TABLE OF CONTENTS

Content Name Page no.

LIST OF FIGURES:

LIST OF TABLES:

Abstract

The development in networking technologies and telecommunication has move forward. In medical diagnosis, many processes have proposed by numerous researchers for securing patients records and medical image which are sending one location to another location. So, to protect the privacy of patients, security in the medical images is very much important because if deterioration is found in medical data and/or images at the time of transmitting then there will arise many problems in the treatment of patients. In this thesis, I have proposed a model which can be used to transmit the medical images securely as well as maintains confidentiality and integrity of the medical images. For secure transmission, I have used Huffman encoding method because this technique helps to both compress and encrypt the watermarked image without any loss of information bits. I have used Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) on each 8x8 block and Singular Value Decomposition (SVD) to embed watermark medical image into the host medical images to maintain confidentiality and integrity.

Keywords: DWT, DCT, SVD, Huffman Encoding, Watermarking, Encryption, E-Healthcare system

CHAPTER 1

INTRODUCTION

1.1 What is Security of Medical Image?

In medical diagnosis, many processes have proposed by numerous researchers for securing patients records and medical image which are sending one location to another location. The paper focused on the modern technique, past work and presets some approaches security of medical images. The security of medical image is basically based on the following:

[1] **Confidentiality:** The transmitted message must go to the intended receiver. Except intended receiver, the message cannot be recognized.

[2] **Integrity:** This property ensure that the data must be exactly same as they were sent. During the transmission, the data must not be changed by any other persons.

[3] **Authentication:** It means that the receiver have to be sure of the identity of the sender's and that the message has not sent by any other.

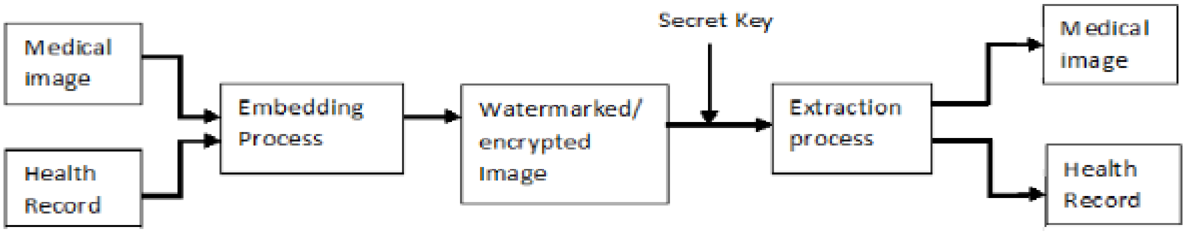


Figure1: An overall process to sending a secure image

Basic process of a sending a secure Image is explained by figure 1.There medical image and health record is first embedded and then some watermarking or encryption algorithm applied on it. Next that encrypted image is send over the network. When receiver receive that image, she extract the image and health record. We should remember, extracted image should be exact as original image for overall this transmission process.

When digital images and the patient's data are transmitted through public networks, then Security is very important issue. So it is necessary to protect them. Cryptography is used for secure transmission and Watermarking is used to maintain confidentiality and integrity. To provide the security we have to encrypt the information when that is sending by the sender.

1.2 The different types of methods used to protect the Medical Images

Medical image sharing through internet becomes very popular nowadays. When send any medical information then we should maintain above properties for secure that information. To provide the security we have to encrypt the information when that is sending by the sender. For encryption we can use different process like watermarking, steganography, digital signature, RSA, AES algorithm etc. To secure the information, we can also use quantum steganography. Quantum image steganography [10] is a method that helps to understand the quantum image processing and that also describe the steganography. The quantum information feature is mainly used in Quantum steganography systems .This models is strictly secured compared with the classical model. After the encryption, the quantum image is embedded into the quantum host image. For this quantum image steganography technique, quantum watermarking uses a quantum host image to hide the information. There was mainly three phases. In the first phase, the watermark image is expanded with 8-bit.In the second phase, the expanded image is now embedded by the controlled-NOT operation and in the third phase, remove the watermark from the host image. We have to observe those method which will be lossless or fully reversible in case of medical image because patient's life is dependent on a medical data and image. Swapped Huffman tree encoding (SHT) method [4] is helps to encrypt and compress image. Now days, steganography technique is more secured than other encryption process. In watermark embedding, the host image can be transformed by mainly three process like DWT,DCT and SVD[1].We can verify how much noise include or image quality distorted or number of changing pixel rate by calculating PSNR value, SNR ,SSIM,NPCR, NC UACI value in the result of extracted image

CHAPTER 2

LOSSLESS COMPRESSION AND TRANSFORMATION TECHNIQUES

2.1 Image Compression

One of the application of data compression process is image compression which encodes the image with some bits. The main aim is to decreases the redundancy of the image to send or store data which gives an efficient result.

2.2 Types of image Compression

i. Lossy Image Compression

Sometimes, when we want to crop a photo, lossy compression discards some parts of a photo. There have two types, 1) JPG or JPEG and 2) Gif.

1) **JPG OR JPEG**

   This format gives free of bits that is depending upon the compression level of that image. In this format, a small quantity of compression can be negotiable but absolute compression may be evident.

2) **GIF**

   GIF generally compresses the files which are mainly cut down the number of colors that file has. When a photo has more than 256 colors, then that format will change the image with less pathetical. GIFs are generally used for images which are animated.

ii. Lossless Image Compression

Lossless compression is a mainly used to reduce the size of a information or image where maintaining the same quality issue as original information or image. So we can say that all original information or image can be recovered when that information or data will be uncompressed. In lossless compression, each single bit of information or image which was exactly same as before. All the data or image can completely recovered. This technique generally used lie some financial data or some medical image .If those are losses or changed which creates some big problems.Types of lossless images compression are: Run-length encoding, DPCM, Adaptive dictionary algorithms etc.

2.3 DCT and its Advantages

The discrete cosine transform (DCT) is a way which is used to transform a signal into frequency components. Usually 2D DCT is required for compression of image. Vertical and horizontal dimensions are considered in the 2-D DCT and 2D DCT gives the frequency Coefficients in form of another matrix. DCT-based Watermarking has mainly two facts. The first one is lies on the most important visual parts of the image where the signal energy of image lies at sub band with low-frequencies. The second one is that high frequency Components are generally reduced by noise attacks and compression.

2.4 SVD and its Advantages

Three sub-matrices is obtain from SVD , three matrices has separate name which are known as left singular matrix (U), singular matrix (S) and right singular matrix (V). The SVD should be applied only a matrix. Suppose X is a symmetric matrix, so we can say that SVD can be computed by the equation $X=USV^T$.Where, X has three new matrices U, S, and V. S is a diagonal matrix and U and V are orthogonal matrices. The advantage of this method is energy compaction and for the local statistical variations of image, it can be easily adapted. SVD can be used on types of matrix of m x n size. So SVD can be required for decrease the storage space of an image and also for compression. After some study, we can say decomposition of SVD gives a good quality result and also MSE and PSNR value.

CHAPTER 3

LITERATURE REVIEW AND COMPARETIVE ANALYSIS

3.1 Literature Review

In medical diagnosis, when transfer of medical images and its information, there security concern is described and different researchers have proposed different method for medical image watermarking and cryptography technique. Thakur et al. [1] elucidated mainly robust watermarking approach where mainly uses transform domain process. Here first apply 2nd level DWT on carrier image and after that apply DCT & SVD on that image. DCT & SVD is also applying in cover image. Chaos based encryption is used on watermarked image for more confidentiality. Reverse processes are used to get original image. By this multilevel watermarking approaches, the experimental results are indicates that this process is highly robust and very secure from different types of attacks and host and cover images are not very distorted.

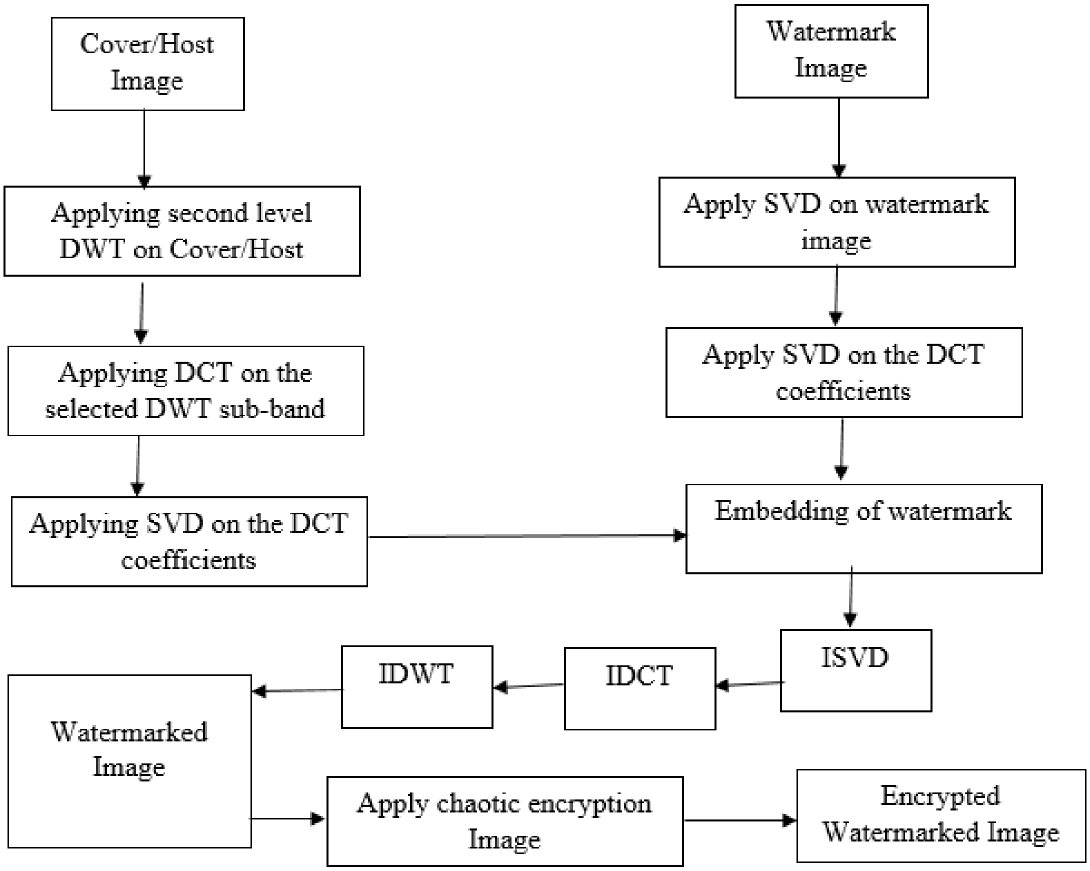

Cover/Host Image
Watermark Image
Applying second level DWT on Cover/Host
Apply SVD on watermark image
Applying DCT on the selected DWT sub-band
Apply SVD on the DCT coefficients
Applying SVD on the DCT coefficients
Embedding of watermark
ISVD
IDCT
IDWT
Watermarked Image
Apply chaotic encryption Image
Encrypted Watermarked Image

Figure 2 Diagram of encryption process of tele-health application

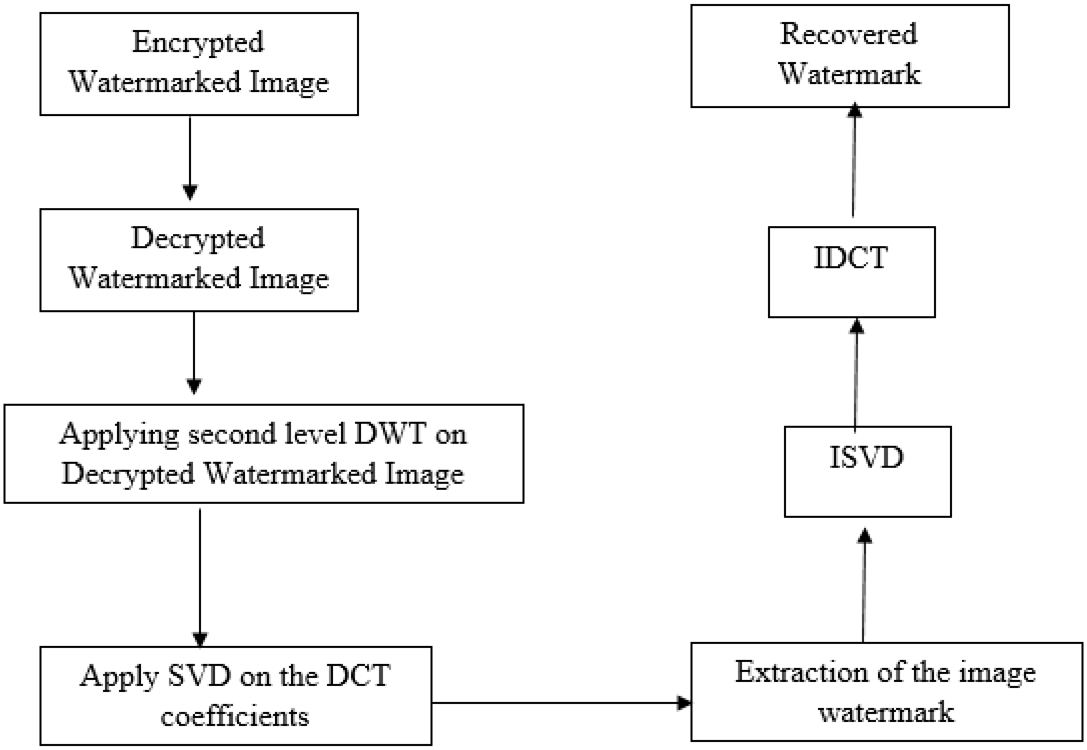

Encrypted Watermarked Image
Decrypted Watermarked Image
Applying second level DWT on Decrypted Watermarked Image
Apply SVD on the DCT coefficients
Extraction of the image watermark
ISVD
IDCT
Recovered Watermark

Figure 3 Diagram of decryption process of tele-health application

Advantages:

- Patient information maintained High Confidentiality.
- Chaotic encryption algorithm provide deterministic and sensitivity towards the parameter.
- Robustness is improved because here used combination of three different transform domain techniques and the experimental Result is indicated a good results.
- The bandwidth is saved to requirements for tele-health applications.

Disadvantages:

- This paper used only single Cover image for Watermarking technique. If there use multiple cover image host image will be more secured.
- The performance of Video and multiple watermarking is not determined.

Parah et al. [2] explained a IoT driven healthcare system, A fragile watermark is used to embed the EPR (Electronic Patient Record). This type of watermark can detect whether the EPR is tampering or not during the transit. At the receiver side, first receiver check the fragile watermark if that is same as before in sender side then receiver confirmed that EPR has not attacked when that is transmitted. If that watermark not same as sender side hen receiver not extract the EPR and send retransmission request to sender. In this process Two address Vector is used to embedding the EPR.

Advantages:

- This system has the capability to detect tamper and it gives better imperceptibility.
- Here used different strategies which is very helpful to embed information which provide a strong security.
- The subjective quality analysis is used in this method which is helps to reach a good results.
- The watermark can be easily recovered.

Disadvantages:

- The main disadvantages is that the embedded image is weak to different geometric attacks and processing of signaling.

Elhoseny et al. [3] explained the medical information is divided into two part like odd and even part of that text for hybrid encryption. In the even part of data, the RSA algorithm is applied and in the odd part of the data, AES algorithm is applied. In the cover Image, 2-level DWT is applied. Next that image is embedded with the Cipher Data and finally stego image is generated. The reverse process is used to extract the data and image.

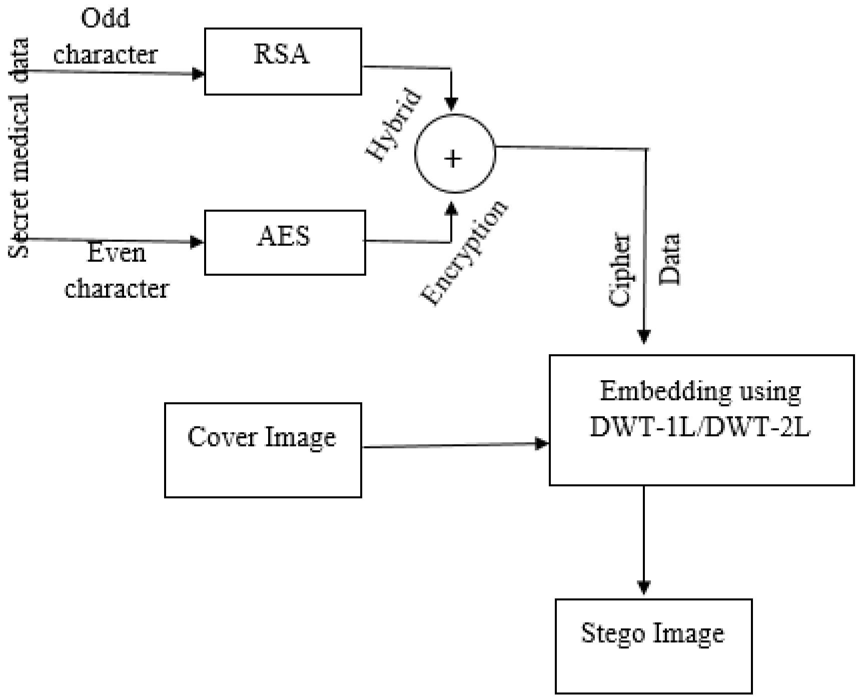


Figure 4 Diagram of encryption process of Health care system using IOT

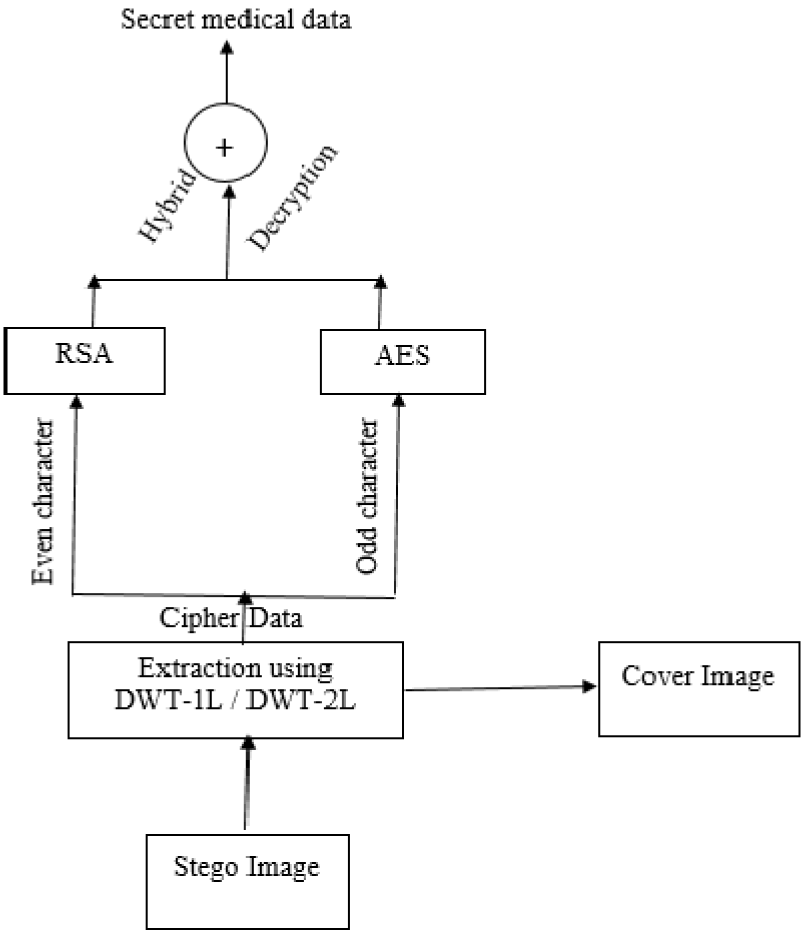


Figure 5 Diagram of Decryption process of Health care system using IOT

Advantages:

- This model gives a smaller MSE value and a higher PSNR value which helps to give a high performance.
- This method provides high imperceptibility and capacity.

Disadvantages:

- Small deterioration is found in the stego-image at receiver site.

Muhammad Arslam Usman [4] presents a method which gives good results with a good imperceptibility and this method also gives high capacity because this method used a lossless compression to the watermark images. Here watermark image is encrypted and compressed by using swapped Huffman tree encoding (SHT) process. Now days, steganography technique is more secured than other encryption process. Here experimental result of histogram of host image and cover image shows that there have high imperceptibility and capacity.

Secret Key= 11001 | 10110 | 111

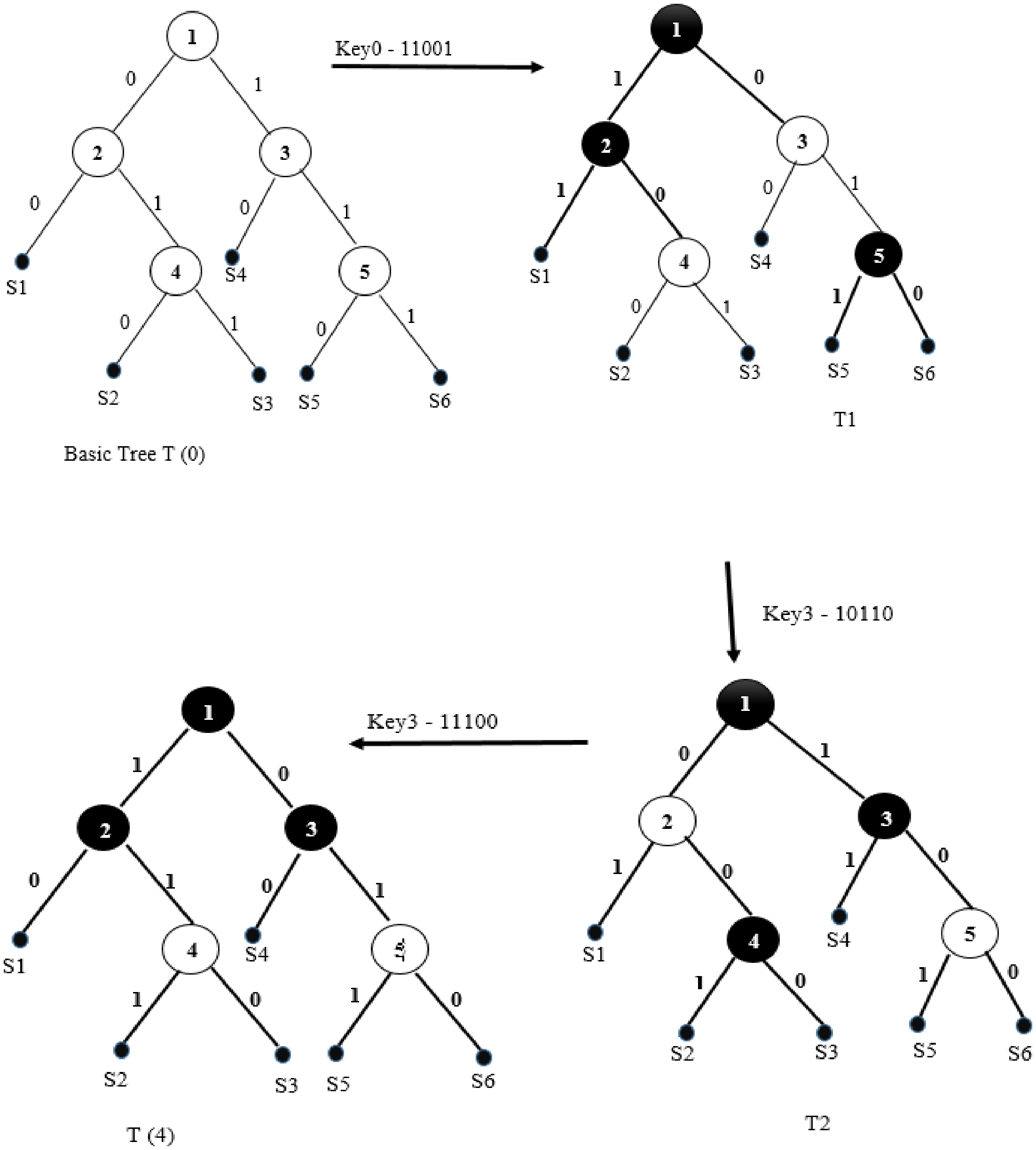


Figure 6 Example of Swapped Huffman Tree Encoding (SHT)

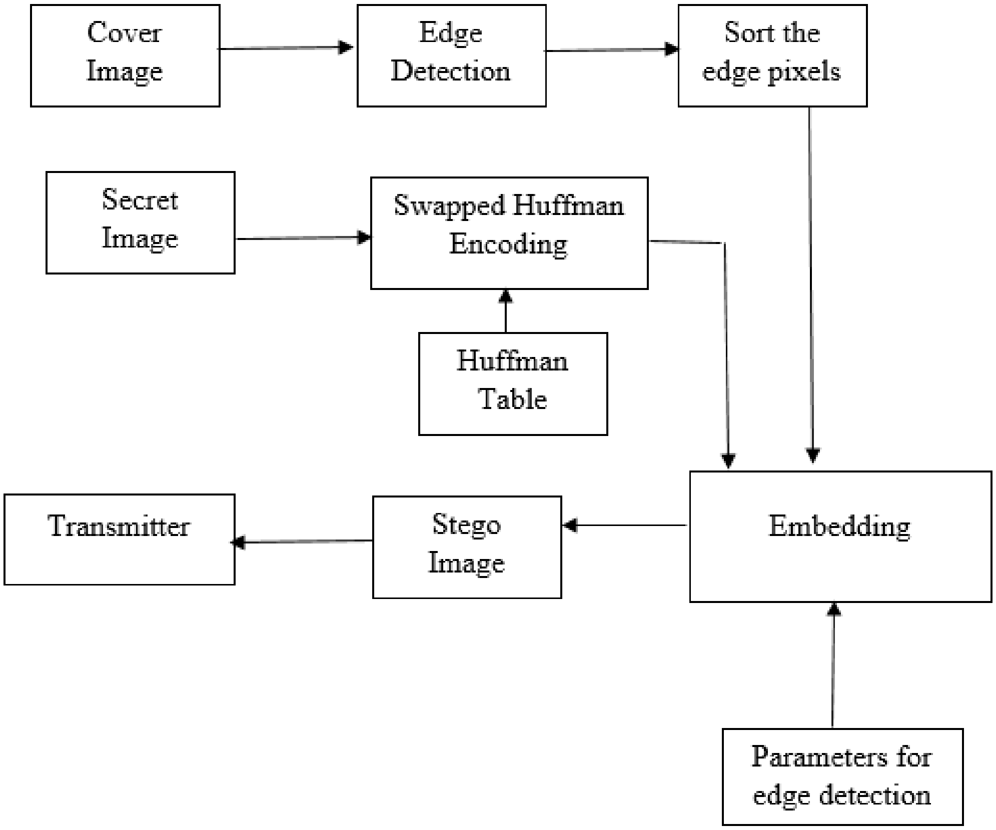


Figure 7 Diagram of encoding process of steganography with swapped Huffman encoding technique

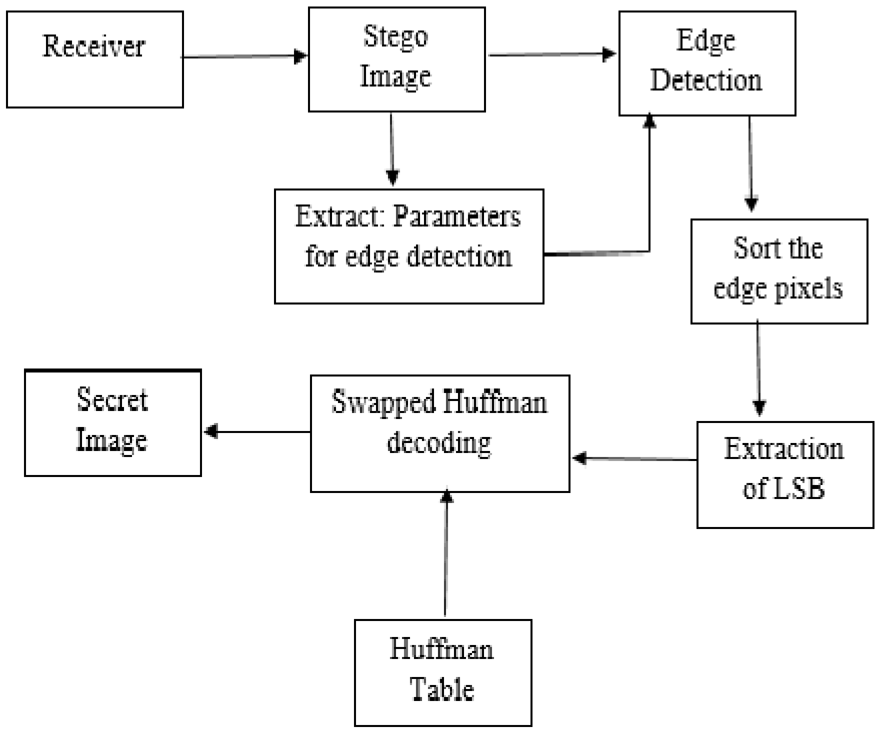


Figure 8 Flow Diagram of decoding process of steganography with swapped Huffman encoding technique

Advantages:

- The advantages of this method are that it provides security, capacity, and robustness. This three aspects of steganography makes it useful in hidden transformation of information through any media and create a highly secured communication.
- The imperceptibility property of the hidden data is maintained.
- As medical image is very important for patient’s treatment so there lossless image encryption is preferable than lossy image encryption techniques, Here image is encrypted by swapped Huffman tree which is a lossless method.

Disadvantages:

- With compared to the host images, There are small distortion is found in the histograms.

Shehab et al. [5] explained a SVD-based fragile watermarking process uses group blocked method to increase security. In VQ attack, authentication of block and recovery bits by itself is used. To recover the tampered region from the neighboring block, here used Arnold Transform. This method gives good results in the NCC and PSNR of the recovered image. By using this method we can also protect from different types of attack.

Advantages:

- This method is a grouped block method which provide more security and helps to protect from different types attacked.
- The Arnold transform is very much helpful to increases the NCC and PSNR of the recovered image.
- Compared to other methods, it improve tamper localization accuracy Performance. Fragile tampered images is handling very good by this process.

Disadvantages:

- Efficiency is not evaluated in case of non-fragile tampered images.

Aparna et al. [6] explained a hybridization of compression and cryptographic algorithm is used for watermarking technique. At fast we have to find the ROI part of input image by using Region Growing Algorithm and the ROI part is now encrypted by SHA-256 algorithm. We have to use elliptical curve cryptography (ECC) to encrypt EHR document and by using Arithmetic coding algorithm (AC), the image and EHR document is concatenate and compressed. Finally embed the complete bit stream into original image.

Advantages:

- The performance of the proposed approach achieves better results in the PSNR value and the capacity of embedding.
- The computational complexity is less because of using simple mathematical calculation.

Disadvantages:

- This paper used only single Cover image for Watermarking technique. If there use multiple cover image host image will be more secured.

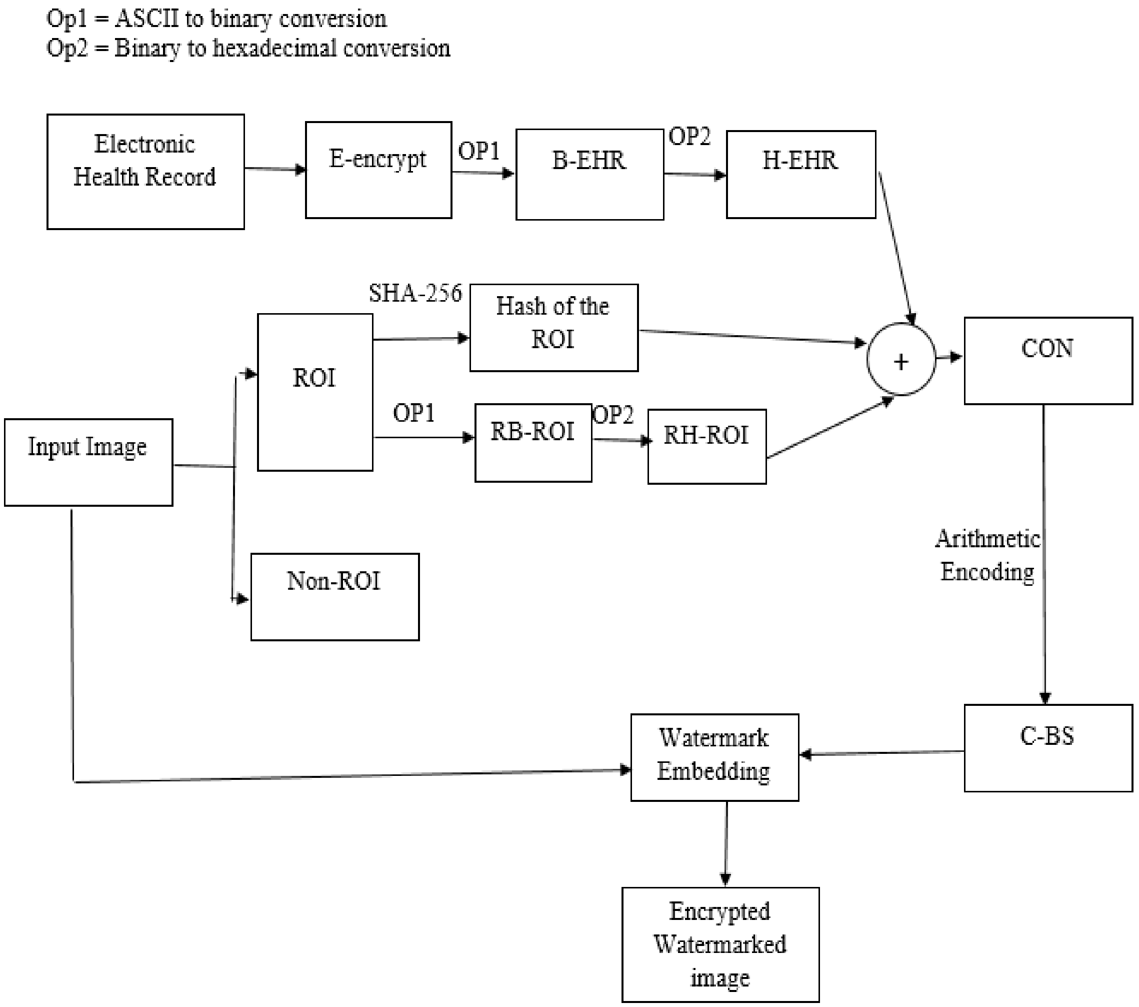


Figure9 Flow diagram of encryption process of hybrid encryption algorithm

Liao et al. [7] elucidated here JPEG image is used for embedding process. First image is separated into sub image which are non-overlapping on the basis of 8x8 blocks and ensuring2 adjacent DCT block belongs two different sub-images. After that calculate the AC coefficient sub image and cost value matrix C by applying cost function. Next cost values are combining and updated the stego image. This process will be continue until the all sub image are embedded.

Advantages:

- This proposed model shows effective results for the embedding and gives better performance in the anti-steganalysis.
- It gives better result with respect to the previous method.

Disadvantages:

- Considering complexity analysis, this process takes more time to obtain high performance.

Praveenkumar et al. [8] explained that a Digital Imaging and communication in Medicine image is first encoded by DNA encoding by using 1D Logistic System. Then by using MSB manipulation, DNA addition and DNA subtraction is applied into that encoded image and concatenate that two part. After that by 1D logistic system DNA decoding is applied on that resultant concatenated image. Next by PWLCM System scrambling is done on that image and generate the final Encrypted image. Then the spectrum sensing technique is used to send the bio signal which is encrypted.

Advantages:

- The pixels are uniformly distributed so attacker cannot recognize easily the relationship between the pixels.
- This method provides a robust encryption because there result shows the values of histogram deviation is too good.
- This method provides high immunity to defend statistical attacks.
- Both the DNA and the chaotic map is used in this method which is helps to increase the algorithm's performance which helps to obtain better results from different analysis.

Disadvantages:

- The proposed method is highly secured but complexity is very high.

Ahmed A et al. [9] explained Robust that one side one healthcare staff send a medical image to the cloud and from other side another healthcare staff receiving that medical image from cloud. For this process at first transform the host image into quantum image controlled NOT. For this process NEQR (Novel Enhanced Quantum Representation) is required. Next the gray code is used to scramble the quantum image. The key is generated by logistic sign map and after that key is transform into quantum image representation. Then resultant the scrambled image is finally encrypted by XOR operation using that generated quantum key. Similarly,

Advantages:

- This method provides the zero-correlation based attacks.
- Based on histogram analysis, the quantum encryption approach is robust.

- This method is very robust for small changes of the pixel.
- Any small changes in secret key, not give the proper result.

Disadvantages:

- This proposed method needs a classical computer, various simulations and numerical methods are required for classical analysis.

Ahmed A Et al. [10] elucidated that a steganography technique is used to hide a quantum watermark image into host image. This quantum watermark image is encrypted by controlled "NOT" gate. After that two most and least significant qbits are used to embed the secret image. Here Before the embedding process, to creating a watermark image, the Arnold's cat map is used. In this method watermark and key are required for extract the watermarked image and not needed the host image and it present clear visibility and high embedding capacity for this propose decryption process.

Advantages:

- The host and encrypted watermarked image cannot be detected by the easily in naked eye.
- This method provides higher security than the other methods.
- This method present good PSNR values, height embedding capacity and excellent visibility.
- The original host image is not required to extract the secret image from the watermarked image.

Disadvantages:

- This proposed method needs a classical computer, various simulations and numerical methods are required for classical analysis.

3.2 Comparative Analysis

Ref. No.	Methods	Advantages	Limitations & Future scope
[1]	• DWT • DCT • SVD • Chaos based encryption	• Robust and secure • Hybrid Encryption process • two dimensional logistic maps gives better confidentiality	• Only single watermark image is used. • multiple watermark image can be used
[2]	• Generating stego RGB image using data embedded • Key is used for final encryption.	• High payload • Imperceptivity and Capability is high	• The embedded data is fragile • System robustness can be improve.
[3]	• RSA • AES • DWT-2L	• PSNR value is high and MSE value is low • High imperceptibility, capacity.	• Minimal deterioration is found. • Remove minimal deterioration.
[4]	• Edge detection algorithm • Swapped Huffman tree	• Provides security, capacity, and robustness • The imperceptibility property is maintained • Swapped Huffman tree is a lossless method	• Slight variations is found in the peaks of the histogram. • Remove those variation
[5]	• SVD • calculate authentication bits • Calculate self-recovery bits by using	• This scheme offer more security • Increases the NCC and PSNR values • Performance is very good in handling fragile	• Efficiency is not evaluated • Detecting and resolve that and other issues.

		tampered images	
[6]	• RG algorithm. • SHA-256 • elliptical curve cryptography algorithm • Arithmetic coding algorithm.	• The watermarked output image is save from attacks • Value of PSNR value and embedding capacity (bits) is better. • Computational complexity is less.	• Used Only single watermark image • Using of multiple watermark image will be more secure.
[7]	• calculate the non-zero AC coefficient of each sub image • Calculate cost value matrix C by cost function	• Better anti-steganalysis performance • Better results than the previous J-UNIWARD process and JPEG image steganalysis	• Time complexity is high to obtain higher security performance • Reduce utilized time.
[8]	• DNA encoding by 1D Logistic System • DNA addition and DNA subtraction by MSB manipulation • PWLCM System scrambling.	• robust • The pixels are uniformly distributed • High immunity to defend statistical attacks. • Algorithm's performance has increased by DNA and the chaotic map	• Complexity is very high. • Reduce the complexity of proposed method.
[9]	• NEQR (Novel Enhanced Quantum Representation) • Quantum controlled NOT image • gray code • Key is generated by logistic sign	• Robust • The zero-correlation requirement • Any tiny changes in the pixel is not allowed • The watermark image is exposed only by the correct secret key	• Various simulations and numerical methods are required and • Quantum watermarking can be use

	map and generate quantum Key by NEQR. • XOR operation is used for final encryption		
[10]	• Steganography • Controlled “NOT” gate • Arnold’s cat map	• High PSNR values and capacity of embedding and excellent visibility. • The cover image is not needed to extract the watermark.	• a classical computer, various simulations and numerical methods are required. • So future work will overcome this limitation.

Chapter 4

PROPOSED MODEL

4.1 Details of proposed model

After reviewing the literatures, I have tried to address some limitations of those paper to find more secured and effective way of transmitting medical data and images one place to another place. So I proposed a secure multilayer lossless watermarking encryption of Medical image which will be a lossless process and robust. In this model, first watermark or secret image is divided into 8x8 block and each 8x8 block is transformed by Discrete Cosine Transform (DCT). Now Singular Value Decomposition (SVD) is applied on that image. The host image is transformed using 2nd level of Discrete Wavelet Transform (DWT) and next that image is divided into 8x8 block. Discrete Cosine Transform (DCT) is now applied on each 8x8 block of image and finally that image is transformed by Singular value Decomposition (SVD).The transformed host image is now embedding with transformed watermark image, by this way watermarked image will be generated. Now, to increase the security and confidentiality, Watermarked medical image is encrypted by using Huffman encoding technique. This technique is used because it helps to both compress and encrypt the watermarked image without a loss in the information bits. So, this method presents both cryptographic and watermarking based hybrid technique. The reverse of the embedding and encrypting steps will follows to recover the secret image. Figure 10 shows this propose encryption model and figure 11 shows description model for securing the medical data transmission from one place to another place.

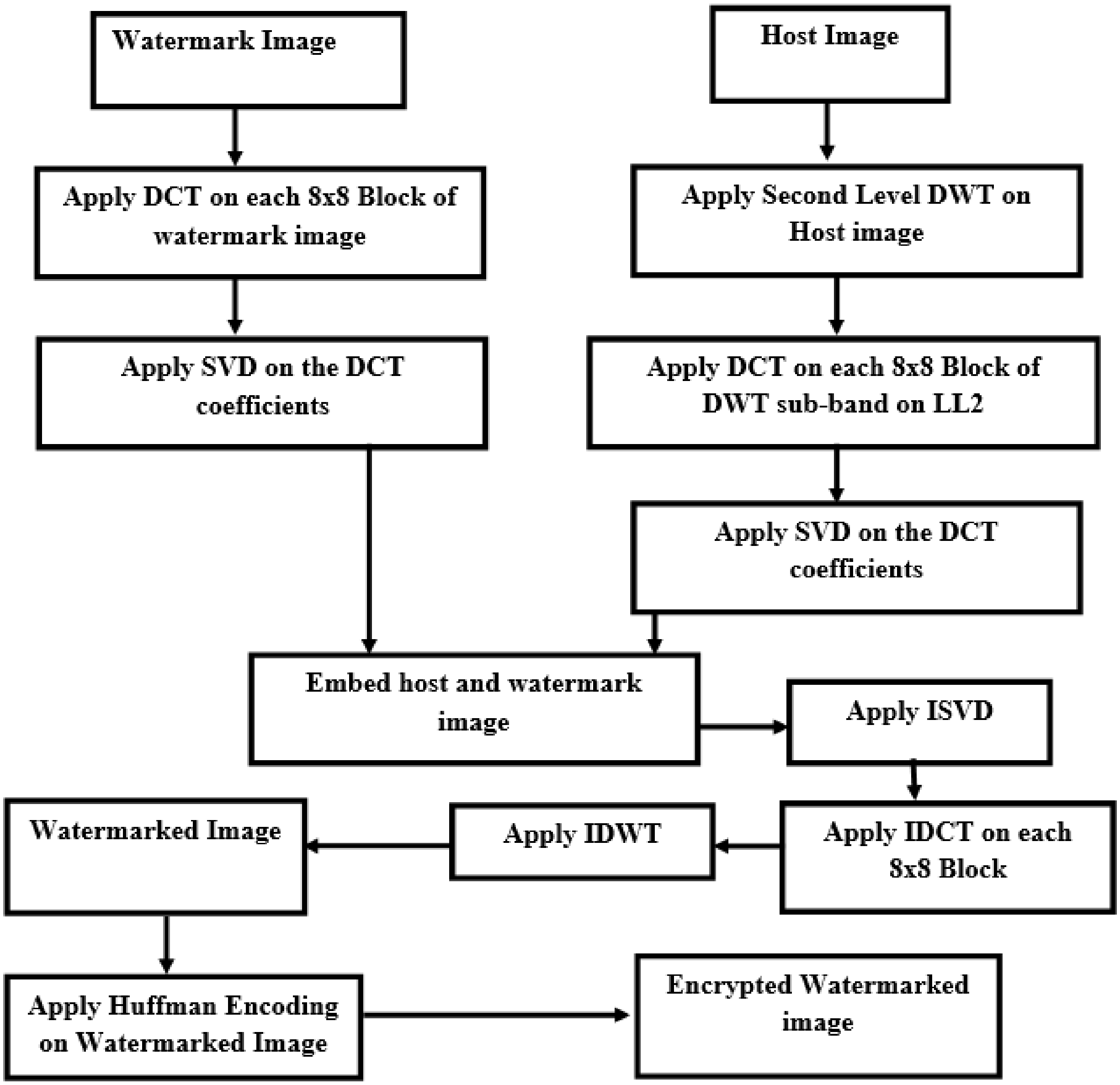

Watermark Image
Host Image
Apply DCT on each 8x8 Block of watermark image
Apply Second Level DWT on Host image
Apply SVD on the DCT coefficients
Apply DCT on each 8x8 Block of DWT sub-band on LL2
Apply SVD on the DCT coefficients
Embed host and watermark image
Apply ISVD
Watermarked Image
Apply IDWT
Apply IDCT on each 8x8 Block
Apply Huffman Encoding on Watermarked Image
Encrypted Watermarked image

Figure10: Proposed Embedding and Encryption Model

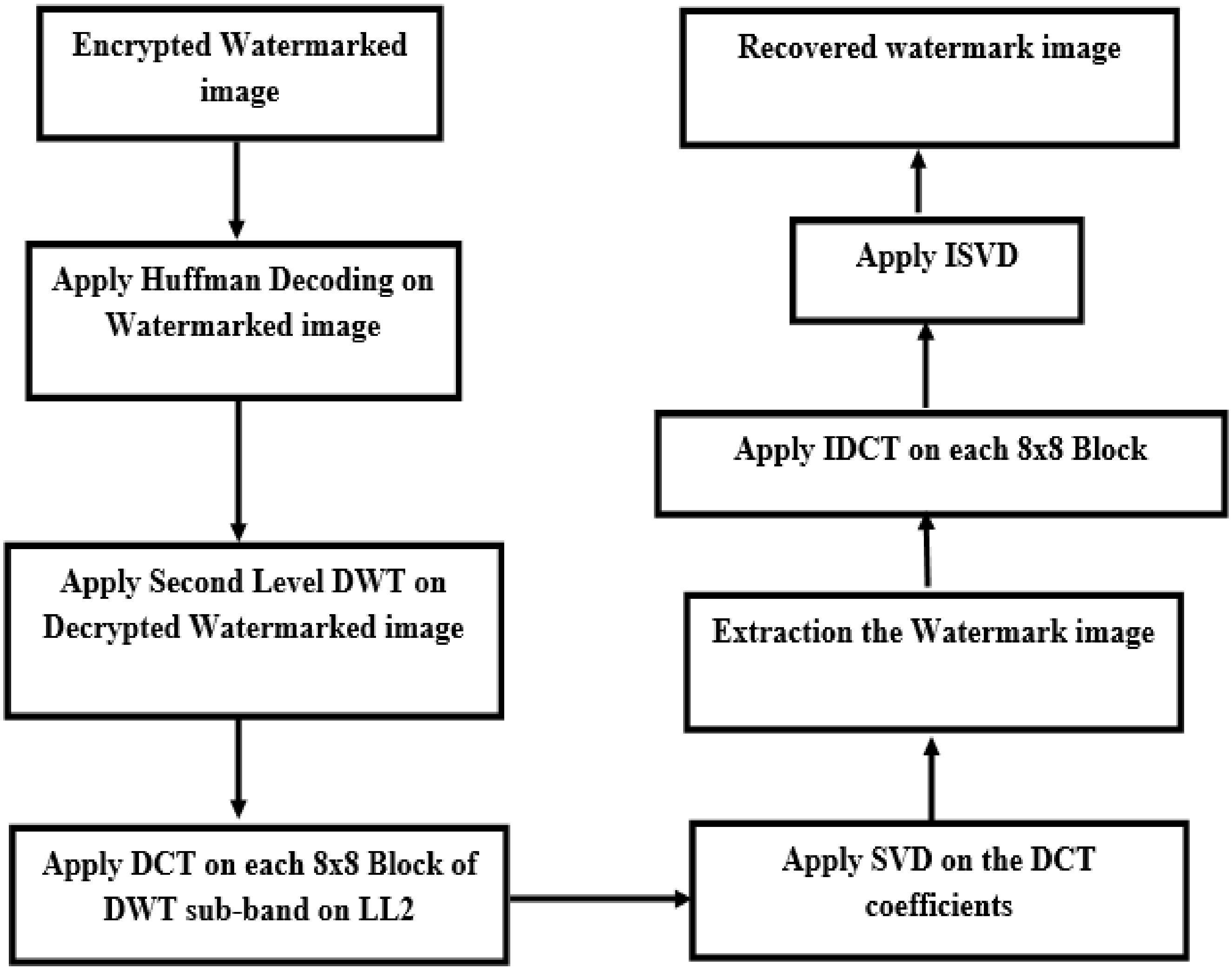

Encrypted Watermarked image
Apply Huffman Decoding on Watermarked image
Apply Second Level DWT on Decrypted Watermarked image
Apply DCT on each 8x8 Block of DWT sub-band on LL2
Apply SVD on the DCT coefficients
Extraction the Watermark image
Apply IDCT on each 8x8 Block
Apply ISVD
Recovered watermark image

Figure 11: Proposed Extraction and Decryption Model

4.2 Embedding Procedure:

Step 1: Read the Input Images:
(i) Host Image (512x512) → X
(ii) Watermark Image (64x64)→ W

Step 2: Apply 2nd level DWT on host image 'X'
(i) Level 1 DWT(X) →[xa, xh, xv, xd]
(ii) Level 2 DWT (xa) → [xxa, xxh, xxv, xxd]

Step 3: Divide 'xxa' into 8x8 blocks and apply DCT on each block
DCT (xxa) → DH
Step 4: Apply SVD on 'DH'
SVD (DH) → SH

Step 4: In case of Watermark Image,
Divide 'W' into 8x8 blocks and apply DCT on each block
DCT (W) → DW

Step 5: Apply SVD on 'DW'
SVD (DW) → SW

Step 6: The watermark image is embedded into cover by using a gain factor α
$WI=SH+\alpha\times SW$

Step 7: After this embedding process, again apply inverse of SVD, inverse of DCT on 8x8 block and inverse of 2nd DWT, respectively
ISVD (WI) →ISWI
IDCT (ISWI)→ IDWI
IDWT (IDWI)→ EmWI

Step 7: Apply Huffman Encoding process by using Huffman dictionary to get an encrypted watermarked image.
Huffman Encoding (EmWI) →EWI

4.3 Extraction Procedure:

Steps for recovered the watermark image as follows:

Step 1: The encrypted watermarked image (EWI) is now decrypted by the decryption process by which we get the decrypted watermarked image (DWI).
EWI → DWI

Step 2: Apply 2nd level DWT on decrypted watermarked image ‘DWI’
(i) Level 1 DWT (DWI) → [za, zh, zv,zd]
(ii) Level 2 DWT (za) → [zza, zzh, zzv, zzd]

Step 3: Divide ‘za’ into 8x8 blocks and apply DCT on each block
DCT (za) → DWI1

Step 4: Apply SVD on ‘DWID’
SVD (DWID) → DWIS

Step 5: the embedded watermark is now extracted
RW = (DWIS - SH)/α; Where α= gain factor

Step 6: After this extraction process, again apply inverse of SVD, inverse of DCT on 8x8 block and inverse of 2nd DWT, respectively
ISVD (RW) →ISRW
IDCT (ISRW)→ WImage

CHAPTER 5

RESULT AND ANALYSIS

5.1 Result and Evolution

Here I have explain the experimental set up and the result of the proposed model. First, I have taken an image of MRI of brain of size 512x512, considered as a host image and an MRI of brain as watermark image of size 128x128. My proposed model is implemented on MATLAB R2015a on a 64-bit machine with Core-i3 processor and 4 GB RAM. This model is proposed for gray level medical images such as MRI, X-ray, CT-Scan and Ultrasound are used .To analyze the result of the proposed model, I have used PSNR, SSIM, NC and MSE values. Basically more accuracy is needed for the medical image where information should not be lost. In Discrete Wavelet Transform (DWT), 'Haar' wavelet Transform is used as it gives better resolution result than other. Discrete Cosine Transform (DCT) is applied on each 8x8 block of image to increase the accuracy of the image. The Huffman Encoding technique is used because it helps to both compress and encrypt the watermarked image without a loss in the information bits. So, this method provides both cryptographic and watermarking based hybrid approach. By this model different attacks like crop, rotation etc. can be avoided because here final encrypted watermarked image is 1D. So comparing with other methods, our method is more secured and robust from different types of attacks.

Table 1 Performance Analysis of our proposed method at different gain factors

Sl No.	Gain Factor	PSNR	MSE	NC	SSIM
1.	0.01	61.9062	0.0419	0.8604	0.4992
2.	0.05	47.1468	1.2543	0.9946	0.9757
3.	0.1	41.0827	5.0677	0.9997	0.9976
4.	0.5	28.6201	89.3442	1.0000	0.9999
5.	1.0	26.7988	135.8941	1.0000	0.9984
6.	1.5	26.4249	148.1126	1.0000	0.9880

The experimental results are shown in the Table 1 where the PSNR, NC, SSIM and MSE values are calculated with different gain factors. Table 1 shows that when the gain factor decreases then the PSNR values are increased. It is also observed that when NC values are increased then gain factor is increased. Figure 11 and figure 14 shows the changes of PSNR and MSE values while changing the gain factors, respectively. Also. Figure 12 and figure 13 shows the changes of NC and SSIM values while changing the gain factors, respectively. I get best PSNR, NC, SSIM and

MSE values are 61.9062 (gain factor = 0.01), 1(gain factor =0.50), 0.9999 (gain factor =0.50) and 148.1126(gain factor =1.5), respectively. In Comparison with paper [1], this method give better results. Form this table, it is observe that our model gives better result to give high security on medical image with various gain factors.

Here I have used X-ray of hand and knee image, MRI of brain and thorax images, C-T scan of brain and lungs and Ultrasound of upper abdomen and lungs images, respectively. Table 2 shows the PSNR, MSE, NC and SSIM values for those different types of Medical Images. Figure 18 shows an effective results of our proposed method of PSNR and NC values.

This proposed model is very much robust from different types of attack because here final encrypted watermarked image is vector image which will be transmitted and if that watermarked encrypted image is attacked by attacker then original watermark image cannot be recovered from that attacked encrypted watermarked image.

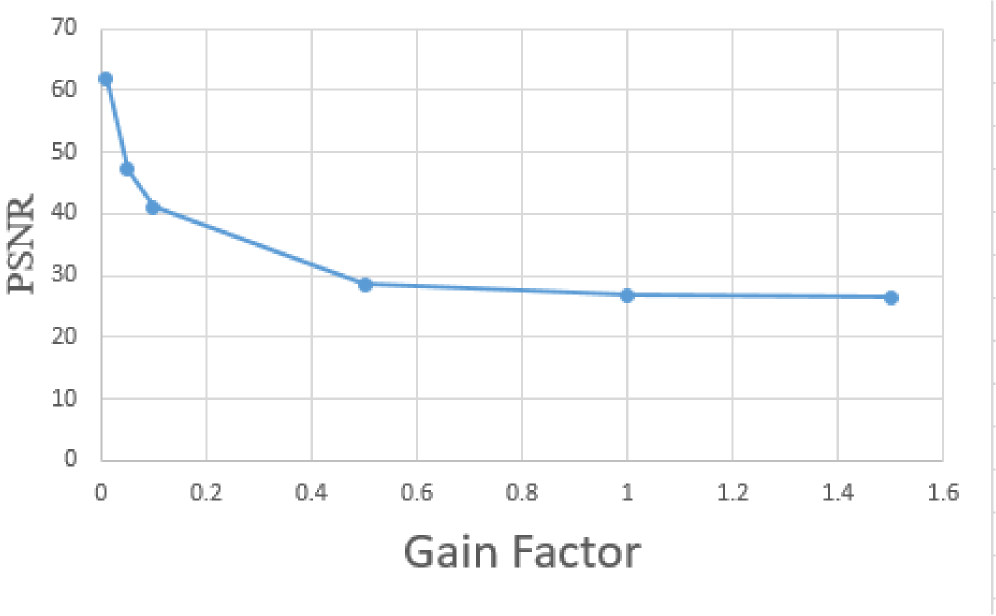


Figure 12 Performance analysis of PSNR values by varying the gain factor

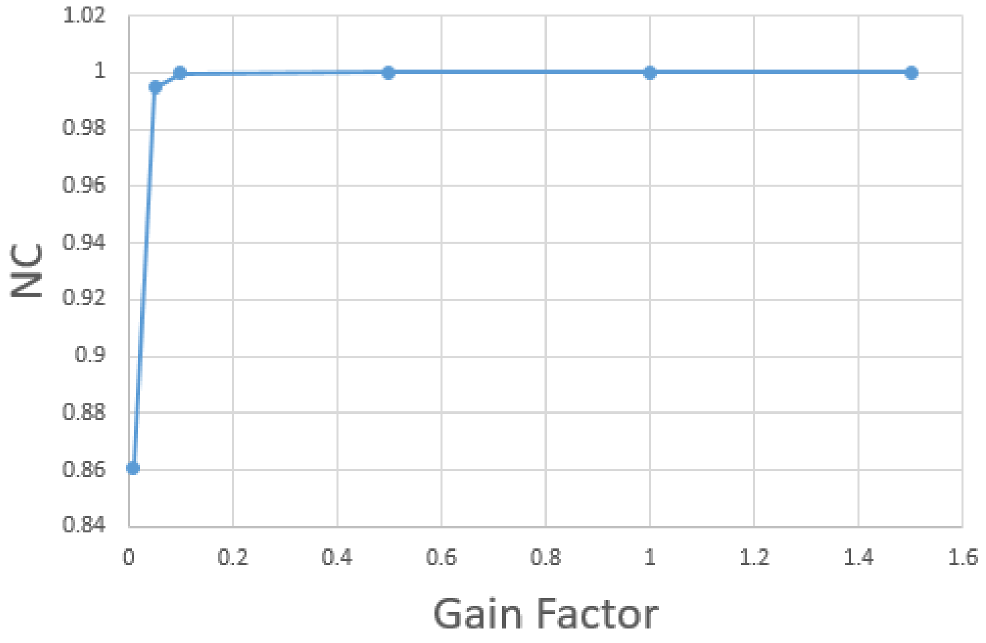


Figure 13 Performance analysis of watermark extraction of NC values by varying the gain factor

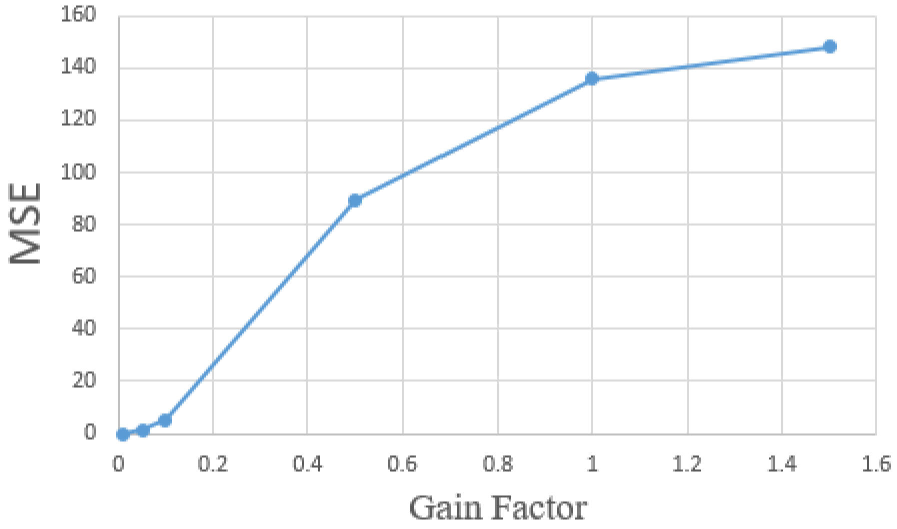


Figure 14 Performance analysis of MSE values by varying the gain factor

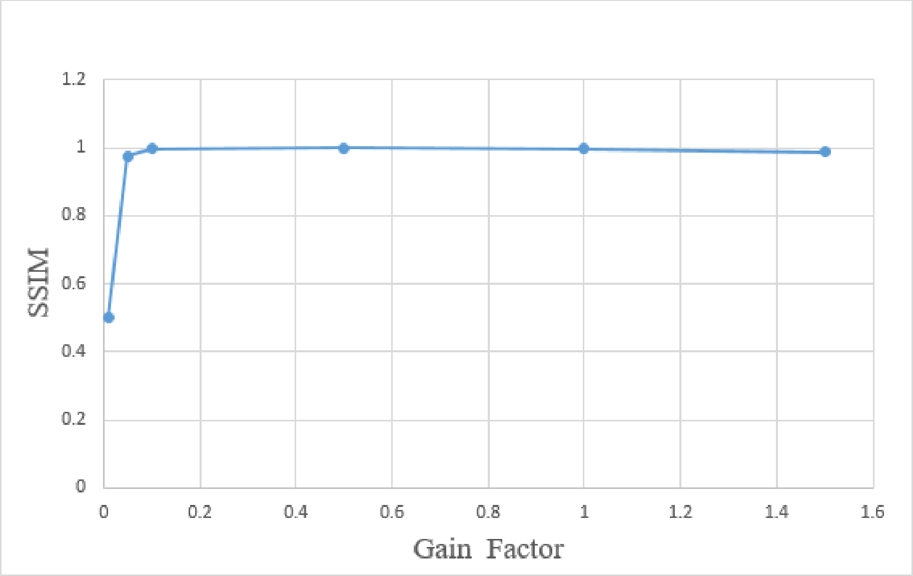
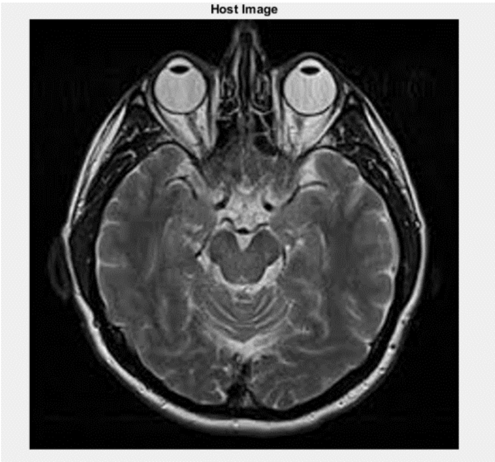


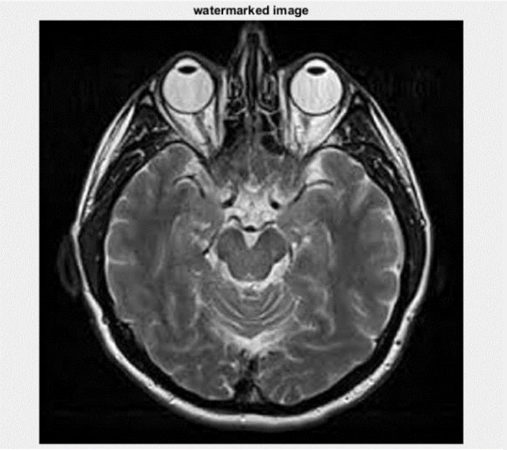
Figure 15 Performance analysis of watermark extraction of SSIM values by varying the gain factor

Table 2 Performance Analysis of our proposed method with different types of Medical Images

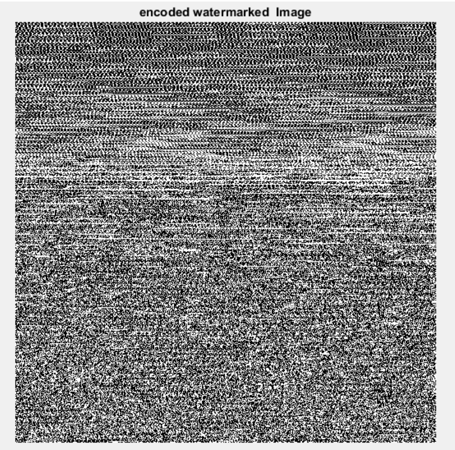
Image Type	Gain Factor	PSNR	MSE	NC	SSIM
MRI Image	0.5	28.6201	89.3442	1.0000	0.9999
C.T Scan Image	0.5	26.7904	136.1577	1.0000	0.2780
X-Ray Image	0.5	27.3155	120.6498	0.9795	0.9227
Ultrasound Image	0.5	30.2624	61.2122	0.9972	0.9640



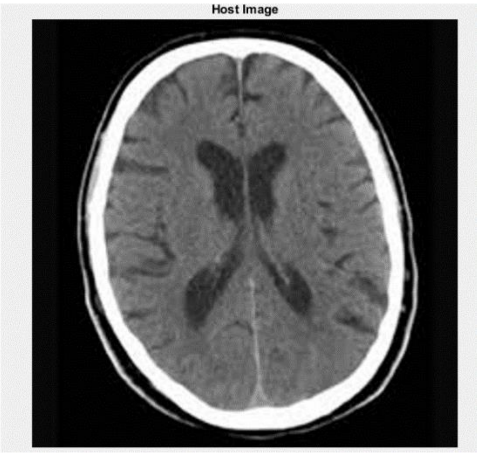
1(a)



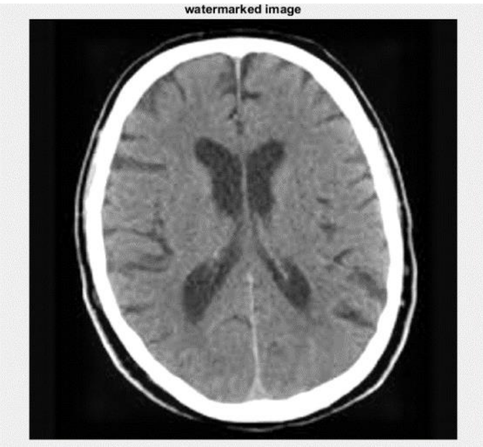
2(a)



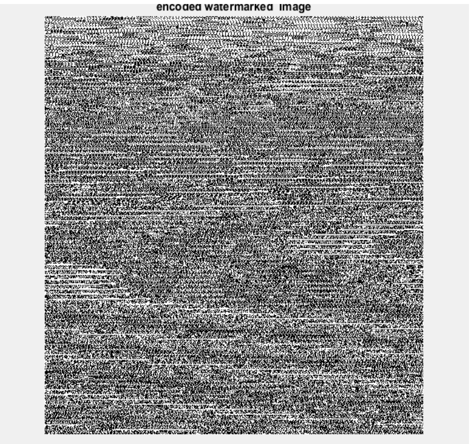
3(a)



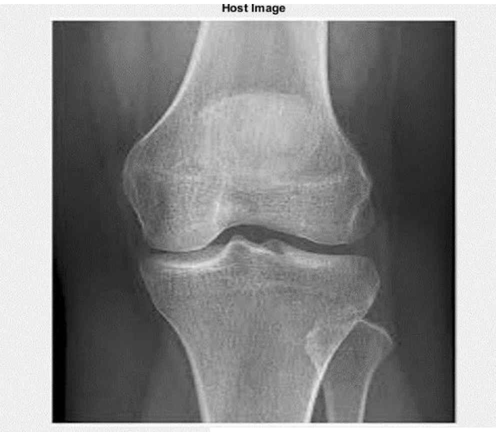
1(b)



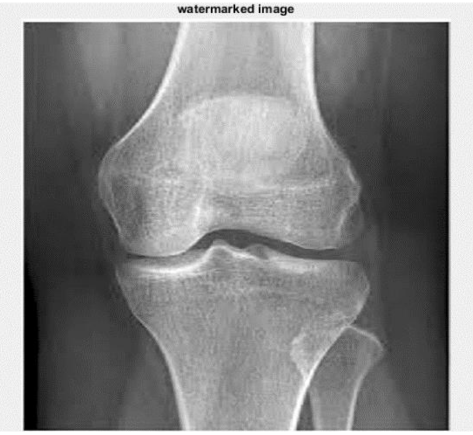
2(b)



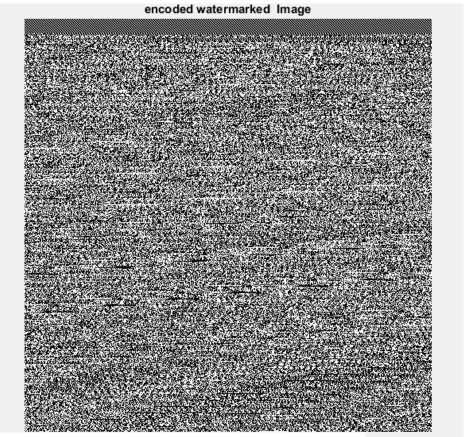
3(b)



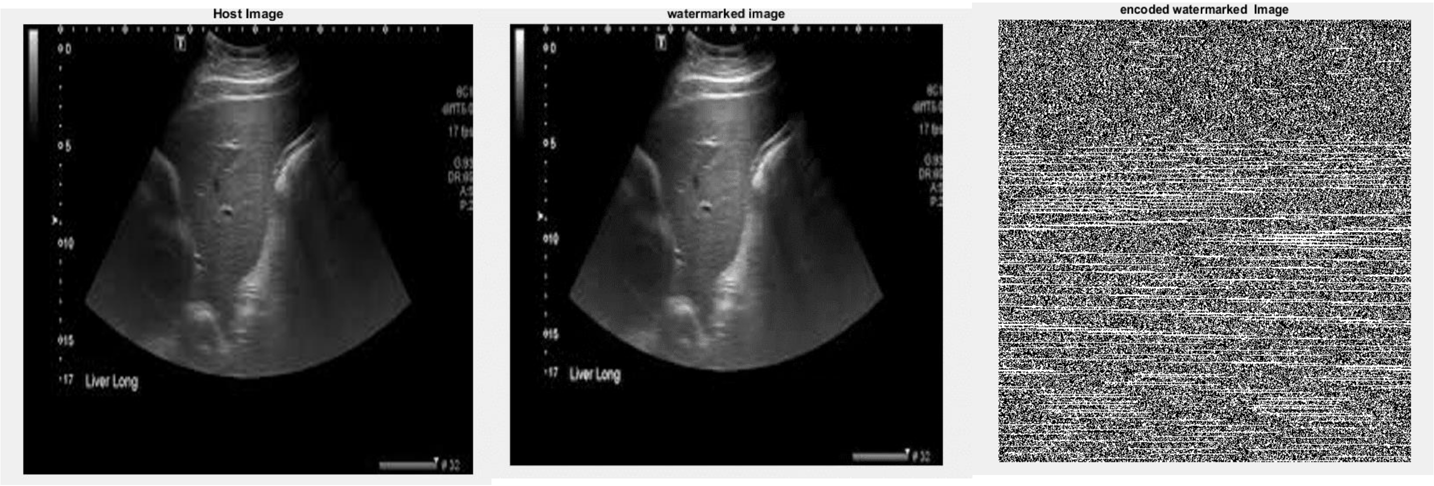
1(c)



2(c)

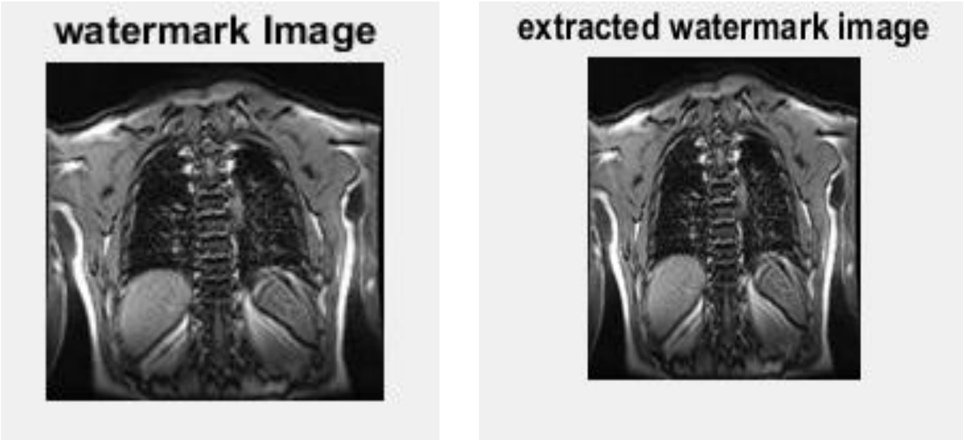


3(c)

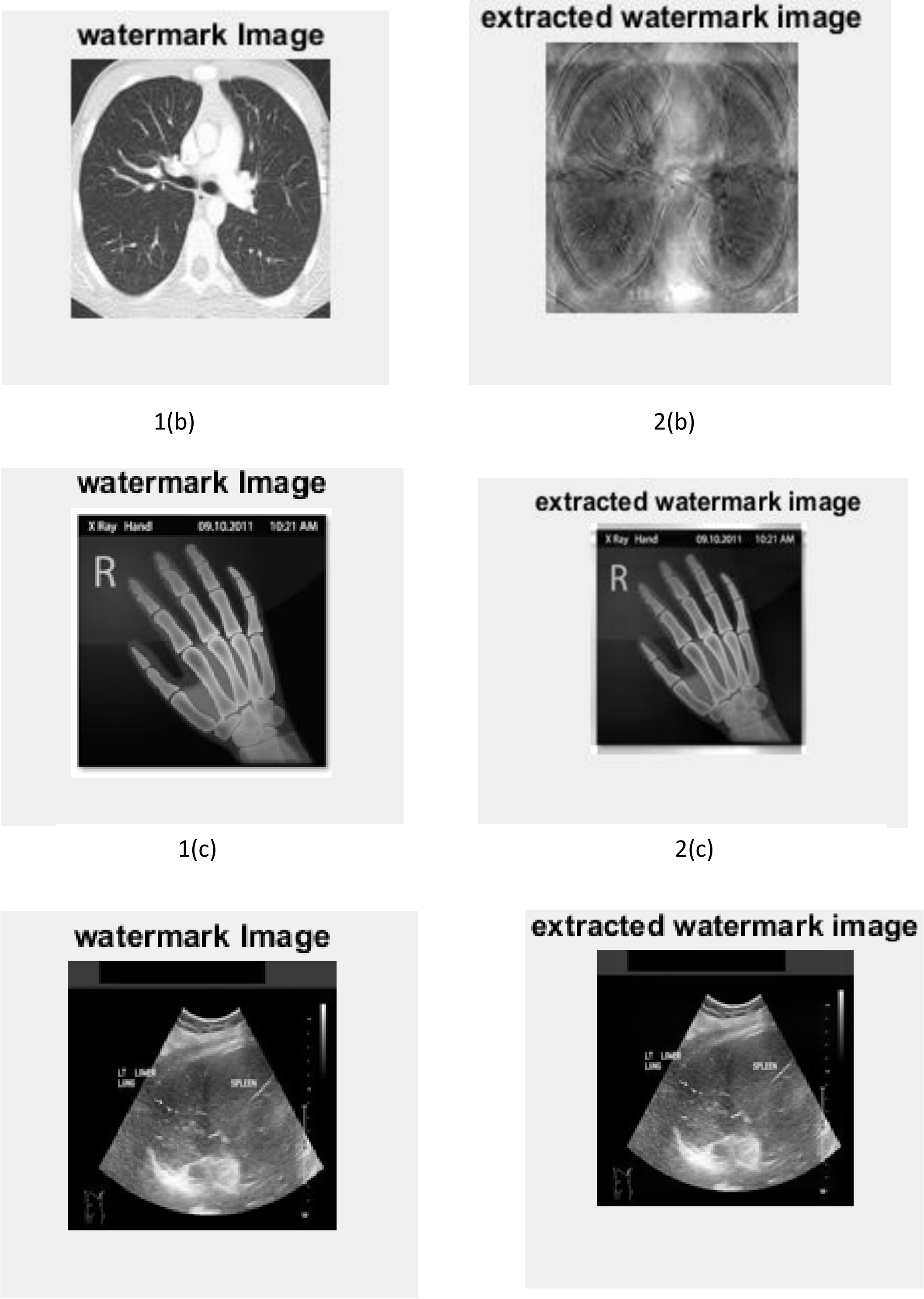


1(d) 2(d) 3(d)

Figure 16 1(a)-1(d) Host Image, 2(a)-2(d) Watermarked Image and 3(a)-3(d) Encrypted Watermarked Image



1(a) 2(a)


watermark Image
extracted watermark image
watermark Image
X Ray Hand 09.10.2011 10:21 AM
R
extracted watermark image
X Ray Hand 09.10.2011 10:21 AM
R
watermark Image
LT LIVER
LUNG
SPLEEN
extracted watermark image
LT LIVER
LUNG
SPLEEN

1(b) 2(b)

1(c) 2(c)

1(d) 2(d)

Figure 17 1(a)-1(d) Watermark Image and 2(a)-2(d) Extracted Watermarked Imag

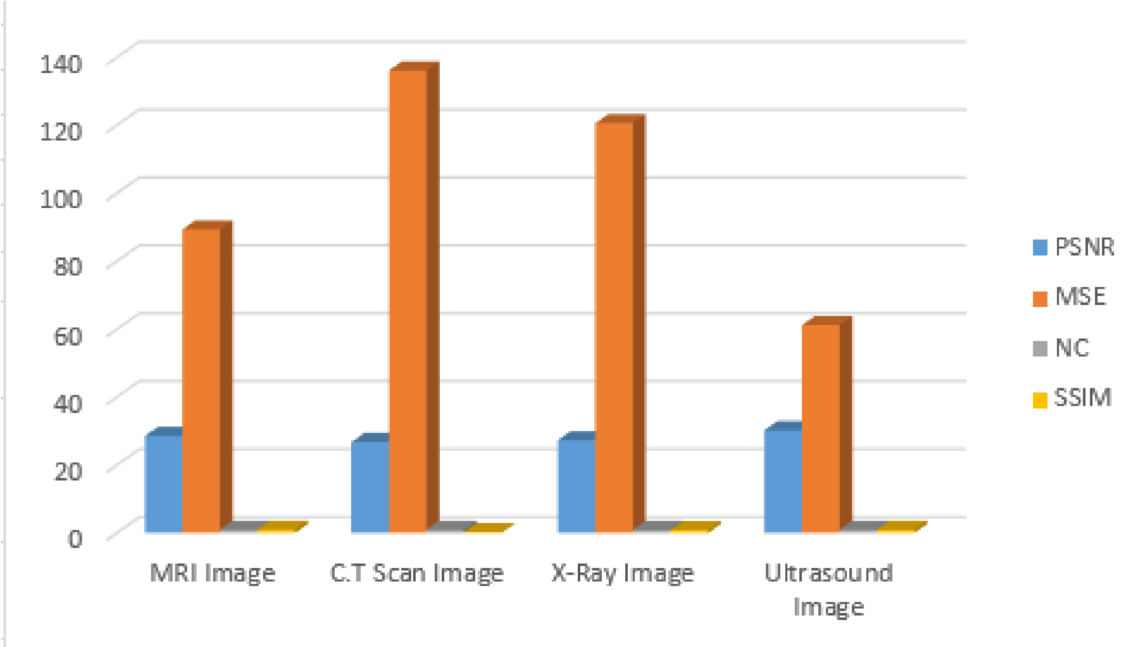
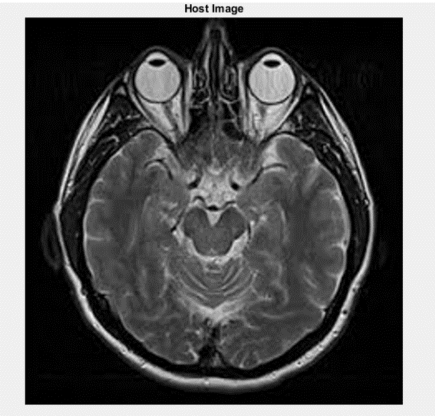
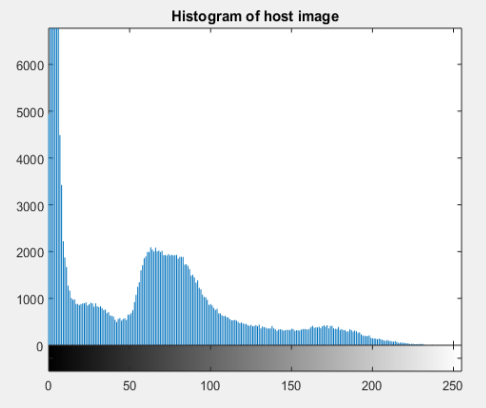


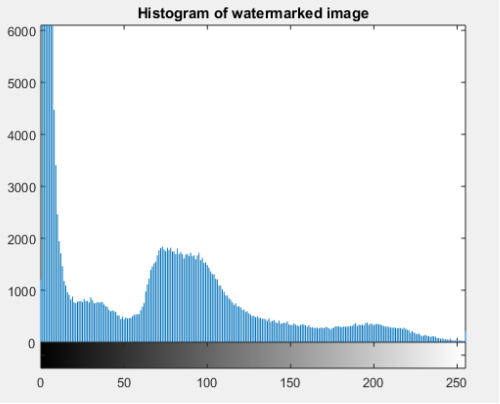
Figure 18 Performance analysis with different types of Medical Images



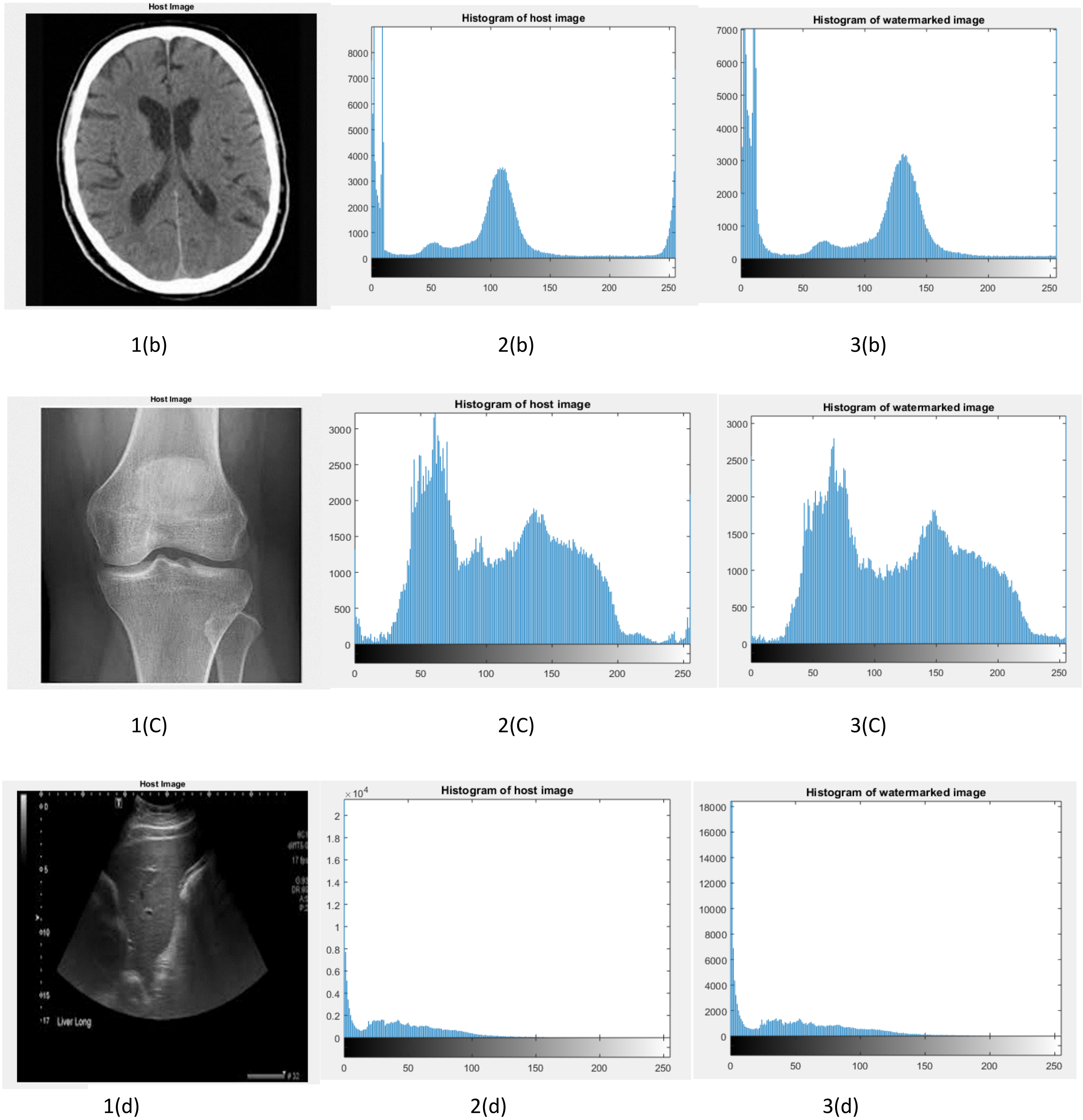
1(a)



2(a)



3(a)



1(b) 2(b) 3(b)

1(C) 2(C) 3(C)

1(d) 2(d) 3(d)

Figure 16 1(a)-1(d) Host Image, 2(a)-2(d) Histogram Analysis of Host Image and 3(a)-3(d) Histogram Analysis of Watermarked Image

4.3 Advantages and limitation of this proposed method

This section deals with advantages and limitations of the proposed model. I have used only gray scale images because maximum types of medical image is gray scale image. This model has many advantages over existing models. To increase the security and confidentiality, we use Huffman encoding technique. This technique is used to encrypt the Watermarked medical image. This Huffman encoding technique is used to helps to both compress and encrypt the watermarked image without any loss of the information bits. So, this method presents both cryptographic and watermarking based hybrid technique. Basically more accuracy is needed for the medical image where information should not be lost. Discrete Wavelet Transform (DWT) provides efficient multi resolution in the time-scale representation Discrete Cosine Transform (DCT) is applied on each 8x8 block of image to increase the accuracy of the image. So by this method we get more effective result than previous with PSNR and NC values. Also this method is very much robust from different types of attacks because here final encrypted watermarked image is vector image. If any changes occurred, the watermark image cannot be extracted. This process consumes more time to obtain the encrypted watermarked image. Also this model cannot handle RGB and 3D images.

CHAPTER 6

CONCLUSION AND FUTURESCOPE

6.1 Conclusion and Future scope

Security process becomes more complex because of the particular concerns of the medical community. We have to use an absolute algorithm to protect medical images. An algorithm have to recover the image which must be exact as previous with no changes in any pixel value. The algorithm should provide high security with low processing time. If medical data security is highly ensured then cybercrimes can be eliminated. All this method has some limitations which is discuss above and by removing those limitations, we can get a more secured new encryption or watermarking process. Basically more accuracy without loss of information is needed for the medical image. My proposed method provides both cryptography and watermarking methods which can be called a hybrid method. This method is very much robust for different attacks. Also it found best than previous published work. The result of analysis is helped to determine the potential value of the proposed method which is used to generate an acceptable quality of watermarked images with different gain factor. My proposed method provides both cryptographic and watermarking based hybrid technique because here first watermark image is embedded and then encrypted by using gain factor and Huffman Encoding process respectively. So my method provides more security than others because it gives a good PSNR and NC value and robust for different attacks.

I would like to further consider the performance of the underlying method for 3D medical Images.

References

1. Thakur, S., Singh, A.K., Ghrera, S.P. and Elhoseny, M., 2018. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia Tools and Applications*, pp.1-14.
2. Parah, S.A., Sheikh, J.A., Ahad, F. and Bhat, G.M., 2018. High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence* (pp. 409-437). Springer, Cham.
3. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N. and Farouk, A., 2018. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access*, *6*, pp.20596-20608.
4. Usman, M.A. and Usman, M.R., 2018, January. Using image steganography for providing enhanced medical data security. In *Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual* (pp. 1-4). IEEE.
5. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A.K., Yang, P., Huang, H. and Hou, G., 2018. Secure and robust fragile watermarking scheme for medical images. *IEEE Access*, *6*, pp.10269-10278.
6. Aparna, P. and Kishore, P.V.V., 2018. An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm. *Journal of Intelligent Systems*, *27*(1), pp.115-133.
7. Liao, X., Yin, J., Guo, S., Li, X. and Sangaiah, A.K., 2018. Medical JPEG image steganography based on preserving inter-block dependencies. *Computers & Electrical Engineering*, *67*, pp.320-329.
8. Praveenkumar, P., Devi, N.K., Ravichandran, D., Avila, J., Thenmozhi, K., Rayappan, J.B.B. and Amirtharajan, R., 2018. Transreceiving of encrypted medical image–a cognitive approach. *Multimedia Tools and Applications*, *77*(7), pp.8393-8418.
9. El-Latif, A.A.A., Abd-El-Atty, B. and Talha, M., 2018. Robust encryption of quantum medical images. *IEEE Access*, *6*, pp.1073-1081.
10. El-Latif, A.A.A., Abd-El-Atty, B., Hossain, M.S., Rahman, M.A., Alamri, A. and Gupta, B.B., 2018. Efficient quantum information hiding for remote medical image sharing. *IEEE Access*, *6*, pp.21075-21083.
11. Roček, A., Slavíček, K., Dostál, O. and Javorník, M., 2016. A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters. *Biomedical Signal Processing and Control*, *29*, pp.44-52.
12. Zhang, Y., Lu, K., Gao, Y. and Wang, M., 2013. NEQR: a novel enhanced quantum representation of digital images. *Quantum Information Processing*, *12*(8), pp.2833-2860.

13. Zhou, R.G., Sun, Y.J. and Fan, P., 2015. Quantum image Gray-code and bit-plane scrambling. *Quantum Information Processing*, *14*(5), pp.1717-1734.
14. Gong, L.H., He, X.T., Cheng, S., Hua, T.X. and Zhou, N.R., 2016. Quantum image encryption algorithm based on quantum image XOR operations. *International Journal of Theoretical Physics*, *55*(7), pp.3234-3250.
15. Rohini, S. and Bairagi, V., 2010. Lossless medical image security. *Int J ApplEng Res, Dindigul*, *3*(1), pp.536-541.
16. Kaur, M. and Kaur, R., 2012. Reversible watermarking of medical images: Authentication and Recovery-A Survey. *Journal of Information and Operations Management*, *3*(1), p.241.
17. Kundu, M.K. and Das, S., 2010, August. Lossless ROI medical image watermarking technique with enhanced security and high payload embedding. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (pp. 1457-1460). IEEE.
18. Wu, Y., Noonan, J.P., Yang, G. and Jin, H., 2012. Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*, *21*(1), p.013014.
19. Wu, Y., Noonan, J.P., Yang, G. and Jin, H., 2012. Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*, *21*(1), p.013014.
20. Zear, A., Singh, A.K. and Kumar, P., 2018. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia Tools and Applications*, *77*(4), pp.4863-4882.
21. Huffman, D.A., 1952. A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, *40*(9), pp.1098-1101.
22. Wu, C.P. and Kuo, C.C., 2005. Design of integrated multimedia compression and encryption systems. *IEEE Transactions on Multimedia*, *7*(5), pp.828-839.
23. Özkaynak, F., Özer, A.B. and Yavuz, S., 2012, April. Analysis of chaotic methods for compression and encryption processes in data communication. In *Signal Processing and Communications Applications Conference (SIU), 2012 20th* (pp. 1-4). IEEE.
24. https://radiopaedia.org/cases/normal-upper-abdominal-ultrasound-male-adult-1
25. https://www.researchgate.net/figure/Chest-CT-scan-showing-multiple-pulmonary-nodules-in-both-lungs_fig1_49782121
26. https://www.slideshare.net/basselericsoussi/ultrasonography-fundamentals-in-critical-care-lung-ultrasound-pleural-ultrasound-other-potetial-utilities-of-ultrasound
27. https://www.dradamrennie.com/diagnostic-neuroradiology/ct-2/
28. https://en.wikipedia.org/wiki/Magnetic_resonance_imaging_of_the_brain
29. http://www.rad.msu.edu/course/Rad553/image_lib/body/BT21_d.htm
30. https://www.istockphoto.com/in/photos/hand-x-ray?assettype=image&sort=mostpopular&mediatype=photography&phrase=hand%20x%20ray
31. http://www.startradiology.com/internships/emergency-medicine/knee/x-knee/