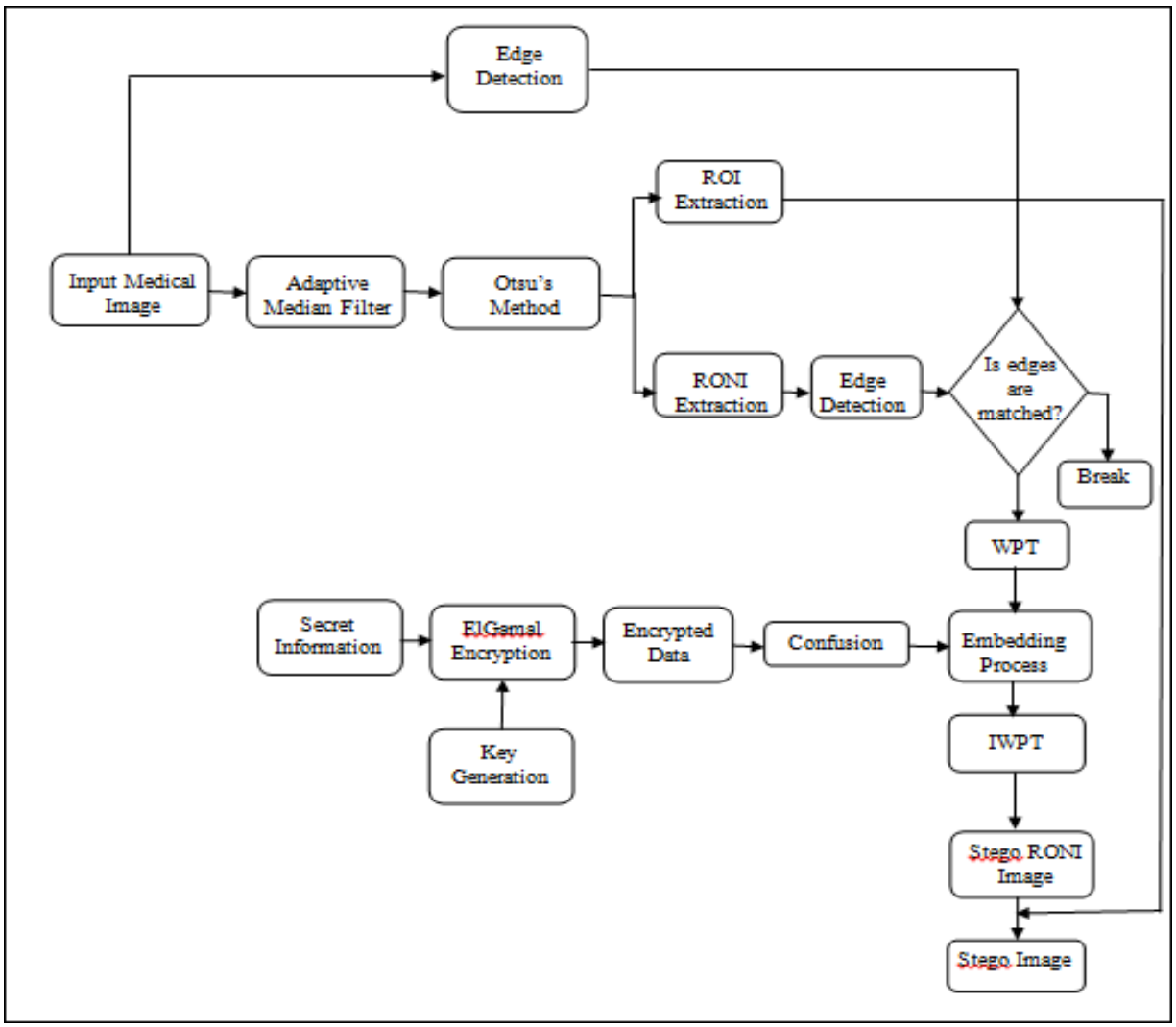

Fig. 1: Flow diagram of embedding process with WPT

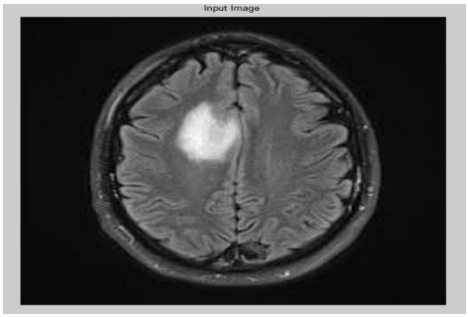

Fig. 2: Input Image

B. Adaptive Median Filter

Median Filter is normally used for minimizing the noise from the image and protects the useful information of an image. This is the smoothing filter which smoothen the data while preserving the sharp and small details of an image. Median filter can remove different kinds of noise effectively. At the same time, it does not differentiate the required details as well as the noise when the required details having the size which is relatively small compared to the neighborhood pixels size. So, this median filter removes the fine details of an image with noise. To avoid this, adaptive median filter is used in many fields. The spatial processing can be performed by Adaptive Median filter and it is used for determining which image pixel is affected by impulse noise. This filter can classify the noise and the required details by comparing every pixel with the neighboring pixels. The major application of Adaptive Median Filter is:

1) Impulse noise can be removed
2) Noises except impulse noise can be smoothing
3) Distortions of an image can be reduced

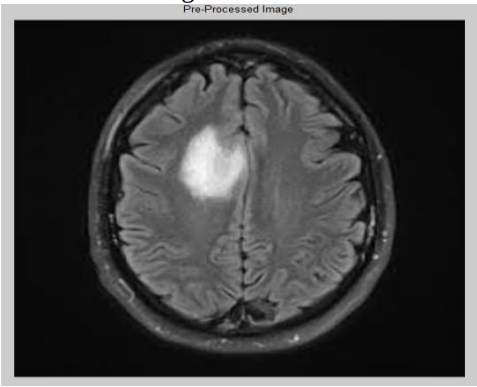

Fig. 3: Pre-Processed Image

Fig. 3 shows that the input medical image with the elimination of noise. The noise can be removed from input image by adaptive median filter.

Algorithm for Adaptive Median Filter

The operation performance and comparison can be done based on the algorithm that is given below:

Stage 1:

$A_1 = Z_{med} - Z_{min}$
$A_2 = Z_{med} - Z_{max}$
If $A_1 > 0$ and $A_2 < 0$,
Then go to Stage 2.
Else window size increased.
If window size $< S_{max}$, Repeat Stage 1.
else Z_{xy} is the output.

Stage 2:

$B_1 = Z_{xy} - Z_{min}$
$B_2 = Z_{xy} - Z_{max}$
If $B_1 > 0$ and $B_2 < 0$,
then Z_{xy} is the output.
else Z_{med} is the output.

Where,
Z_{min} = Minimum gray level value in S_{xy}
Z_{max} = Maximum gray level value in S_{xy}
Z_{med} = Median gray level in S_{xy}
Z_{xy} = Gray level at (x, y)
S_{max} = Maximum allowed size of S_{xy}
and S_{xy} is the size of neighborhood that can be changed by adaptive median filter during the operation.

C. Otsu's Method

Otsu's method is a global thresholding method which separates the given input image into two parts named as ROI and RONI based on the threshold value which is automatically generated by this method [13]. Thresholding is used to extract the required image from its background based on the intensity value (threshold) of an image. This threshold can divide the input image into two parts. One part having the intensity value which is below the assigned threshold value.Another part having the value which is equal or greater than the assigned threshold value.Thresholding convert the gray image into binary image. If the pixel value greater than the threshold value then these are belonging to ROI region and the pixel less than the threshold value are belongs to RONI region. Fig. 4 shows that the ROI and RONI region separately. So that the secret information can be embedded in RONI region of medical image.

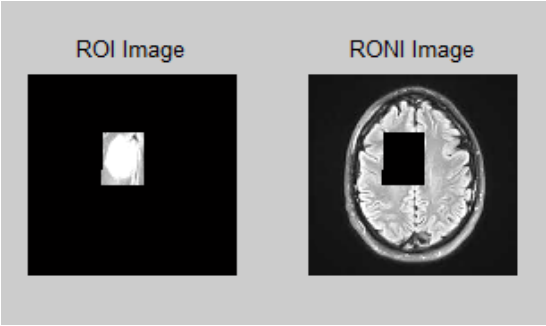

Fig. 4: Segmentation of ROI and RONI region

D. Edge Detection Technique

The basic tool for image segmentation is edge detection. Edge detection technique is the process of identifying and locating sharp discontinuities in an image. These discontinuities are abrupt changes in pixel intensity which characterize boundaries of regions in an image [15]. Many edge detection techniques are used to separate the regions sharply. Among these techniques, the performance of Canny edge detection technique is better which is analyzed in [16]. All the edge detection methods are used to detect the pixels in an image at which the brightness of an image changes to a considerable rate and separate ROI from RONI. Fig. 5 shows that the output image obtained after the canny edge detection method.

E. Canny Edge Detection

Canny Edge detector is one of the edge detection operators which use the algorithm with many stages for detecting the edges present in the input image. It is used to extract the important structural information of an image from various vision objects. In order to detect the edges in image canny edge detection method follows certain algorithm steps [18]. They are as follows:

Step 1: Initially, the noise in the original image can be removed and the sensitive to noise is reduced when the width of Gaussian mask is large.

Step 2: Once the noise in an image is removed then take the gradient of image for finding the strength of an edge.

Step 3: Determine the edge direction by using the following formula,

$$\theta = tan^{-1}\left(\frac{G_y}{G_x}\right)\ldots \quad (1)$$

Where,

G_y is the gradient in y-direction

G_x is the gradient in x- direction

Step 4: The edge of an image can be traced by using the edge direction obtained by equation (1).

Step 5: After finding the edge direction, apply non-maximum suppression. This non-maximum suppression is used to suppress the pixel value that is not considered for the edge of an image.

Step 6: To eliminate the lines appeared in various colors present the surrounding of an edge; hysteresis [17] method is used.

Fig. 5: Canny Edge Detection

F. Wavelet Packet Transform (WPT)

The wavelet functions are linearly combined and formed wavelet packets. WPT is the extension of Wavelet Transform (WT). In WT, the filtering process is applied only at the low frequency range. So, the high frequency range is not considered for processing [19]. The WPT transform is otherwise called as Wavelet Packet Decomposition (WPD). $\Psi^x_{y,z}(t)$ is the wavelet packet and x, y and z are the indices in which x indicates modulation, y indicates scale and z indicates translation parameters. The wavelet packet is defined in [20],

$$\Psi^x_{y,z} = 2^{y/2}\Psi^y(2^j t - z)\ \ldots \quad (2)$$

In this paper, the WPT transform is used to split both high and low frequency sub bands for RONI region. After dividing the sub band, the required medical information can be stored anyone of the sub band which may be low frequency or high frequency. The secret medical information can be embedded in one of such sub band having minimum energy value. The energy value of each sub bands are calculated by using the following formula,

$$E_{min} = \left[\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x(i,j)\right)^2\right]\ldots \quad (3)$$

The sub band decomposition provides high robustness and imperceptibility of this system [20].

G. Encryption Techniques

Encryption is the process of changing ordinary text or image into another format which cannot be understood by the one who wants to corrupt or change the particular information. An algorithm is used to generate the key. Using that key the ordinary original text can be encrypted. This key only known by the sender and the receiver not by the intruders.So that the required information stored safely. Many encryption techniques are used to save the information from the intruders. In this paper, ElGamal Encryption technique is used to encrypt the information and provide secure transmission. Bb

H. ElGamal Encryption Technique

ElGamal Encryption technique is an asymmetric key encryption algorithm. This algorithm based on Diffie-Hellman key exchange (DH). DH is the method or process of changing the required data secretly with a cryptographic key over a public channel. This technique comprises of three components. They are: key generation, encryption and decryption algorithm.

Key Generation:

The key can be generated by the following algorithm:

Step 1: Create the description having cyclic group G of order q with the generator g.

Step 2: From the set {1, …… , q-1}, choose x randomly.

Step 3: Compute the value $h := g^x$

Step 4: Publish h then assigning G, q, and g as a public key and x as private key.

ElGamal Encryption:

The ElGamal encryption can be done by using the following algorithm:

Step 1: Choose y from set {1, …… , q-1} and find $c_1 := g^y$

Step 2: Find shared secret $s := h^y := g^{xy}$

Step 3: Mapping the secret data m on m′ of G

Step 4: Find $c_2 := m'$s

Step 5: Finally, the encrypted text is obtained.

$(c_1, c_2) = (g^y, m'.h^y) = (g^y, m'.g^{xy})$

ElGamal Decryption

The encrypted records can be decrypted with the private key x and the flow of algorithm is given below:

Step 1: Find the shared secret $s := c_1^x$

Step 2: Calculate $m' := c_2 s^{-1}$

This decryption algorithm produces the original information,

$$c_2\, s^{-1} = m' h^y (g^{xy})^{-1}$$
$$= m' g^{xy} g^{-xy}$$
$$c_2\, s^{-1} = m'$$

I. Confusion and Diffusion

The properties to make a secure encryption are termed as confusion and diffusion. These are used to prevent encryption key from its deduction and the original information are also prevented. Confusion is a technique in which the encrypted information provides no clue about the original information. In this technique the encrypted information and the encryption key is maintained as complex as possible. The confusion can be obtained by using substitution and complex scrambling algorithm that relies on key and the original information. Diffusion is a cryptographic technique used to enhance the redundancy of the original information. In the diffusion the statistical structure of the original information can vanish into long range statistics of the encrypted information and the relationship between them is complex so that the intruders cannot find the original key. Diffusion can be obtained by using transposition techniques.

Fig. 6 shows that the output of the medical image having the information of EPR details using ElGamal encryption technique and confusion technique.

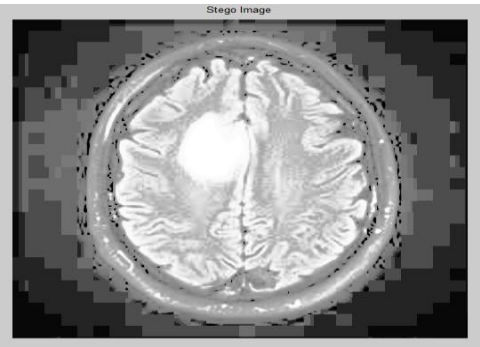

Fig. 6: Stego Image

Extraction process is exactly reverse of embedding process. Fig. 8 shows that the extraction of secret records and the medical image. Stego image is the input image of extraction process which is embedded with patients' records. Otsu's method is used to extract the ROI and stego RONI image. Then the extraction process is done through IWPT. This extraction block extracts the stego RONI image into encrypted data and RONI image. Then combine RONI image and ROI image which produce the medical output image. The encrypted data is decrypted using ElGamal decryption and this produce the secret information. Fig. 7 shows that the restored output image after extraction of secret EPR details from the medical image.

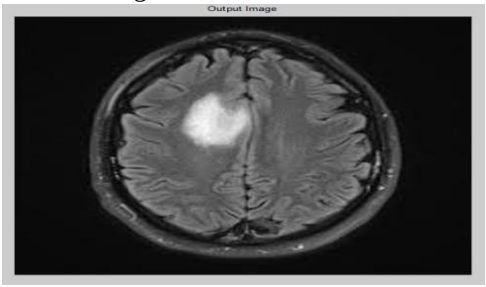

Fig. 7: Restored Output Image

J. Extraction Process

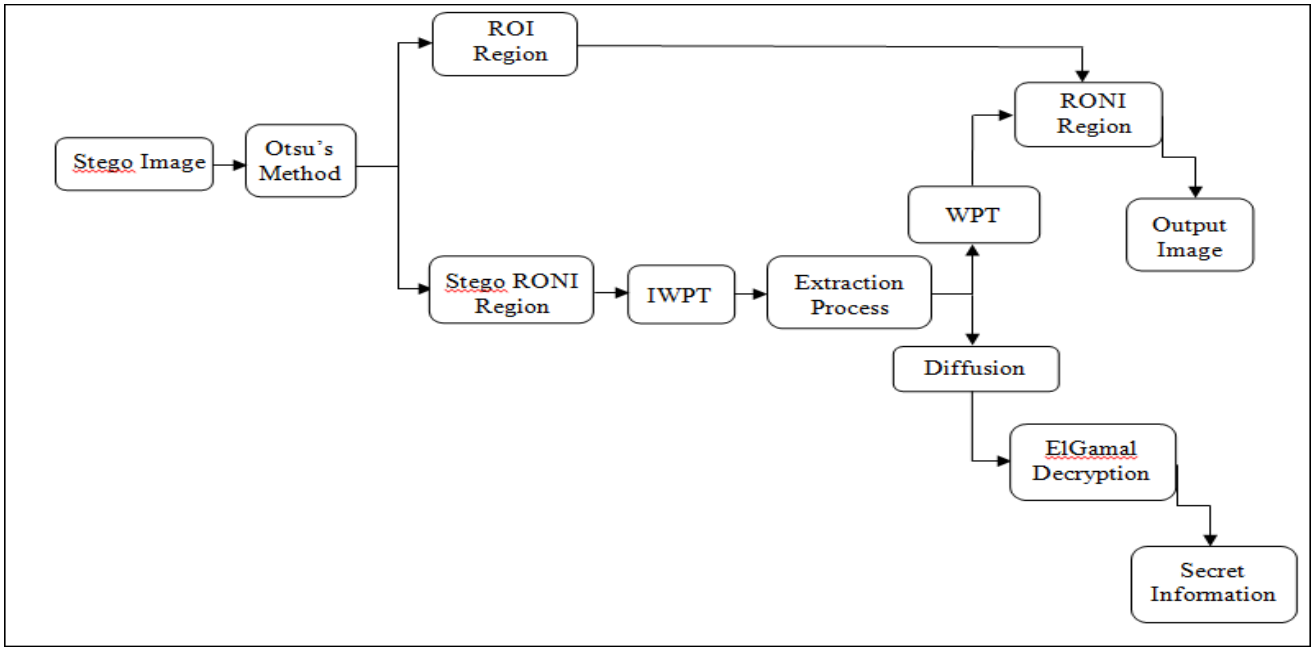

Fig. 8: Flow diagram of extraction process with WPT

IV.SIMULATION RESULTS

The proposed methodology can be analyzed and the parameter Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Weighted PSNR (WPSNR) and Average Difference are calculated and compared with the existing system.

Mean Square Error (MSE)

MSE is a measure of quality of an estimator. MSE measures the average of squares of error. That is the average squared difference between the estimated value and predicted value. The MSE value should be positive (Non-negative).It is the mean of squared error.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - \hat{X}_i\right)^2 \ldots \quad (4)$$

Where, X_i is the estimated value

$\hat{X}_i$ is the predicted value

n is the number of prediction created from n data points

Peak Signal to Noise Ratio (PSNR)

Usually, PSNR can be represented in logarithmic decibel. PSNR can be defined through MSE value. The formula for PSNR is written as,

$$PSNR = 10\ log_{10}\left(\frac{Max^2}{MSE}\right) \ldots \quad (5)$$

$$PSNR = 20\ log_{10}(Max) - 10\ log_{10}(MSE) \ldots \quad (6)$$

Where,

Max denotes the maximum pixel value of an image.

Weighted Peak Signal to Noise Ratio (WPSNR)

WPSNR is similar to PSNR. Noise Visibility operate (NVF) is used for an additional parameter for flat surface.

$$WPSNR = 10\ log_{10}\left(\frac{Max^2}{\|NVF(S-C)\|^2}\right) \ldots \quad (7)$$

Coefficient of Correlation (CoC)

The linear relationship exists between the two measured image quantities for establishing the degree of probability is called Coefficient of Correlation (CoC). The Pearson's Correlation Coefficient is defined in [22] for a monochrome digital image is,

Correlation Coefficient

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sqrt{\sum_i (x_i - x_m)^2}\sqrt{\sum_i (y_i - y_m)^2}} \quad \ldots \quad (8)$$

Where,

x_i and y_i is the intensity value present in ith pixel of an input and output images respectively.

x_m and y_m is the mean intensity value of input and output image respectively.

If r=1, two images are identical.

If r=0, two images are uncorrelated.

If r=-1, two images are anti-correlated [23].

Structural Similarity Index Matrices (SSIM)

This measures the quality of the resultant image by comparing the original image. SSIM is fully depends on full reference image quality assessment method. SSIM is used to find the similarity between the resultant output image and the original input image. The main goal of image quality assessment is to quantify the strength of perceptual similarity between the output image and reference image. The similarity between the images is calculated by comparing three parameters present in the images. They are: luminance, contrast and structure. The luminance of image can be compared and the mean density is given by,

$$\mu_x = \hat{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \ldots \quad (9)$$

The luminance comparison function $l(x, y)$ is converted into $l(\mu_x, \mu_y)$.

For obtaining the contrast comparison, the mean intensity is removed from the image and it is given as,

$$\sigma_x = \left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu_x)^2\right)^{\frac{1}{2}} \ldots \quad (10)$$

The contrast comparison function $c(x, y)$ is converted into $c(\sigma_x, \sigma_y)$.

Finally, the structure can be estimated by using luminance and contrast and it is given by,

$$s(x, y) = s\left(\frac{x - \mu_x}{\sigma_x}, \frac{y - \mu_y}{\sigma_y}\right) \ldots \quad (11)$$

The SSIM can be derived from the above equations (9), (10) and (11),

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad \ldots \quad (12)$$

Where, C_1 and C_2 are constants.

Table 1: Comparison OfMse, Psnr, Wpsnr And Average Difference For Proposed System With Existing System

Method	Embedding rate	5%	10%	20%	25%	30%	40%
WPT-ElGamal& Confusion	MSE	0.0012	0.0034	0.00611	0.0291	0.0431	0.0675
	PSNR	81.0244	70.2416	68.4315	65.1354	62.1684	60.5738
	WPSNR	77. 0592	66.4215	60.2134	59.2467	56.8943	55.4973
	Average Difference	0.0014	0.0025	0.0022	0.0146	0.0168	0.0349
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

Table 1 shows that the comparison of different parameter performance such as MSE, PSNR, WPSNR and Average Difference of a proposed method with other existing system. The embedding rate is taken as 5%, 10%, 20%, 25%, 30% and 40%. Based on this comparison, it is shows that the proposed system produces reduced MSE value and increasing PSNR and WPSNR value. The output image quality is high when increasing the PSNR value. So, the proposed system produces the output image with better quality.

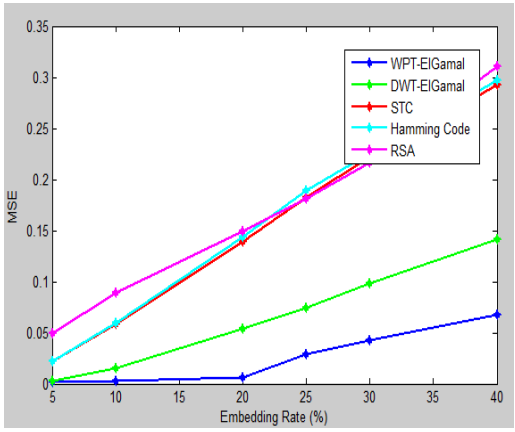

Fig. 9: MSE performance for different techniques

Fig. 9 shows the performance of MSE value for different techniques such as WPT-ElGamal, DWT-ElGamal, STC, Hamming Code and RSA. Among these methods the proposed method WPT-ElGamal produces better performance in terms of MSE value. The MSE value of proposed system can be reduced compared to the other existing techniques.

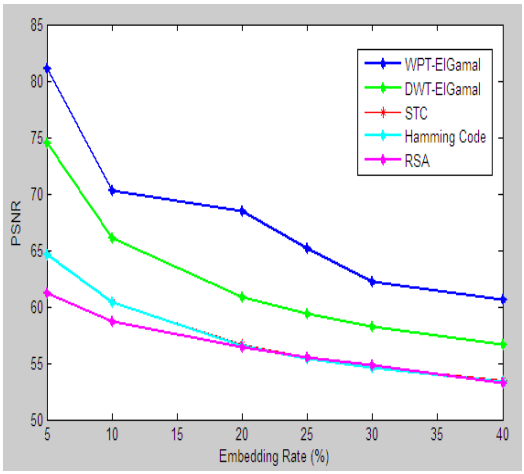

Fig. 10: PSNR performance of different techniques

Fig. 10 shows that the performance comparison of PSNR value with different techniques such as WPT-ElGamal, DWT-ElGamal, STC, Hamming Code and RSA. Compared to these existing techniques the proposed technique (WPT-ElGamal) produces high PSNR value. So that the quality of an output image is increased.

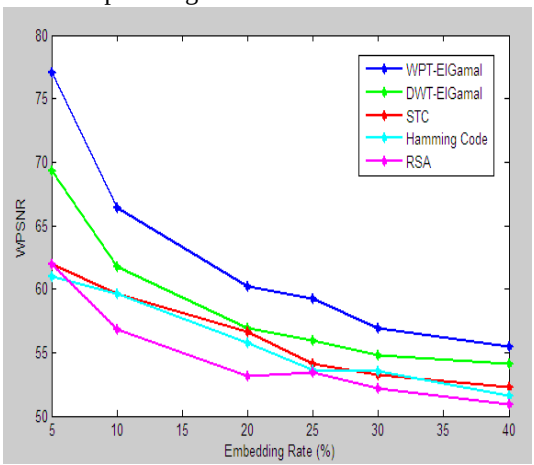

Fig. 11: WPSNR performance of different techniques

Fig. 11 shows that the performance comparison of Weighted PSNR value for various techniques such as WPT-ElGamal, DWT-ElGamal, STC, Hamming Code and RSA. WPSNR value further improved to a considerable rate by the proposed technique (WPT-ElGamal) compared to other existing techniques.

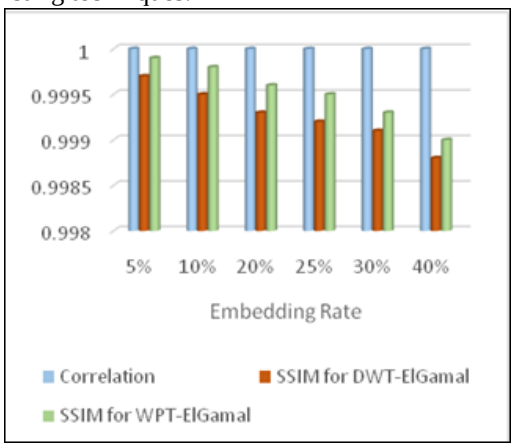

Fig. 12: Performance Comparison of SSIM

Fig. 12 shows that the comparison of SSIM for the proposed and existing (DWT-ElGamal) system for different embedding rate such as 5%, 10%, 20%, 25%, 30% and 40%. It shows that the similarity of the input and the output image has been improved compared to the previous techniques. So that based on this parameter, the quality of an image can be improved and the restored output is similar to the input image.

V.CONCLUSION

In order to improve the security related to medical images and EPR which is stored in the cloud, Steganographic method is used. In this the input image is divided as ROI and RONI regions. ROI region should not be disturbed because the information present in ROI is needed for further diagnosis. So, the RONI region is chosen for embedding the EPR data. Before embedding process, the medical images are segmented by using WPT and find the energy value for each sub band. The EPR data can be encrypted by ElGamal Encryption technique and this encrypted data is confused by confusion block. Then this encrypted data is embedded in RONI region's sub band where the energy value is minimum. This double protection provides more security to the medical image and EPR data. It is observed from the simulation results that the PSNR value of the proposed system can increase 8.8%, 6.2%, 12.5%, 9.6%, 6.7% and 6.9%for embedding rate 5%, 10%, 20%, 25%, 30% and 40% respectively from the existing (DWT-ElGamal) technique. The WPSNR value of WPT-ElGamal technique can improve the performance by 11.1%, 7.6%, 5.7%, 5.9%, 3.9% and 2.5% for embedding rate 5%, 10%, 20%, 25%, 30% and 40% respectively from the existing (DWT-ElGamal) technique.

REFERENCES

1. "Health Insurance Portability and Accountability Act (HIPAA) and Its Impact on IT Security", Regulatory Compliance Series 3 of 6, Apani Networks White Paper Compliance Series. http://www.apani.com, May 2005.
2. Quist AphetsiKester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo M. Eghan and NiiNarkuQuaynor, "A Cryptographic Technique for Security of Medical Images in Health Information systems", 2nd International Symposium on Computer Vision and the Internet: Signal Processing, Image Processing and Pattern Recognition (SIPR'15), Procedia Computer Science, vol. 58, 2015, pp. 538-543.
3. T. Moerland Steganography and Steganalysis [online]. Available: www.liacs.nl/home/tmoerl/privtech.pdf.
4. R. H. Choplin, J. M. Boehme and C. D. Maynard, "Picture Archiving and Communication Systems: An Overview", RadioGraphics, vol. 12, no. 1, Jan. 1992.
5. Rafael A. Sampaio and Marcel P. Jackowski, "Assessment of Steganographic Methods in Medical Imaging", pp. 1-5.
6. V. Mahalakshmi, S. Satheeshkumar and Dr. S. Sivakumar, "Performance of Stegnographic Methods in Medical Imaging", International Journal of Computational and Applied Mathenatics, vol. 12, no. 1, 2017.
7. PouriaMortazavian, Mohammad Jahangiri and EmadFatemizadeh, "A Low-Degradation Steganography Model For Data Hiding in Medical Images", Proceedings of the Fourth IASTED International Conference VISUALIZATION, IMAGING AND IMAGE PROCESSING, pp. 914-920, Jan. 2004.
8. Ming Yang, Monica Trifas and Lei Chen, "Secure Patient Information and Privacy in Medical Imaging", Journal of Systemics, Cybernetics and Informatics, vol. 8, no. 3, pp. 63-66, 2010.
9. VinayPandey and Manish Shrivastava, "Medical Image Protection using Steganography by Crypto Image as Cover Image", International Journal of Advanced Computer Research, vol. 2, no. 3, pp. 45-48, Sep. 2012.
10. P. Thiyagarajan and G. Aghila, "Reversible Dynamic Secure Steganography for Medical Image Using Graph Coloring", Health Policy and Technology, vol. 2, no. 3, pp. 151-161, Sep. 2013.
11. Hayat Al-Dmour and Ahmed Al-Ani, "Quality Optimized Medical Image Steganography Based on Edge Detection and Hamming Code", IEEE 12th International Symposium on Biomedical Imaging (ISBI), Jul. 2015.
12. RohitThanki, SurekhaBorra, VedvyasDwivediabdKomalBorisagar, "A Steganographic Approach for Secure Communication of Medical Images based on the DCT-SVD and the Compressed Sensing (CS) theory", The Imaging Science Journal, vol. 65, no. 8, Sep. 2017.
13. Hayat Al-Dmour and Ahmed Al-Ani, "A Medical Image Steganography Method Based on Integer Wavelet Transform and Overlapping Edge Detection", International Conference on Neural Information Processing (ICONIP), pp. 436-444, Nov. 2015.
14. Vikas Kumar Mishra, Shobhit Kumar and NeerajShukia, "Image Acquisition and Techniques to Perform Image Acquisition", MRI Publication, vol. 9, no. 1, 2017.
15. Raman Maini and HimanshuAggarwal, "Study and Comparison of Various Image Edge Detection Techniques", International Journal of Image Processing (IJIP), vol. 3, no. 1, pp. 1-11, Feb. 2009.
16. EhsanNadernejad, Sara Sharifzadeh and Hamid Hassanpour, "Edge Detection Techniques: Evaluations and Comparison", Applied Mathematical Sciences, vol. 2, no. 31, pp. 1507-1520, 2008.
17. J. Canny, "Finding Edges and Lines in Image", Master's Thesis, MIT, 1983.
18. Raman Maini and Dr. HimanshuAggarwal, "Study and Comparison of Various Image Edge Detection

Techniques", International Journal of Image Processing (IJIP), vol. 3, no. 1, Feb. 2009, pp. 1-12.
19. Musaruddin M and Kouzani A. Z., "Embedding Data in Images using Wavelet Packets", TENCON, Nov. 2004.
20. Mohammad Ali Lotfollahi-Yaghin and Mahdi Koohdaragh, "Examining the Function of Wavelet Packet Transform (WPT) and Continues Wavelet Transform (CWT) in Recognizing the Crack Specification", KSCE Journal of Civil Engineering, vol. 15, no. 3, Mar. 2011, pp. 497-506.
21. Mothi R and Dr. M. Karthikeyan, "Color Image Watermarking Using Wavelet Packet Transform", IEEE International Conference on Computational Intelligence and Computing Research, Sep. 2015.
22. J. L. Rodgers and W. A. Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", The American Statistician, vol. 42, no. 1, Feb. 1988, pp. 59-66.
23. Eugene K. Jen and Roger G. Johnston, "The ineffectiveness of Correlation Coefficient for Image Comparisons", Research Paper prepared by Vulnerability Assessment Team, Los Alamos National Laboratory, New Mexico.