WATERMARKING IN MEDICAL IMAGES BY USING DWT, DCT, DFT AND LSB ALGORITHMS

HASAN VOLKAN KAYA

JULY 2015

WATERMARKING IN MEDICAL IMAGES BY USING DWT, DCT, DFT and LSB ALGORITHMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES OF
ÇANKAYA UNIVERSITY

BY

HASAN VOLKAN KAYA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
COMPUTER ENGINEERING

JULY 2015

Title of the Thesis: **WATERMARKING IN MEDICAL IMAGES BY USING DWT, DCT, DFT and LSB ALGORITHMS**

Submitted by **Hasan Volkan KAYA**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr Müslim BOZYİĞİT
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Doç. Dr. Ersin ELBAŞI	Yrd. Doç. Dr. Abdül Kadir GÖRÜR
Co-Supervisor	Supervisor

Examination Date: 13.07.2015

Examining Committee Members

Yrd. Doç. Dr. Abdülkadir GÖRÜR	(Çankaya Univ.)	
Doç. Dr. Ersin ELBAŞI	(İpek Univ)	
Yrd. Doç. Dr. Reza Zare HASSANPOUR	(Çankaya Univ.)	
Doç. Dr. Hakan MARAŞ	(Çankaya Univ)	
Yrd. Doç. Dr. Bülent Gürsel EMİROĞLU	(Kırıkkale Univ)	

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name	:	Hasan Volkan KAYA
Signature	:	
Date	:	13.07.2015

ABSTRACT

WATERMARKING IN MEDICAL IMAGES BY USING DWT, DCT, DFT and LSB ALGORITHMS

KAYA, Hasan Volkan
M.Sc., Department of Computer Engineering
Supervisor: Yrd. Doç. Dr. Abülkadir GÖRÜR
Co-Supervisor: Doç.Dr. Ersin ELBAŞI

July 2015, 101 pages

Digital watermarking is a research area that is becoming increasingly common nowadays. Watermarking is performed by hiding a logo in the original image. In this thesis, logo images are embedded into the medical images (MRI) using DCT, DWT and DFT methods and various attacks are applied on the resulting images. After the attacks, the PSNR values of the attacked images are measured and the SR values of the recovered logo images are calculated. Moreover, using the LSB method, encrypted messages are embedded into the medical images. Then, by applying various attacks, the PSNR values and encrypted messages are extracted from these images. The main objectives of this study are to digitally watermark the medical images and compare the PSNR and SR values before and after the attacks on the images.

Keywords: Digital Watermarking, Peak Signal-to-Noise Ratio, Similarity Ratio, Discrete Wavelet Transform, Discrete Cosines Transform, Discrete Fourier Transform, Least Significant Bit.

ÖZ

DCT, DWT, DFT ve LSB ALGORİTMALARI KULLANILARAK MEDİKAL RESİMLERDE DİJİTAL DAMGALAMA

KAYA, Hasan Volkan
Yüksek lisans, Bilgisayar Mühendisliği Anabilim Dalı
Tez Yöneticisi: Yrd. Doç. Dr. Abülkadir GÖRÜR
Ortak Tez Yöneticisi: Doç.Dr. Ersin ELBAŞI

Temmuz 2015, 101 Sayfa

Dijital damgalama yöntemi son günlerde giderek yaygınlaşan bir araştırma konusudur. Damagalama orjinal resmin içine logo resmi gizlenerek yapılmaktadır. Bu tezde, medikal resimler üzerinde (MR) DCT, DWT ve DFT yöntemleri kullanılarak logo resmi gömülmüştür. Daha sonra bu resimlere çeşitli ataklar uygulanmıştır. Ataklardan sonra ise atak uygulanmış resimlerin PSNR değerleri ölçülmüştür ve atak sonrası geri çıkartılan logo resimleri üzerinde ise SR değerleri hesaplanmıştır. Ayrıca LSB yöntemi ile şifreli mesaj medical resimlerin içine gömülmüştür. Sonrasında ise ataklar uygulanarak bu resimlerin PSNR değerleri ile birlikte şifreli mesaji geri çıkartılma işlemi yapılmıştır. Çalışmanın temel amacı medikal resimler üzerinde damgalama işlemi ve saldırılardan sonraki PSNR ve SR değerlerini karşılaştırmaktır.

Anahtar Kelimeler: Dijital Damgalama, Yoğun Sinyal Gürültü Oranı, Benzerlik Oranı, Ayrık Dalgalı Dönüşüm, Ayrık Kosinüs Dönüşüm, Arık Fourier Dönüşüm, En Önemsiz Bit.

ACKNOWLEDGEMENTS

This project would not have been possible without the support of many people. Many thanks to my supervisor, Yrd. Doç. Dr. Abdülkadir GÖRÜR and, Dr. Ersin ELBAŞI (co-supervisor) who read my numerous revisions and helped make some sense of the confusion. Also thanks to my committee members Yrd. Doç. Dr. Reza Zare HASSANPOUR, who offered guidance and support. And finally, thanks to my wife, my family, and numerous friends who endured this long process with me, always offering support and love.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

FIGURES

FIGURES

FIGURES

FIGURES

FIGURES

FIGURES

FIGURES

FIGURES

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
DFT	Discrete Fourier Transform
DYWT	Dyadic Wavelet Transform
LSB	Least Significant Bit
PSNR	Peak Signal to Noise Ratio
SR	Similarity Ratio
SVD	Singular Value Decomposition
LU	Lower and Upper
RDM	Recursive Dither Modulation
IA	Interval Arithmetic
LL	Lower Low
LH	Lower High
HH	Higher High
HL	Higher Low
MSE	Mean Square Error
RSA	Rivest Shamir Adleman
ROI	Region of Interest
RONI	Region of Non Interest

CHAPTER 1

INTRODUCTION

Digital watermarks are bits of data added to digital information (audio, video, or images) that can be detected or extracted later to make an affirmation about the information. This data can be literary information about the creator, its copyright, and so on; or it can be an image itself. The data to be covered up is embedded by controlling the substance of the digital information, permitting somebody to recognize the first proprietor, or on account of unlawful duplication of bought material, the purchaser included. These digital watermarks stay in place under transmission/change, permitting us to secure our possession rights in digital structure.

Watermarks may be noticeable, in which case their utilization is two-fold to dishearten unapproved use, furthermore go about as a commercial. On the other hand, the emphasis is on invisible watermarks, as they don't create any debasement in the stylish quality or in the value of the information. They can be identified and extricated later to encourage a case of possession, yielding relevant information as well. Watermarks might likewise be delegated robust or fragile. Fragile watermarks are those that are easily destroyed by any attempt to tamper with them. Absence of a watermark in a previously watermarked document would lead to the conclusion that the data has been tampered with.

Three approaches to embed a watermark: compressed domain, spatial domain, and transform domain watermarking. Compressed domain watermarking uses only audio or video files. The spatial domain is modified pixel value to embed watermark in the original image. Least Significant Bits technique is an example of spatial domain to

embed the bits of message into the least significant bits plane of the cover image [1]. The transform domain likes to spatial domain, difference is a modifying coefficients with Discrete Fourier Transform, Discrete Wavelet Transform or Discrete Cosine Transform [2].

In this work medical images which are original images were used and attacked. Different methods are used to embed a watermark image into original images. These methods are Discrete Cosine Transform, Discrete Wavelet Transform, Discrete Fourier Transform and Least Significant Bit.

The main objective of this thesis is to compare the PSNR and SR values on different attacks and comparing PSNR and SR values after these attacks.

1.1 Previous Work and Objective of the Study

In literature many studies are made like this. Some of these references are summarized in the following sections.

JANE and ELBAŞI presented a study about combination of DWT and singular value decomposition (SVD) and lower and upper (LU) decomposition non-blind watermarking algorithm to detect watermark [3].

A.Kannammal and S. Subha Rani studied two level security for medical image using watermarking encryptions. Watermarking is performed by using new nontensor product wavelet filter banks, which can uncover singularities in different directions. The medical image is embedded into the LH sub band of the natural image. RSA, AES and RC4 algorithms which are performed for encryption [4].

A. Giakoumaki, S. Pavlopoulos, D. Koutsouris studied A medical image watermarking scheme based on wavelet transform The scheme embeds multiple watermarks serving different purposes: a robust watermark containing the doctor's digital signature for authentication, a caption watermark with patient's personal and examination related data, and a fragile watermark for the purpose of data integrity control [5].

To solve security of digital medical image problem MIAO et al. had a study about zero watermarking encryption algorithm based on the Arnold scrambling to

preprocess on original watermarking and DWT-DFT. To provide double protection for medical images their algorithm combines the image visual feature vector. [6]

Baiying Lei, Ee-Leng Tan, Siping Chen, Dong Ni, Tianfu Wang, Haijun Lei studied a new and reversible watermarking method is proposed to address this security issue. Specifically, signature information and textual data are inserted into the original medical images based on recursive dither modulation (RDM) algorithm after wavelet transform and singular value decomposition. [7]

Pritesh Pathak, S. Selvakumar studied the main issue in Blind Steganalysis is the non-availability of knowledge about the Steganographic technique applied to the image.

Feature extraction approaches best suited for Blind Steganalysis, either dealt with only a few features or single domain of an image. [8]

Teruya Minamoto. Ryuji Ohura, studied a new blind digital image watermarking method based on the dyadic wavelet transform (DYWT) and interval arithmetic (IA). Because the DYWT has a redundant representation, the amount of information that the watermark must contain is greater than inthe case of the methods based on the ordinary discrete wavelet transforms. [9]

1.2. Organization of Thesis

Watermark embedding and extracting algorithms, attacks on watermarked image for example, salt & pepper attack, Resize attack, Gaussian attack, histogram attack, intensity attack and so forth and assessment of watermarking procedures are clarified in the second chapter.

In the third chapter, used methodology and the experimental results are illustrated.

Conclusion of this work and Interpretation of results are explained in the fourth and fifth chapters.

CHAPTER 2

DIGITAL WATERMARKING

Digital Watermarking in a late years turns out to be more critical. Since watermark is a noteworthy innovation to protect copyright insurance. Multimedia object, for example, content, image and video can be embed original image by means of watermark methods. In the wake of embedding methodology can be separated the multimedia object from watermarked image. To secure multimedia can be encrypted image or video however when decrypted multimedia it doesn't promise to ensure copyright of image or video.

Digital watermarks are the electronic forms of their customary partner. Originally utilized as a part of the photography showcase as a method for distinguishing the copyright proprietor of digital photographs, digital watermarking is a method for embedding information into digital and simple substance keeping in mind the end goal to recognize its proprietor. The watermark turns into a changeless piece of the substance, even as it is dispersed to others.

The watermark must be either robust or fragile, contingent upon the application. By "robust", we mean the ability of the watermark to oppose controls of the media, for example, lossy pressure (where compressing information and after that decompressing it recovers information that may well be not quite the same as the original, however is sufficiently close to be valuable somehow), scaling, and cropping, among others. At times, the watermark may should be fragile. "Fragile" implies that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

In digital watermarking, visible watermark can be seen by eyes, other hand invisible watermarked image can't visible. Invisible watermarked image is generally utilized

for security. To identify watermark if original image is utilized, is non-blind watermarking. In the event that original image is not obliged, this is blind watermarking. Semi-blind watermark obliges seed and watermarked document to distinguish the watermark.

2.1. Watermarking Methods

- **Discrete Wavelet Transform:** DWT divides into four sub bands. These sub bands are LL, LH, HL, HH. The magnitudes of DWT coefficients are larger in the lowest bands (LL) at each level of decomposition. Embedding watermark in larger amount of sub bands (HL, LH, HH) give productive robustness of watermark. But the image quality can decrease which can be measured by PSNR. The wavelet transform is similar to the Fourier transform (or much more to the windowed Fourier transform) with a completely different merit function. The main difference is this: Fourier transform decomposes the signal into sines and cosines, i.e. the functions localized in Fourier space; in contrary the wavelet transform uses functions that are localized in both the real and Fourier space. [11], [12], [13] Generally, the wavelet transform can be expressed by the following equation:

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\, \psi^*_{(a,b)}(x)\, \mathrm{d}x$$

- **Discrete Cosine Transform:** DCT divides image into different frequency bands. The frequency components are ordered in a sequential order such as low frequency, mid frequency, and high frequency components. If most of the high frequency coefficients are zero, then they represent a smooth block. Discrete Cosine Transform (DCT) attempts to decorrelate the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency (Syed Ali Khayam et al 2003) The following equation:

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

- **Discrete Fourier Transform:** This approach first extracts the components of the image to be watermarked, computing its full frame DFT, and then taking the magnitudes of the coefficients. Fourier Transform for signals known only at instants separated by sample times *T.* This approach first extracts the components of the image to be watermarked, computing its full frame DFT, and then taking the magnitudes of the coefficients. Given a sequence of N samples f(n), indexed by n = 0..N-1, the Discrete Fourier Transform (DFT) is defined as F(k), where k=0..N-1:

$$F(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} f(n)\, e^{-j2\pi kn/N}$$

- **Least Significant Bit**

The most common method of watermark embedding is to to embed the watermark into the least significant-bits of the cover object [14]. Despite being a simple method, LSB substitution suffers from many drawbacks. Although it can survive transformations like cropping, any addition of undesirable noise or lossy compression but a more sophesticated attack thatcould simply set the LSB bits of each pixel to one can fully defeat the Watermark with negligible impact on the cover object.Once the algorithm is known to a hacker, the embedded watermark could be easily modified by him without any difficulty. [15]

2.2. Attacks on Watermarked Image

One of the important issues watermark image should be robust against type of attacks. These attacks are as geometric, statistical and direct or indirect attacks. Some type of attacks can be defined below:

Gaussian Attack: Gaussian attack is a signal processing attack that should detect watermark after signal processing.

Jpeg Compression Attack: JPEG compression attack could degrade the data's quality through irretrievable loss of data.

Rotation Attack: Rotation is a geometric attack. Change the rotation of the image clockwise or counter clockwise with an angle.

Intensity Adjustment Attack: Intensity adjustment attack maps the intensity values in grayscale image to new values in low and high intensities.

Noise (Pepper & Salt) Attack: Adding salt and pepper noise to the image with noise density.

Speckle Noise Attack: Adding multiplicative noise to the image with uniformly distributed random noise with mean and variance.

Gamma Correction Attack: Gamma correction is used to adjust for color difference that is same image displayed on two different workstations might look different colors due to differences in the display monitor.

Evaluation of Watermarking

Image quality estimation is a challenging issue in numerous applications to attacks. Images' target measures are mean square error, peak signal to noise ratio and similarity ratio.

- **Mean Square Error**: MSE is a control and quality measurement. The MSE is characterized as below

$$MSE = \frac{1}{M * N} \sum_i \sum_j [A(i,j) - W(i,j)]^2$$

Where A(i, j) is the original image and W(i, j) is the watermark that includes M x N pixels.

- **Peak Signal to Noise Ratio**: The PSNR is used as a measurement of quality of recreation in image watermarking. It is a ratio among the maximum signal value and background noise's magnitude.

$$PSNR = 20 * \log(\frac{255}{\sqrt{MSE}})$$

- **Similarity Ratio**: SR is used for assessment of non-blind watermark extraction. SR delivers high accuracy to binary image watermarks. At this point when different pixel values converge to 0, SR is going to be near to 1 which is the ideal optimum and preferred condition. SR is characterized as follows

$$SR = {}^{S}/_{(S+D)}$$

Where S and D denote the quantity of matching pixel values in analyzed images and the quantity of different pixel values in compared images separately.

CHAPTER 3

METHODOLOGY

Watermark embedding and extract processes were realized with this thesis. While watermark processes are applied, different methods are used which are DCT, DFT, DWT and LSB algorithms.

By using Matlab PSNR values of Watermarked and Original images have been calculated. After performing many attacks were applied to Watermarked image and then at this time PSNR values of attacked Watermarked images were measured and both PSNR values were compared. Many image attacks were done on the watermarked image. They are called “Scaling, Gaussian Attacks”, “Decoding Attacks”, “Histogram Equalization Attacks”, ” JPEG Compression Attacks”, “Rotation Attacks”, “Filter Attacks”, ”Intensity Adjustment Attacks”, “Gamma correction Attacks”, “Noise Attack Pepper & Salt”, “Speckle Noise Attacks”.

Also, SR values of embedded watermark image of original image were evaluated and compared. Brain-MRI, Breast-MRI and Neck-MRI medical images were used in this thesis.

Also, with LSB method the text message was embedded into original image as encrypted by doing RSA encryption. After that again the attacks were applied to watermarked image and again the PSNR values of attacked images were calculated. In addition this, the encrypted message which were embedded into attacked images was decrypted and the results were observed.

3.1. Discrete Wavelet Transform

Original image which is 1115 x 2173 pixels and 24 bit depth is used for watermark experiments

Figure 1 MR Image

Figure 2 Watermarked Image

Figure 3 Watermark Image

Figure 4 Watermark Image 2

11 different attacks are used in this experience by using MATLAB. They are “Filter attack, Gamma attack, Gaussian attack, Histogram equalization attacks, Imnoise attack, rotate attack, Jpeg compression, salt & pepper and speckle noise attacks”.

Watermark embedding process is done by DWT. In this process, watermark images are embedded into LL, LH, HL and HH bands (Figure 3 Watermark Image, Figure 4 Watermark Image 2). After that the attacks, which are mentioned in the above, are applied to watermarked image. (Figure 2 Watermarked Image). Then, the extract process is done.

The images that are applied attack are shown in the following:

Figure 5 Filter Attack

Figure 6 Cropping Attack

Figure 7 Histogram Attack

Figure 8 Gamma Attack

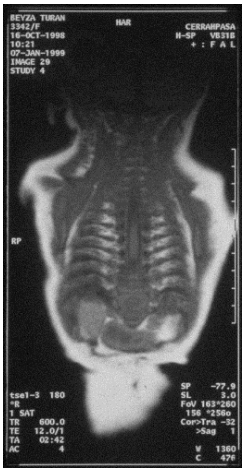


Figure 9 Gaussian Attack

Figure 10 Rotate Attack

Figure 11 Pepper Attack

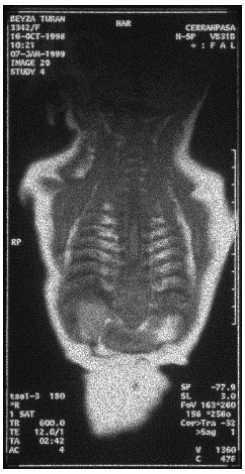


Figure 12 Speckle Attack

Figure 13 Intensity Attack

Figure 14 Jpeg (75) Attack

Figure 15 Jpeg (50) Attack

With this experience, the quality of watermark image that is created again is measured by using PSNR algorithm to decide image quality. Similarity ratio of watermark image is evaluated by using SR.

Figure 16 shows that original image and attacked image for Gaussian attack and Figure 17 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Gaussian Attack = 29,62778

Figure 16 *PSNR values original and Gaussian attack images*

SR gaussian attack = 0,6925

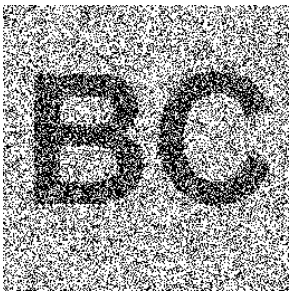


Figure 17 SR value of watermarked image after Gaussian attack

Figure 18 shows that original image and attacked image for Filter attack and Figure 19 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Filter Attack = 42,256476

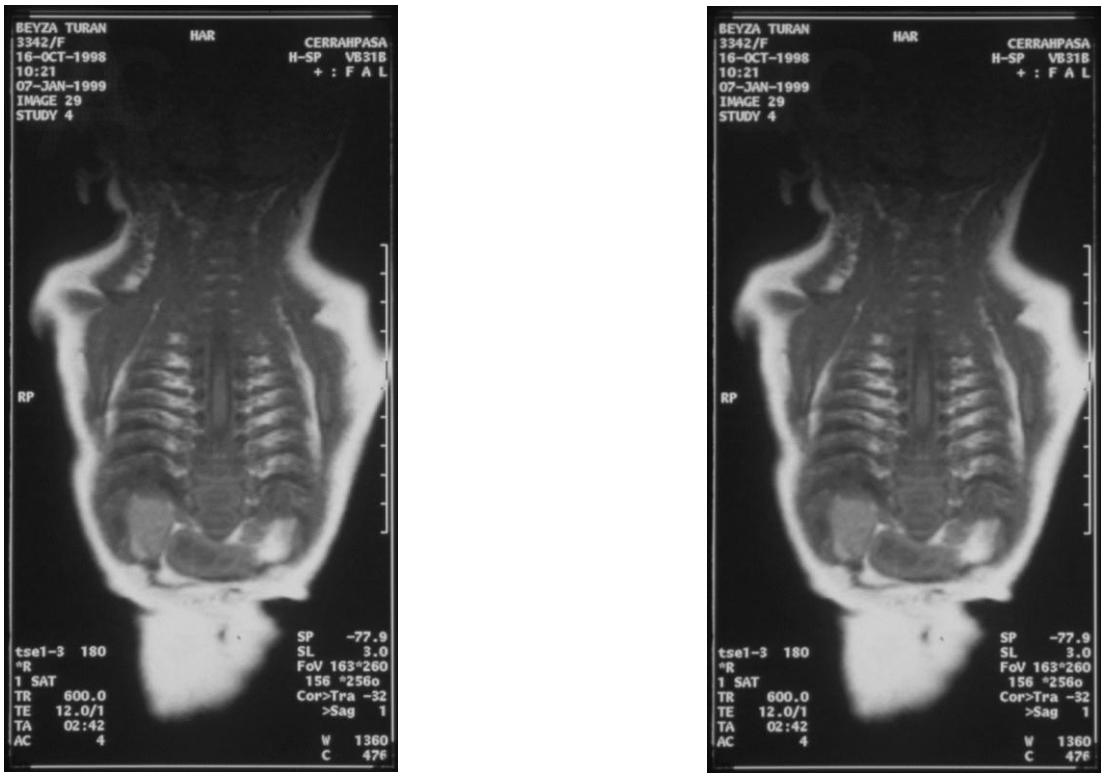


Figure 18 PSNR values original and filter attack images

SR filter attack = 0,9429

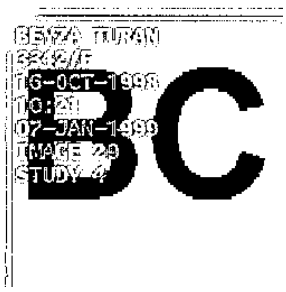


Figure 19 SR value of watermarked image after filter attack

Figure 20 shows that original image and attacked image for Gamma attack and Figure 21 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Gamma Attack = 17,217422

Figure 20 PSNR values original and gamma attack images

SR gamma attack = 0,9289

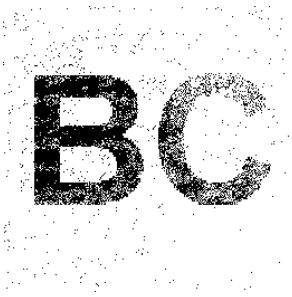


Figure 21 SR value of watermarked image after gamma attack

Figure 22 shows that original image and attacked image for rotate attack and Figure 23 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Rotate Attack = 10,408897

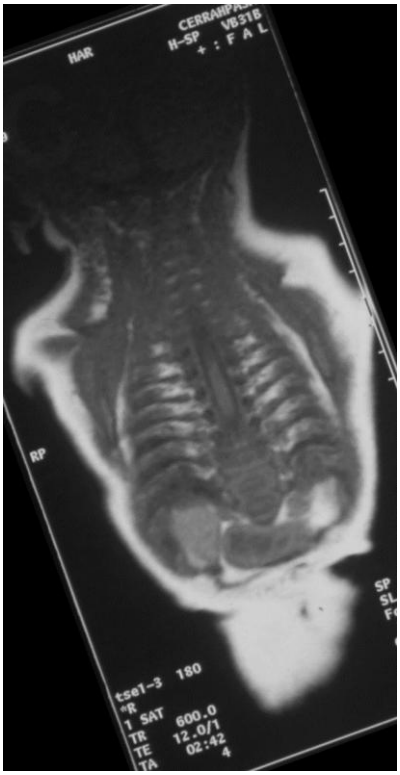


Figure 22 PSNR values original and rotate attack images

SR rotate attack = 0,8806

Figure 23 SR value of watermarked image after rotate attack

Figure 24 shows that original image and attacked image for Histogram attack and Figure 25 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Hist. Attack = 12,154761

Figure 24 PSNR values original and Histogram attack images

SR histogram attack = 0,4546

Figure 25 SR value of watermarked image after histogram attack

Figure 26 shows that original image and attacked image for Cropping attack and Figure 27 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Cropping. Attack = 27,25297

Figure 26 PSNR values original and cropping attack images

SR cropping attack = 0,9520

Figure 27 SR value of watermarked image after cropping attack

Figure 28 shows that original image and attacked image for Intensity attack and Figure 29 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Intensity. Attack = 20,9342

Figure 28 PSNR values original and intensity attack images

SR intensity attack = 0,9956

Figure 29 SR value of watermarked image after intensity attack

Figure 30 shows that original image and attacked image for Speckle attack and Figure 31 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Speckle. Attack = 22,88850

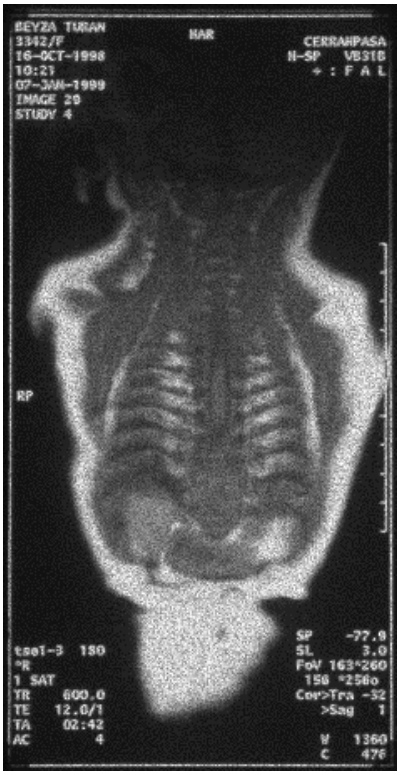


Figure 30 PSNR values original and Speckle attack images

SR Speckle Attack = 0,28330

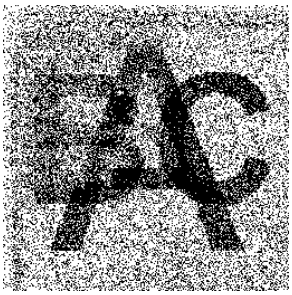


Figure 31 SR value of watermarked image after speckle attack

Figure 32 shows that original image and attacked image for Salt & Pepper attack and Figure 33 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Salt&Pepper Attack = 21,646320

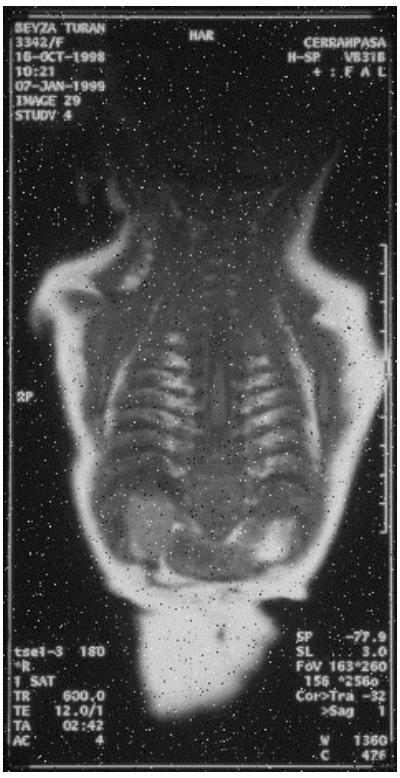


Figure 32 PSNR values original and Salt & Pepper attack images

SR Salt & Pepper Attack = 0,164000

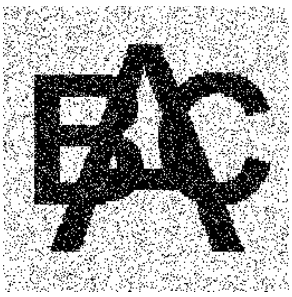


Figure 33 SR value of watermarked image after salt & pepper attack

Figure 34 shows that original image and attacked image for Jpeg (75) attack and Figure 35 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Jpeg(75) Attack = 43,8200

Figure 34 PSNR values original and Jpeg (75) attack images

SR Jpeg(75) attack = 0,9869

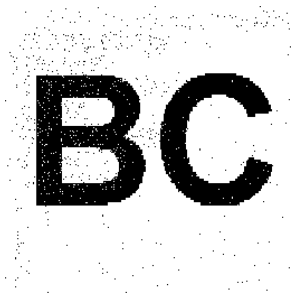


Figure 35 SR value of watermarked image after Jpeg (75) attack

Figure 36 shows that original image and attacked image for Jpeg (50) attack and Figure 37 show that SR value of attacked image

PSNR value = 46,756416

PSNR value after Jpeg(50) Attack = 41,9413

Figure 36 PSNR values original and Jpeg (50) attack images

SR Jpeg(50) Attack = 0,9442

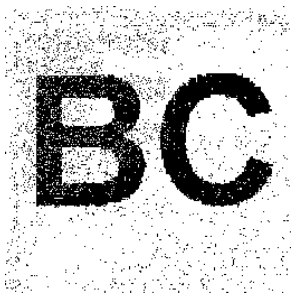


Figure 37 SR value of watermarked image after Jpeg (50) attack

Table 1 PSNR and SR values after attacks

Attacks	PSNR	PSNR values after attacks	SR
Cropping	46,756416	27,252977	0,9520
Gaussian	46,756416	29,627788	0,6925
Filter	46,756416	42,256476	0,9429
Rotate	46,756416	10,408897	0,8806
Gamma	46,756416	17,217422	0,9289
Histogram	46,756416	12,154761	0,4546
Salt&Pepper	46,756416	21,646320	0,1640
Speckle noise	46,756416	22,888509	0,2833
Jpeg(75)	46,756416	43,820000	0,9869
Jpeg(50)	46,756416	41,941300	0,9442
Intensity	46,756416	20,934200	0,9956

Table 1 summarizes PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. If PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For example PSNR value is 46,756416 before Filter attack and after Filter attack the PSNR value became 42,256476, meaning PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. The SR method compares pixel values of two watermark images. This values are between 0 and 1. If SR values close to 1, it means that recovered watermark image is in ideal optimum and preferred condition. Histogram, Salt & Pepper and Speckle attacks' SR values are not good because they have the nearest values to 0. Other attack types' SR values are nearest to 1, as you can see in table 1. Best PSNR values are in Filter, Jpeg (50) and JPEG (75) attacks. Rotate attack has the worst PSNR value.

In Figure 38 Original Image (Brain-MRI) by using Discrete Wavelet Transform, the embedding process of watermark images is done. PSNR and SR values are calculated for watermark embedded images (Figure 41 Watermarked Image).

Figure 38 Original Image

Figure 39 Watermark Image

Figure 40 Watermark Image

Figure 41 Watermarked Image

The images that are applied attack are shown in the following:

Figure 42 Gamma Attack

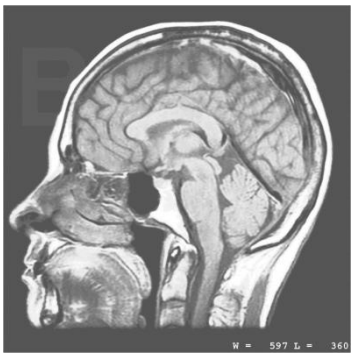


Figure 43 Histogram Attack

Figure 44 Intensity Attack

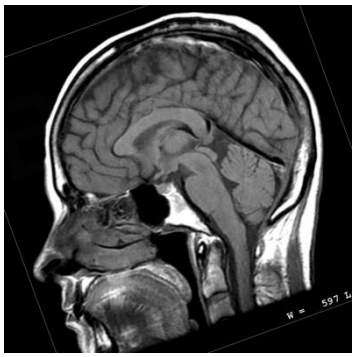


Figure 45 Rotate Attack

Figure *46* Filter Attack

Figure 47 Resize Attack

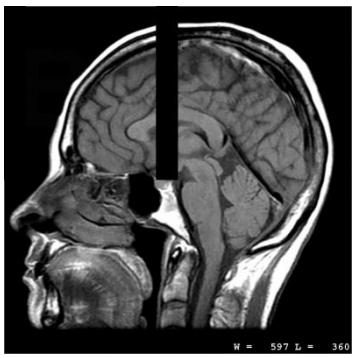


Figure 48 Cropping Attack

Figure 49 Gaussian Attack

Figure 50 Jpeg(75) Attack

Figure 51 Jpeg(50) Attack

Figure 52 shows that original image and attacked image for Gamma attack and Figure 53 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Gamma Attack = 20,154851

Figure *52* PSNR values original and Gamma attack images

SR gamma attack = 0,8774

Figure 53 SR value of watermarked image after gamma attack

Figure 54 shows that original image and attacked image for Histogram attack and Figure 55 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Histogram Attack = 10,0353

Figure 54 PSNR values original and Histogram attack images

SR histogram attack = 0,8813

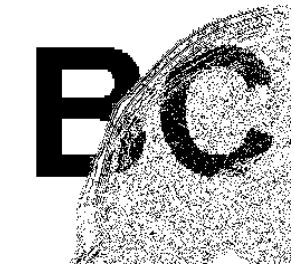


Figure 55 SR value of watermarked image after Histogram attack

Figure 56 shows that original image and attacked image for Intensity attack and Figure 57 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Intensity Attack = 22,583412

Figure 56 PSNR values original and Intensity attack images

SR intensity attack = 0,9824

Figure 57 SR value of watermarked image after Intensity attack

Figure 58 shows that original image and attacked image for rotate attack and Figure 59 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Rotate Attack = 10,357190

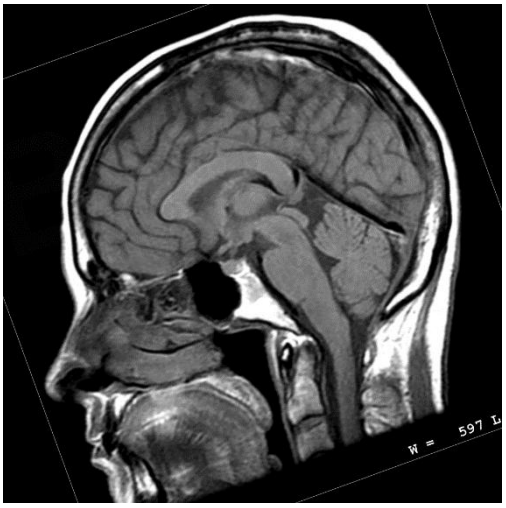


Figure 58 PSNR values original and rotate attack images

SR intensity attack = 0, 9685

Figure 59 SR value of watermarked image after rotate attack

Figure 60 shows that original image and attacked image for Filter attack and Figure 61 show that SR value of attacked image.

PSNR value = 44,660772

PSNR value after Filter Attack = 28,933958

Figure 60 PSNR values original and Filter attack images

SR filter attack = 0,9609

Figure 61 SR value of watermarked image after filter attack

Figure 62 shows that original image and attacked image for Resize attack and Figure 63 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Resize Attack = 30,0445

Figure 62 PSNR values original and Resize attack images

SR resize attack = 0,9028

Figure 63 SR value of watermarked image after resize attack

Figure 64 shows that original image and attacked image for Gaussian attack and Figure 65 show that SR value of attacked image.

PSNR value = 44,660772

PSNR value after Gaussian Attack = 31,01152

Figure 64 PSNR values original and Gaussian attack images

SR gaussian attack = 0,8774

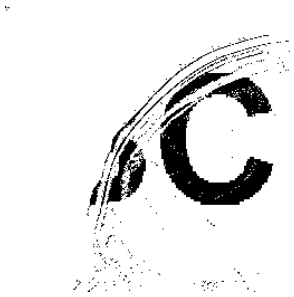


Figure 65 SR value of watermarked image after Gaussian attack

Figure 66 shows that original image and attacked image for Cropping attack and Figure 67 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Cropping Attack = 23,14363

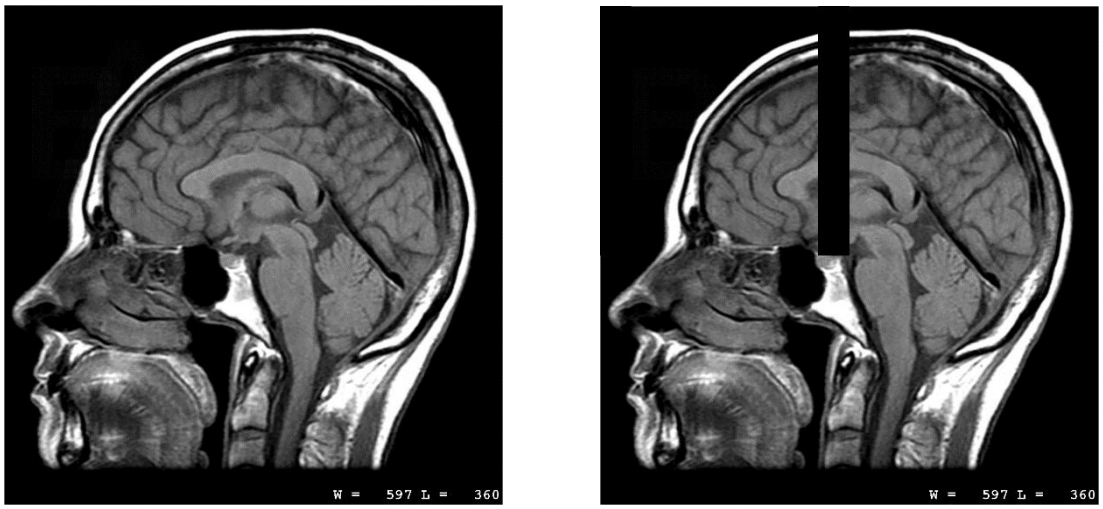


Figure 66 PSNR values original and Cropping attack images

SR cropping attack = 0,9799

Figure 67 SR value of watermarked image after cropping attack

Figure 68 shows that original image and attacked image for Jpeg (75) attack and Figure 69 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Jpeg(75) Attack = 44,2701

Figure 68 PSNR value original and after Jpeg (75) attack

SR Jpeg(75) attack = 0,9840

Figure 69 SR value of watermarked image after jpeg (75) attack

Figure 70 shows that original image and attacked image for Jpeg (50) attack and Figure 71 show that SR value of attacked image

PSNR value = 44,660772

PSNR value after Jpeg(50) Attack = 41,7065

Figure 70 PSNR values original and Jpeg (50) attack images

SR Jpeg(50) attack = 0,9315

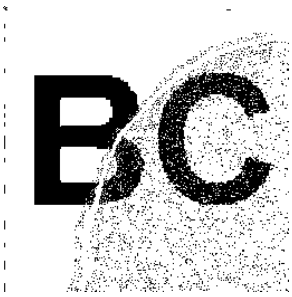


Figure 71 SR value of watermarked image after jpeg (50) attack

Table 2 PSNR and SR values after attacks

Attacks	PSNR	PSNR values after attacks	SR
Cropping	44,660772	23,14363	0,9799
Gaussian	44,660772	31,01152	0,8774
Filter	44,660772	28,933958	0,9609
Rotate	44,660772	10,357190	0,9685
Gamma	44,660772	*20,154851*	0,8774
Histogram	44,660772	*10,035300*	0,8813
Imnoise attack	44,660772	21,646320	0,1640
Speckle noise	44,660772	22,888509	0,2833
Jpeg(75)	44,660772	44,270100	0,9869
Jpeg(50)	44,660772	41,706500	0,9315
Resize	44,660772	30,044500	0,9028
Intensity	44,660772	22,583412	0,9824

Table 2 PSNR shows that PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. If PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For example PSNR value is 44,660772 before Jpeg (75) attack. After Jpeg (75) attack the PSNR value is 44,270100 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. The SR method compares pixel values of two watermark images. This values are between 0 and 1. If SR values close to 1, it means that recovered watermark image is in ideal optimum and preferred condition. Imnoise and Speckle attacks' SR values are not good because they have the nearest values to 0. Other attack types' SR values are nearest to 1, as you can see in table 2. Best PSNR values are in Gaussian, Jpeg (50) and JPEG (75) attacks. Histogram attack has the worst PSNR value.

If we compare Table 1 and Table 2 PSNR values are nearly same for original images. For attacked images for example after Filter attack Table 1 PSNR value is better than Table 2 PSNR values. But most of PSNR values after attack are closer. And SR values are also nearly same and closer to 1 except Speckle Noise, Salt & Pepper and Histogram attacks after SR values.

3.2. Discrete Cosine Transform

Figure 72 MR Image

Figure 73 Watermarked Image

Figure 74 Watermark Image

10 different attacks are used in this experience by using MATLAB. They are “Filter attack, Scaling attack, Intensity attack, Gamma attack, Gaussian attack, Histogram equalization attacks, Imnoise attack, rotate attack and speckle noise attacks”.

Watermark embedding process is done by DCT. Watermark images (Figure 74 Watermark Image) are created by embedding process. After that the attacks, which are mentioned in the above, are applied to watermarked image. Then, the extract process is done.

The images that are applied attack are shown in Figure 75 Noise Attack – Figure 84 Gaussian

Figure 75 Noise Attack

Figure 76 Cropping Attack

Figure 77 Histogram Attack

Figure 78 Filter Attack

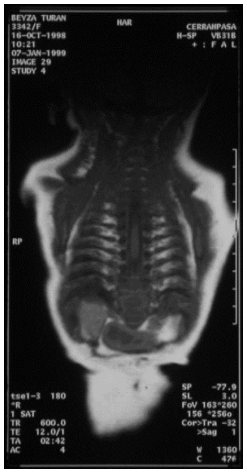


Figure 79 Gamma Attack

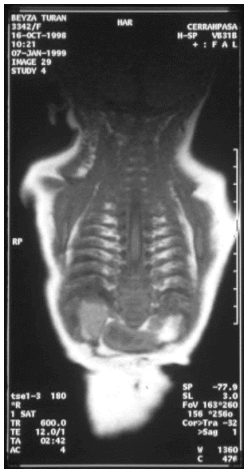


Figure 80 Intensity Attack

Figure 81 Scaling Attack

Figure 82 Rotate Attack

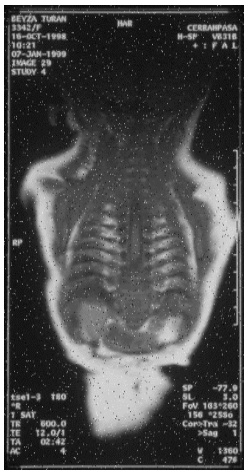


Figure 83 Salt&Pepper Attack

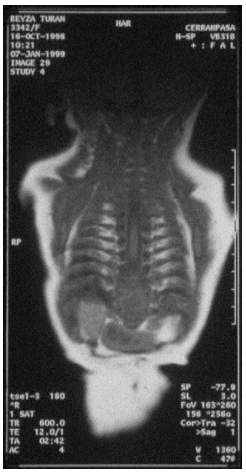


Figure 84 Gaussian Attack

In this work to measure for images quality were calculated PSNR values which is used as quality of reconstruction in watermark image and attacked images. Similarity ratio was calculated watermark image and extracted watermark image.

Figure 85 shows that original image and attacked image for Cropping attack and Figure 86 show that SR value of attacked image

PSNR value = 35,649740 PSNR value after Cropping. Attack = 14,80300

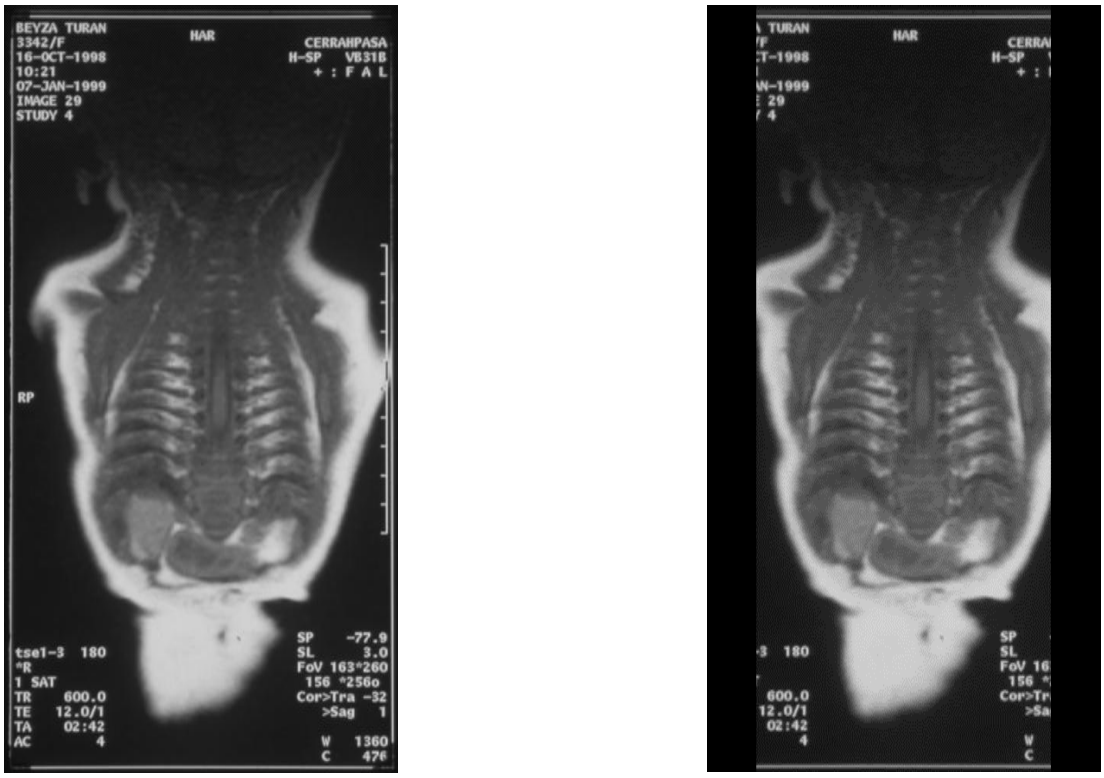


Figure 85 PSNR values original and cropping attack images

SR cropping attack = 0,6787

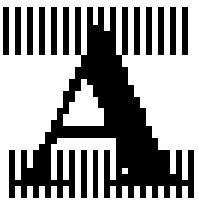


Figure 86 SR value of watermarked image after cropping attack

Figure 87 shows that original image and attacked image for Histogram attack and Figure 88 show that SR value of attacked image

PSNR value = 35,649740

PSNR value after Hist. Attack = 12,186193

Figure 87 PSNR values original and Histogram attack images

SR Histogram attack = 0,8848

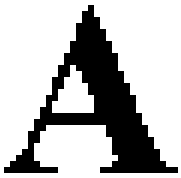


Figure 88 *SR value of watermarked image after Histogram attack*

Figure 89 shows that original image and attacked image for Filter attack and Figure 90 show that SR value of attacked image

PSNR value = 35,649740

PSNR value after Filter Attack = 29,244117

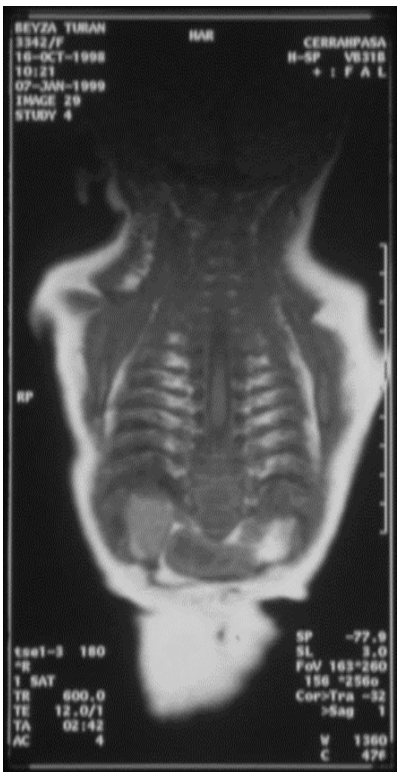


Figure 89 PSNR values original and Filter attack images

SR Filter attack = 0.8848

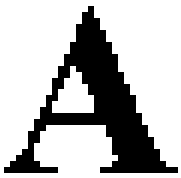


Figure 90 *SR value of watermarked image after Filter attack*

Figure 91 shows that original image and attacked image for Gamma attack and Figure 92 show that SR value of attacked image

PSNR value =35,649740

PSNR value after Intensity Attack = 20,938350

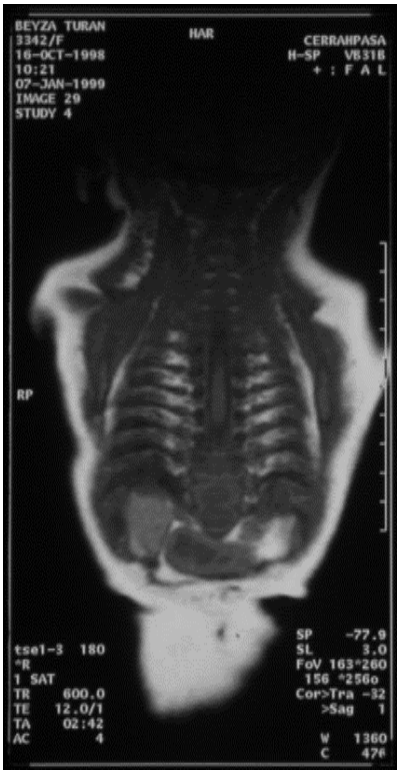


Figure 91 PSNR values original and Gamma attack images

SR Gamma attack = 0,8848

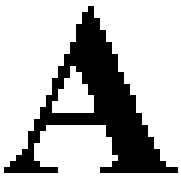


Figure 92 SR value of watermarked image after Filter attack

Figure 93 shows that original image and attacked image for Intensity attack and Figure 94 show that SR value of attacked image

PSNR value =35,649740

PSNR value after Intensity Attack = 20,938350

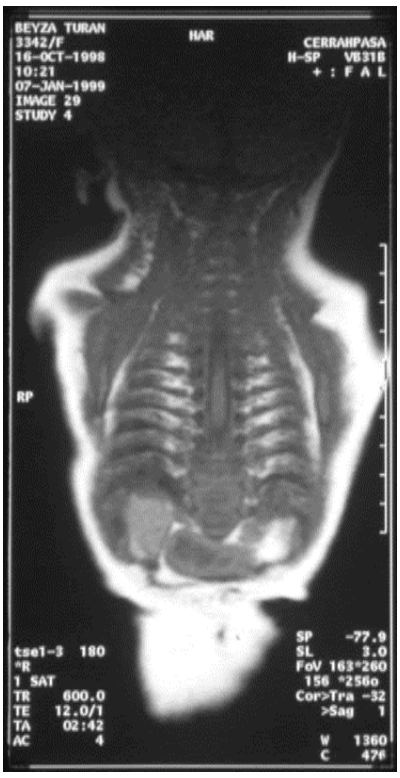


Figure 93 PSNR values original and Intensity attack images

SR Intensity attack = 0,8848

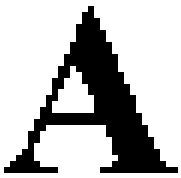


Figure 94 SR value of watermarked image after Intensity attack

Figure 95 shows that original image and attacked image for rotate attack and Figure 96 show that SR value of attacked image

PSNR value =35,649740

PSNR value after Rotate Attack = 11,177377

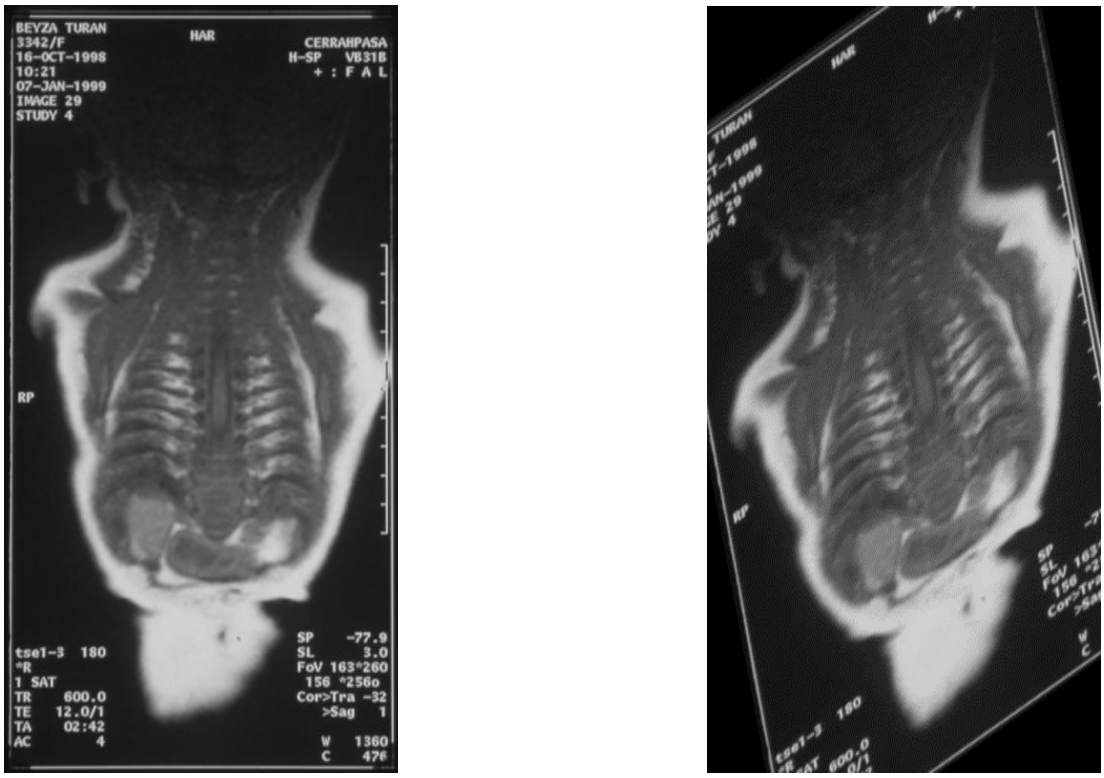


Figure 95 PSNR values original and rotate attack images

SR Rotate attack = 0,4092

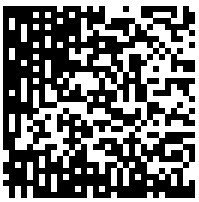


Figure 96 SR value of watermarked image after rotate attack

Figure 97 shows that original image and attacked image for Gaussian attack and Figure 98 show that SR value of attacked image

PSNR value = 35,649740 PSNR value after Gaussian Attack = 29,37244

Figure 97 PSNR values original and Gaussian attack images

SR Gaussian attack = 0,8848

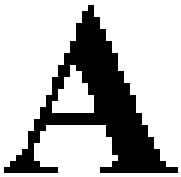


Figure 98 SR value of watermarked image after Gaussian attack

Figure 99 shows that original image and attacked image for Speckle Noise attack and Figure 100 show that SR value of attacked image

PSNR value = 35,649740

PSNR value after Speckle Attack = 22,902788

Figure 99 PSNR values original and Speckle Noise attack images

SR Speckle Noise attack = 0,8838

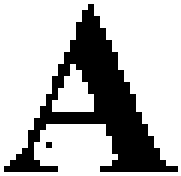


Figure 100 SR value of watermarked image after Speckle Noise attack

Figure 101 shows that original image and attacked image for Salt & Pepper attack and Figure 102 show that SR value of attacked image

PSNR value = 35,649740 PSNR value after Salt&Pepper Attack = 21,65746

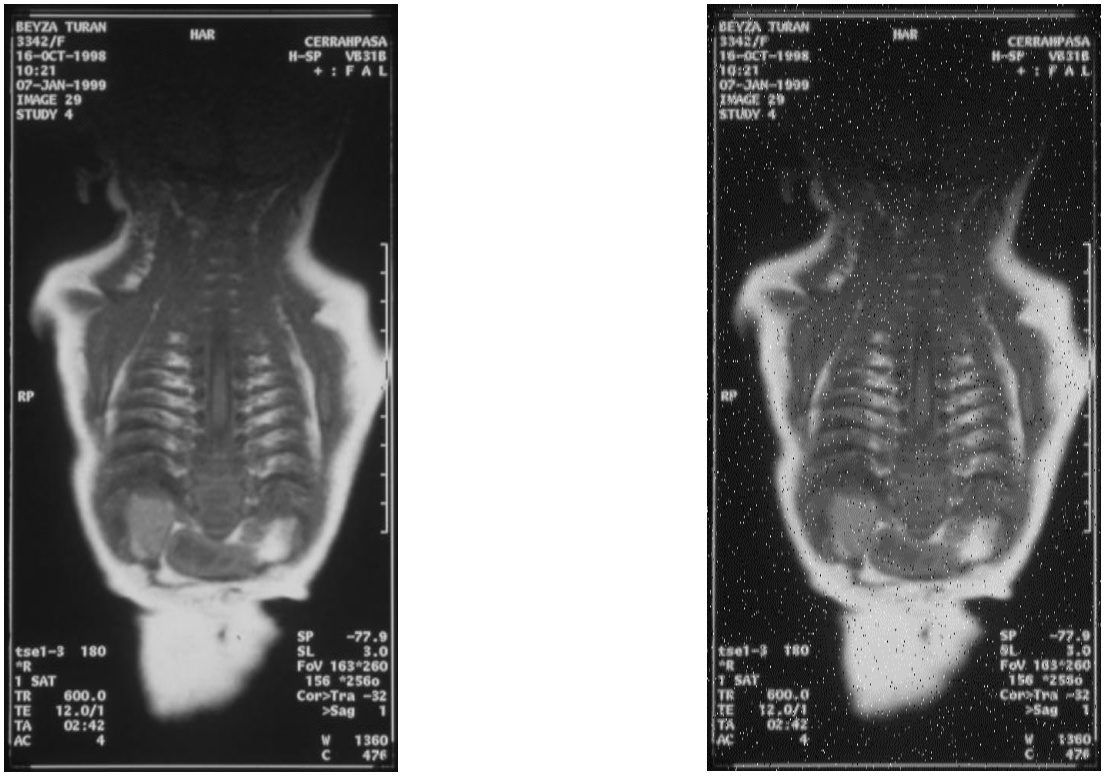


Figure 101 PSNR values original and Salt & Pepper Noise attack images

SR Salt & Pepper Noise attack = 0,6181

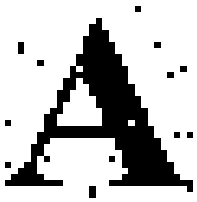


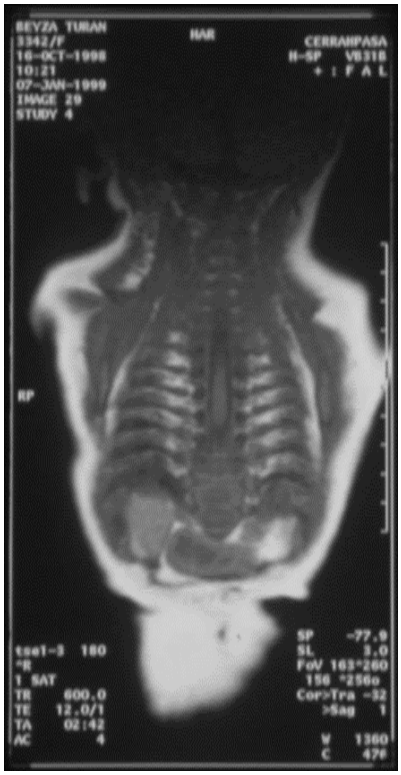
Figure 102 SR value of watermarked image after Salt & Pepper Noise attack

Attacks	PSNR	PSNR values after attacks	SR
Cropping	35,649740	14,803008	0,6787
Gaussian	35,649740	29,372440	0,8848
Filter	35,649740	29,244117	0,8848
Rotate	35,649740	11,177377	0,4092
Gamma	35,649740	17,781681	0,8848
Histogram	35,649740	12,186193	0,8848
Intensity	35,649740	20,938350	0,8848
Salt & Pepper	35,649740	21,657467	0,6181
speckle noise	35,649740	22,902788	0,8838

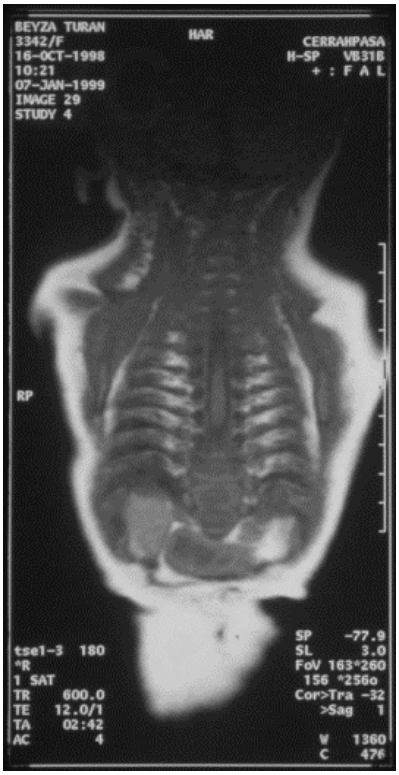
Table 3 PSNR and SR values after attacks

Table 3 *PSNR* demonstrates that PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. In the event that PSNR values are higher, it demonstrates to us vastly improved quality of the compressed or reconstructed image. On the off chance that PSNR worth is vastness, it implies that two images are indistinguishably same and at this reason PSNR quality result is infinity. For instance PSNR value is 35,649740 before Gamma attack. After Gamma attack the PSNR value is 17,781681 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. The SR method compares pixel values of two watermark images. This values are between 0 and 1. If SR values close to 1, it means that recovered watermark image is in ideal optimum and preferred condition. Rotate attack SR value is not good because they have the nearest values to 0. Other attack types' SR values are nearest to 1, as you can see in table 3. Best PSNR values are in Gaussian and Filter attacks. Rotate attack has the worst PSNR value.

Filter Attack (DCT) PSNR value =29,244117



Filter Attack (DWT) PSNR value =42, 256476



When we compare above two images PSNR values is better than the image which is applied DCT algorithm. After attacks (Filter Attack) when we calculates PSNR value for each images, the image which is applied DWT algorithm and attacked PSNR value is better than other image that is applied DCT algorithm and attacked. And SR values are nearly same and close to 1 value.

In Figure 103 Original Image (Breast) (Breast-MRI) by using Discrete Cosine Transform, the embedding process of watermark images is done. PSNR and SR values are calculated for watermark embedded images (Figure 104 Watermarked Image (Breast))

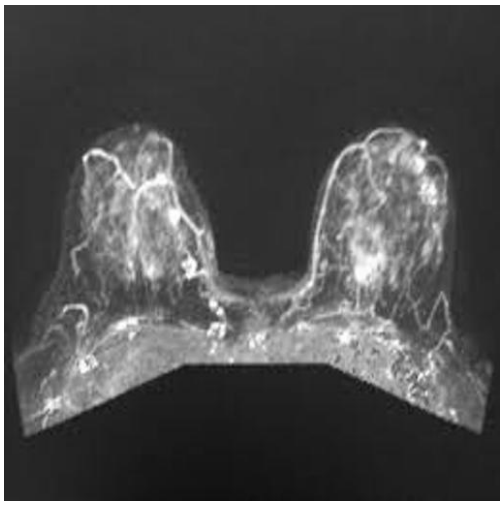


Figure 103 Original Image (Breast)

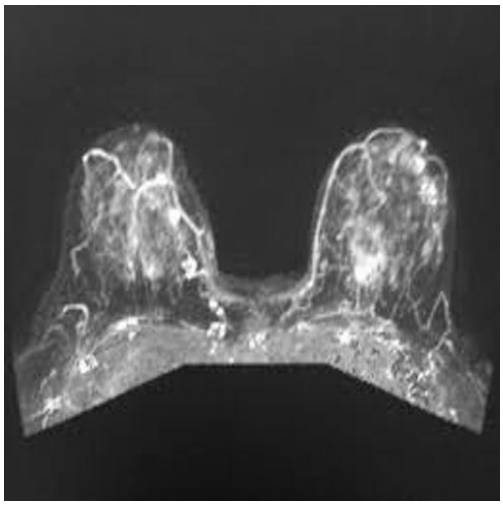


Figure 104 Watermarked Image (Breast)

Figure 105 Watermark Image

The images that are applied attack are shown **Figure 106** Cropping – Attack **Figure 117** Jpeg(50)

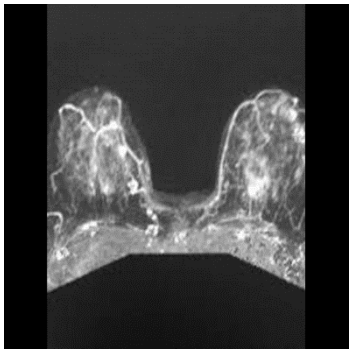
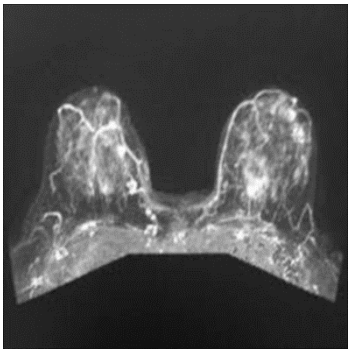
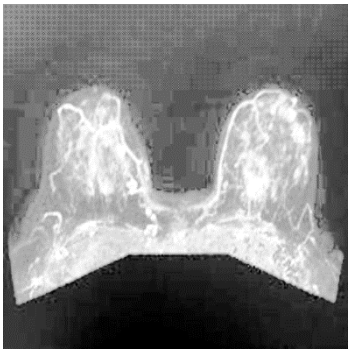




Figure 106 Cropping Attack **Figure 107** Filter Attack **Figure 108** Histogram Attack

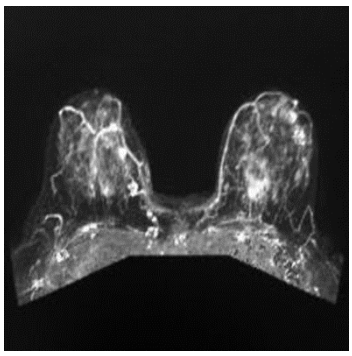
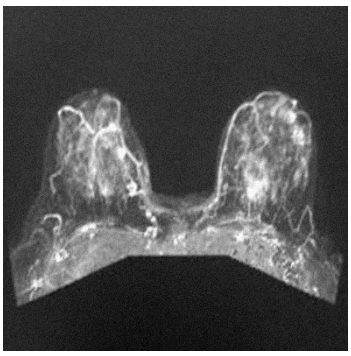
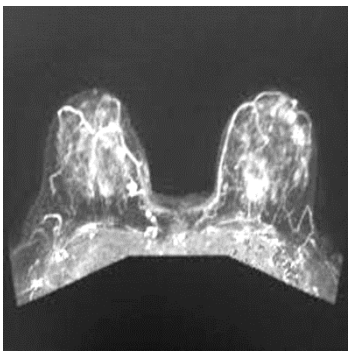




Figure 109 Gamma Attack **Figure 110** Gaussian Attack **Figure 111** Intensity Attack

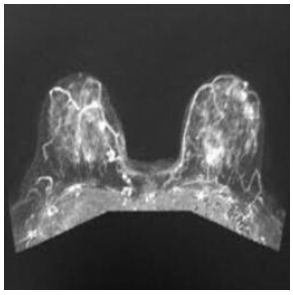
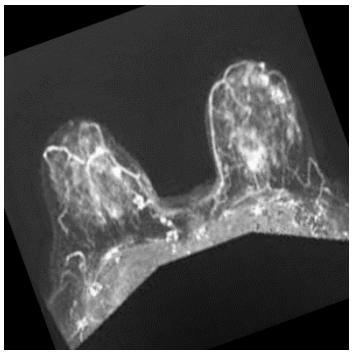
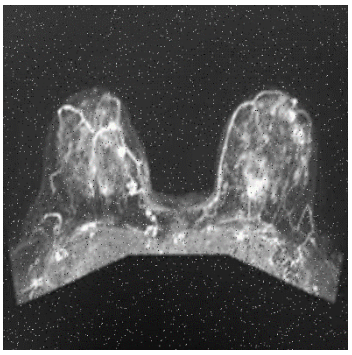




Figure 112 Resize Attack **Figure 113** Rotate Attack **Figure 114** Salt&Pepper Attack

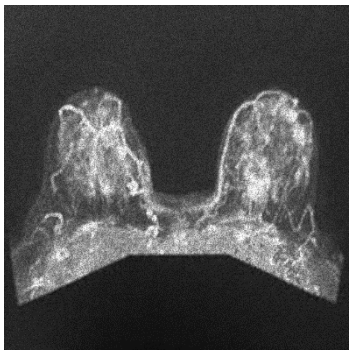
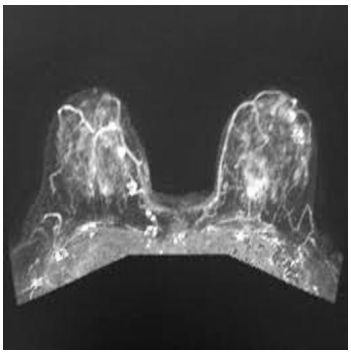
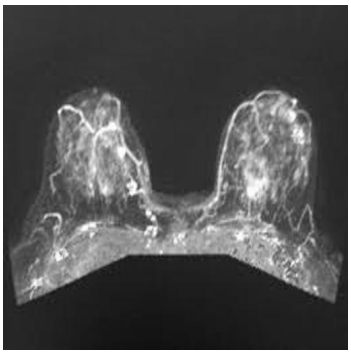




Figure 115 Speckle Attack **Figure 116** Jpeg (75) Attack **Figure 117** Jpeg(50) Attack

PSNR value watermarked images = 37, 5363

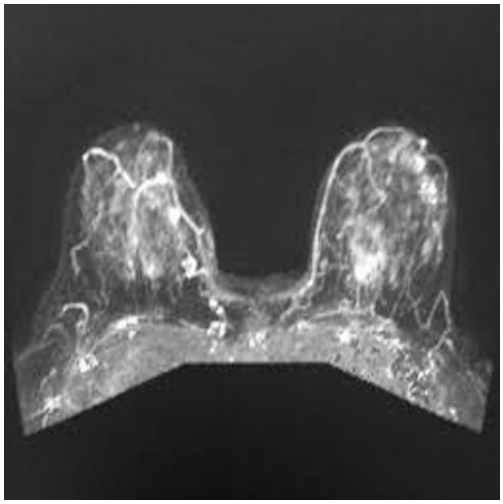


Figure 118 PSNR values original and Watermarked images

Figure 119 shows that original image and attacked image for Cropping attack and Figure 120 show that SR value of attacked image

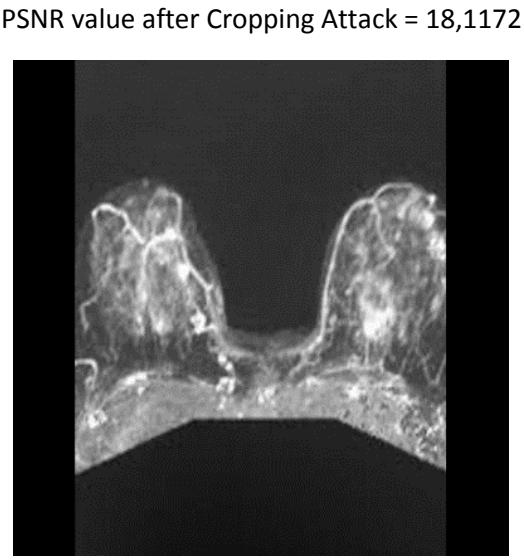


Figure 119 PSNR values Cropping attack images

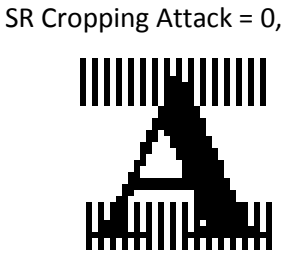


Figure 120 SR value of watermarked image after cropping attack

Figure 121 shows that original image and attacked image for Filter attack and Figure 122 show that SR value of attacked image

PSNR value after Filter Attack = 36, 6585

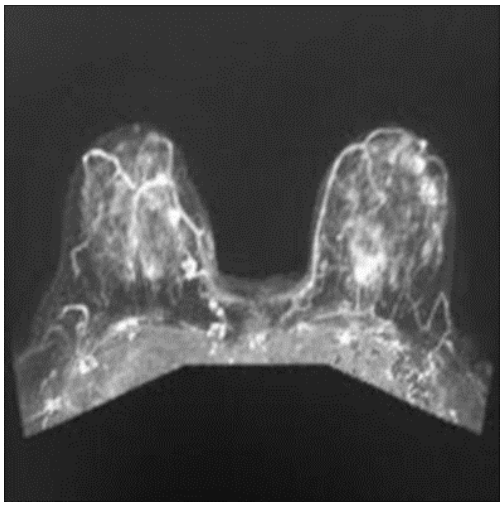


Figure 121 PSNR values Filter attack images

SR Filter Attack = 0, 8848

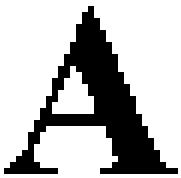


Figure 122 SR value of watermarked image after filter attack

Figure 123 shows that original image and attacked image for Histogram attack and Figure 124 show that SR value of attacked image

PSNR value after Histogram Attack = 11, 9156

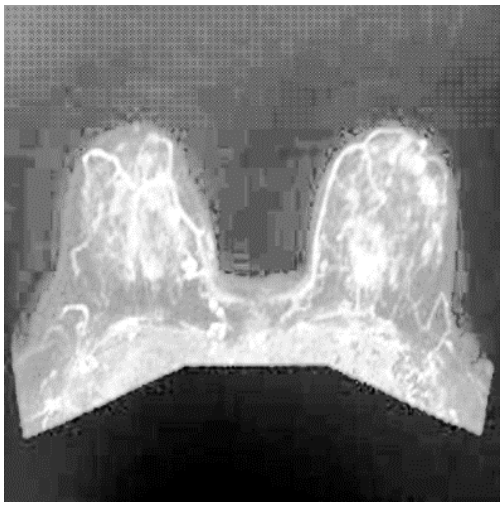


Figure 123 PSNR values Histogram attack images

SR Histogram Attack = 0, 8848

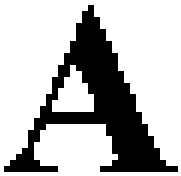


Figure 124 SR value of watermarked image after Histogram attack

Figure 125 shows that original image and attacked image for Gamma attack and Figure 126 show that SR value of attacked image

PSNR value after Gamma Attack = 19, 0065

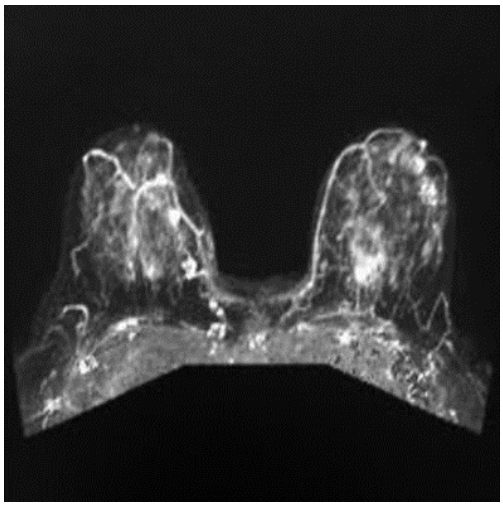


Figure 125 PSNR values Gamma attack images

SR Gamma Attack = 0, 8848

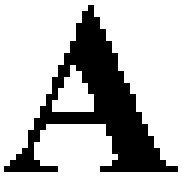


Figure 126 SR value of watermarked image after gamma attack

Figure 127 shows that original image and attacked image for Gaussian attack and Figure 128 show that SR value of attacked image

PSNR value after Gaussian Attack = 30, 0133

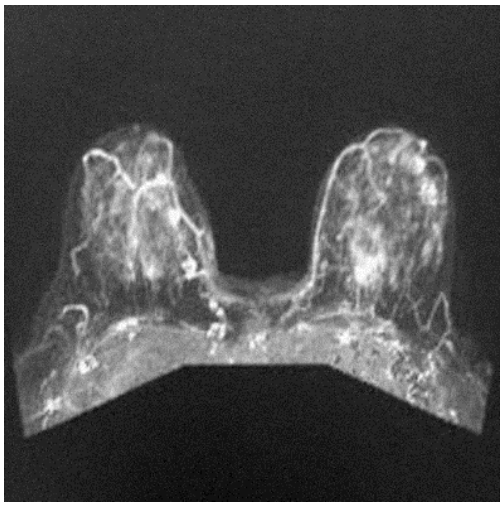


Figure 127 PSNR values Gaussian attack images

SR Gaussian Attack = 0, 8848

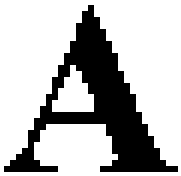


Figure 128 SR value of watermarked image after Gaussian attack

Figure 129 shows that original image and attacked image for Filter attack and Figure 130 show that SR value of attacked image

PSNR value after Intensity Attack = 21, 4528

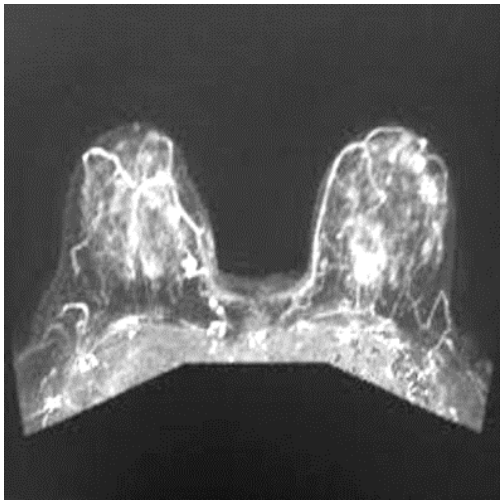


Figure 129 PSNR values Intensity attack images

SR Intensity Attack = 0, 8848

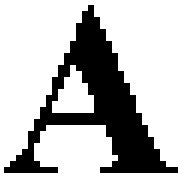


Figure 130 SR value of watermarked image after intensity attack

Figure 131 shows that original image and attacked image for Resize attack and Figure 132 show that SR value of attacked image

PSNR value after Resize Attack = 36, 0273

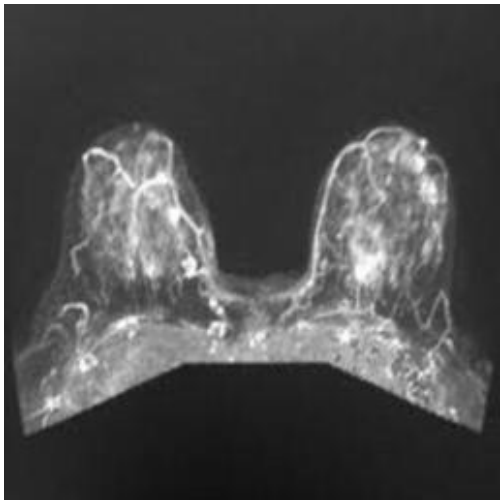


Figure 131 PSNR values Resize attack images

SR Resize Attack = 0, 4570

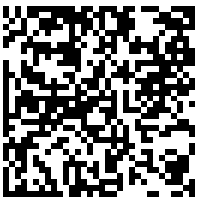


Figure 132 SR value of watermarked image after resize attack

Figure 133 shows that original image and attacked image for rotate attack and Figure 134 show that SR value of attacked image

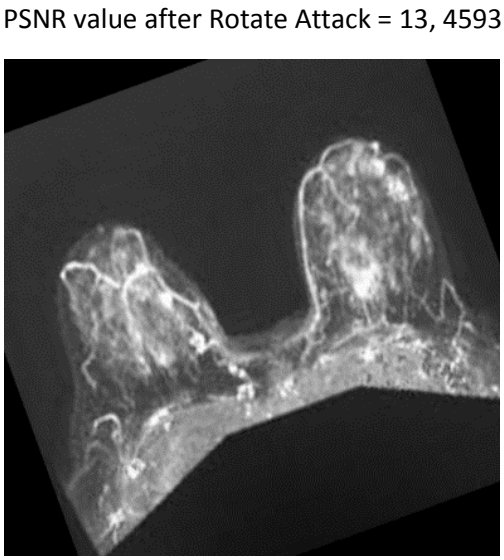


Figure 133 PSNR values rotate attack images

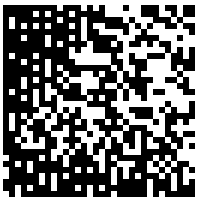


Figure 134 SR value of watermarked image after rotate attack

Figure 135 shows that original image and attacked image for Salt & Pepper attack and Figure 136 show that SR value of attacked image

PSNR value after Salt& Pepper Attack = 21, 7250

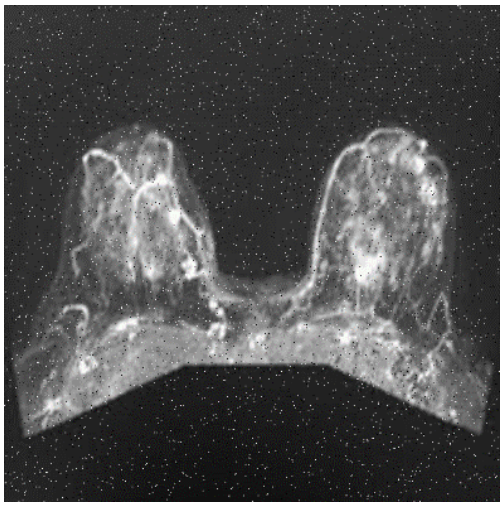


Figure 135 PSNR values Salt & Pepper attack images

SR Salt & Pepper Attack = 0, 8701

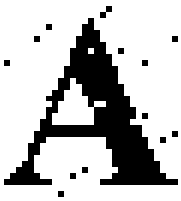


Figure 136 SR value of watermarked image after salt & pepper attack

Figure 137 shows that original image and attacked image for Speckle attack and Figure 138 show that SR value of attacked image

PSNR value after Speckle Attack = 23, 2045

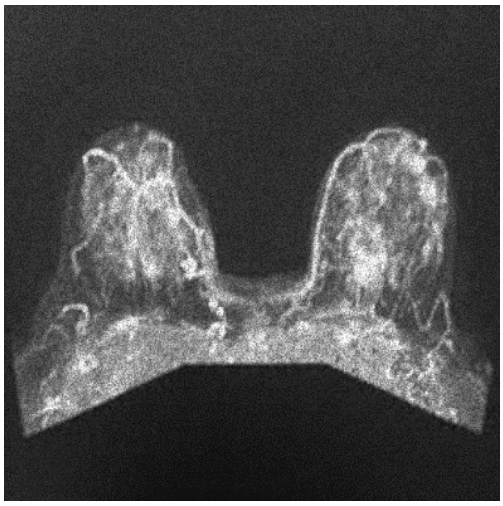


Figure 137 PSNR values Speckle attack images

SR Speckle Attack = 0, 8848

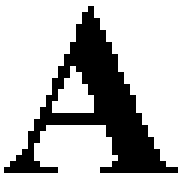


Figure 138 SR value of watermarked image after speckle attack

Figure 139 shows that original image and attacked image for Jpeg (75) attack and Figure 140 show that SR value of attacked image

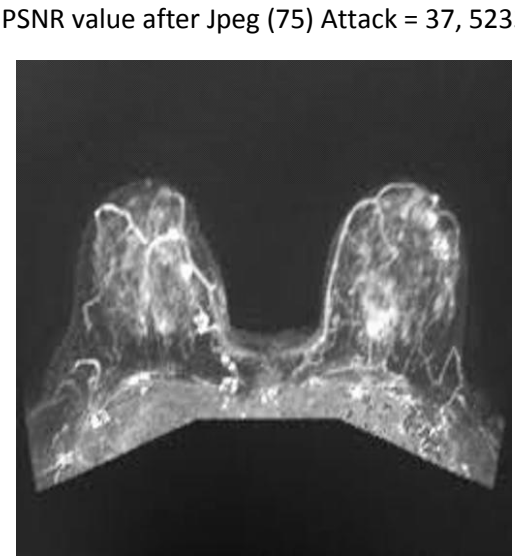


Figure 139 PSNR values Jpeg (75) attack images

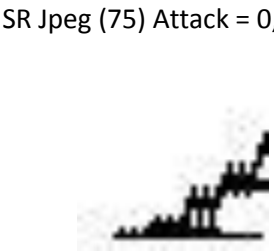


Figure 140 SR value of watermarked image after jpeg (75) attack

Figure 141 shows that original image and attacked image for Jpeg (50) attack and Figure 142 show that SR value of attacked image

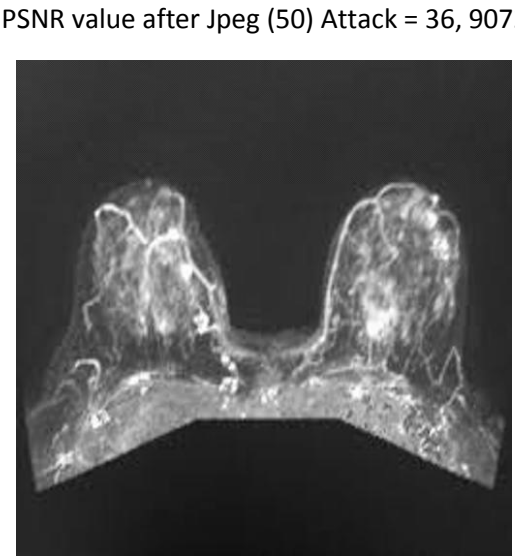


Figure 141 PSNR values Jpeg (50) attack images

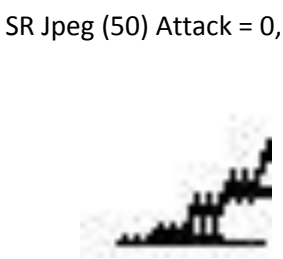


Figure 142 SR value of watermarked image after jpeg (50) attack

Table 4 PSNR and SR values after attacks

Attacks	PSNR	PSNR values after attacks	SR
Cropping	37,5363	18,1172	0,2219
Gaussian	37,5363	36,6585	0,8848
Filter	37,5363	29,244117	0,8848
Rotate	37,5363	13,4593	0,4150
Gamma	37,5363	19,0065	0,8848
Histogram	37,5363	11,9156	0,8848
Intensity	37,5363	21,4528	0,8848
Salt & Pepper	37,5363	23,2045	0,8701
Speckle noise	37,5363	23,2045	0,8848
Jpeg(75)	37,5363	37,5233	0,6748
Jpeg(50)	37,5363	36,9072	0,6748
Resize	37,5363	36,0273	0,4570

When we examine table 4 we realized that if PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For instance PSNR value is 37, 5363 before Resize attack. After Resize attack the PSNR value is 36, 0273 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. The SR method compares pixel values of two watermark images. This values are between 0 and 1. If SR values close to 1, it means that recovered watermark image is in ideal optimum and preferred condition. Cropping, Rotate and Resize attacks' SR values are not good because they have the nearest values to 0. Other attack types' SR values are nearest to 1, as you can see in table 4. Best PSNR values are in Gaussian, Jpeg (50), Resize and JPEG (75) attacks. Histogram attack has the worst PSNR value.

3.3. Discrete Fourier Transform

Figure 143 Original Image

Figure 144 Watermark Image

Figure 145 Watermarked Image

10 different attacks are used in this experience by using MATLAB. They are "Intensity attack, Gamma attack, Cropping attack, Gaussian attack, Histogram equalization attacks, Imnoise attack, rotate attack and speckle noise attacks". Watermark embedding process is done by DFT. After that the attacks, which are mentioned in the above, are applied to watermarked image (Figure 145 Watermarked Image). Then, the extract process is done. The images that are applied attack are shown in Figure 146 Noise Attack – Figure 155 Jpeg (50) Attack.

Figure 146 Noise Attack **Figure 147** Gamma Attack **Figure 148** Intensity Attack

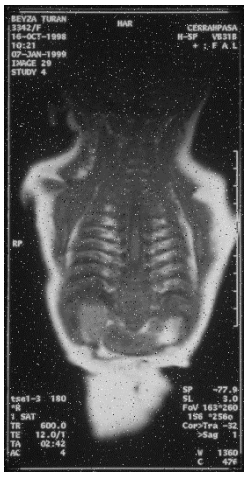


Figure 149 Histogram Attack **Figure 150** Cropping Attack **Figure 151** Salt & Pepper Attack

Figure 152 Gaussian Attack

Figure 153 Rotate Attack

Figure 154 Jpeg (75) Attack

Figure 155 Jpeg (50) Attack

PSNR value = 35,176721 PSNR value after Cropping Attack = 10,810788

Figure 156 PSNR values original and cropping attack images

SR Cropping Attack = 0,7312

Figure 157 SR value of watermarked image after cropping attack

PSNR value = 35,176721 PSNR value after Histogram Attack = 12,18047

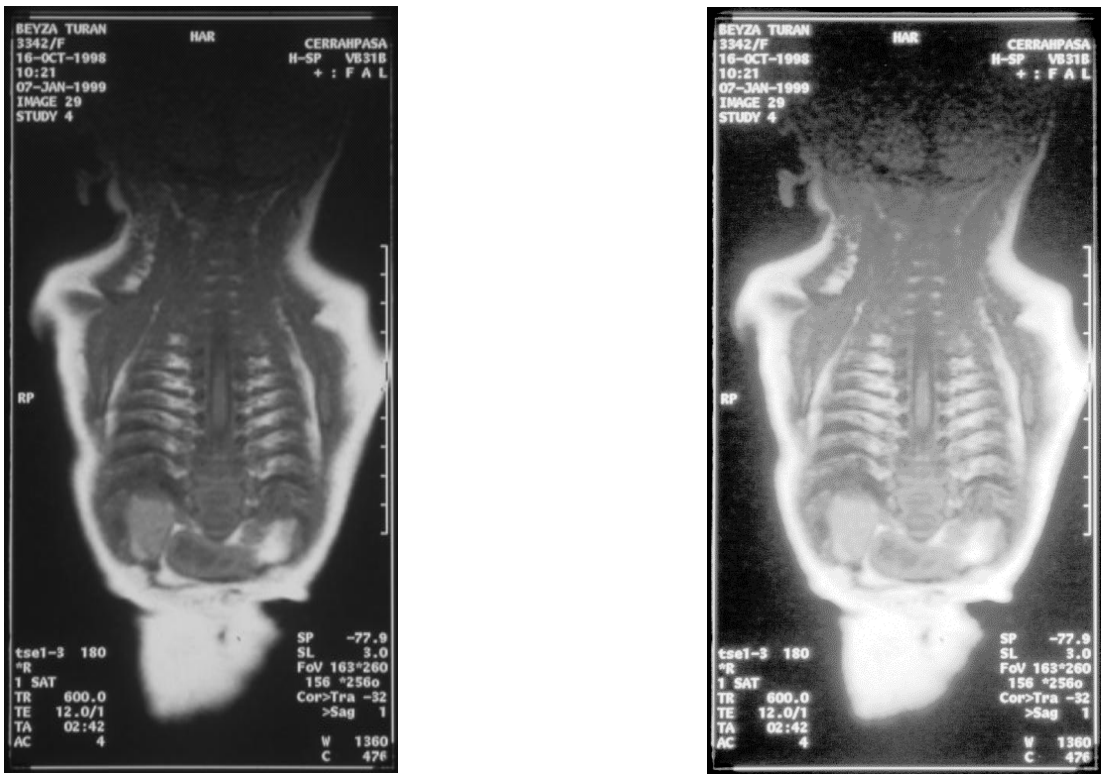


Figure 158 PSNR values original and histogram attack images

SR Histogram Attack = 0,8788

Figure 159 SR value of watermarked image after Histogram attack

PSNR value = 35,176721

PSNR value after Gamma Attack = 14,606989

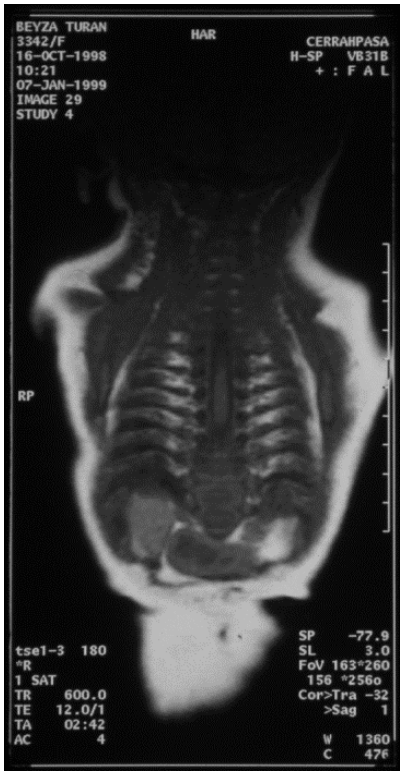


Figure 160 PSNR values original and gamma attack images

SR Gamma Attack = 0, 2756

Figure 161 SR value of watermarked image after Gamma attack

PSNR value = 35,176721 PSNR value after Rotate Attack = 10,352137

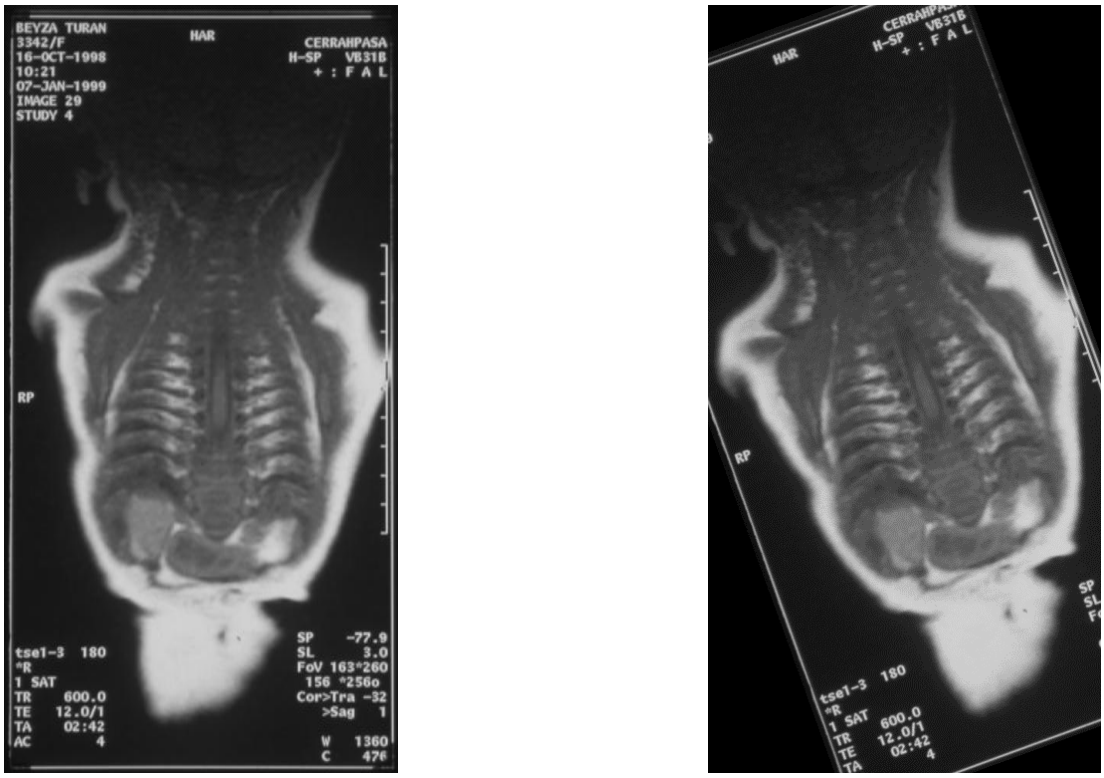


Figure 162 PSNR values original and rotate attack images

SR Rotate Attack = 0, 1275

Figure 163 SR value of watermarked image after rotate attack

PSNR value = 35,176721 PSNR value after Gaussian = 20,506922

Figure 164 PSNR values original and Gaussian attack images

SR Gaussian Attack = 0, 1394

Figure 165 SR value of watermarked image after Gaussian attack

PSNR value = 35,176721 PSNR value after Salt&Pepper Attack = 16,88813

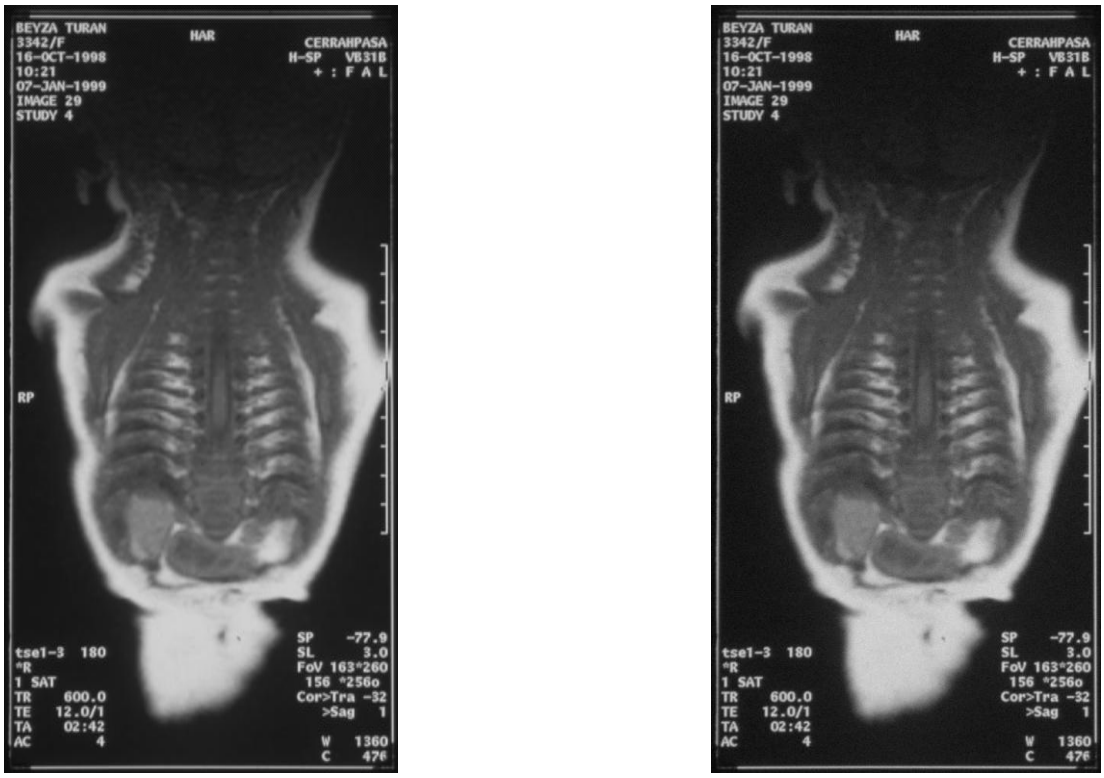


Figure 166 PSNR values original and salt & pepper attack images

SR Salt & Pepper Attack = 0, 1894

Figure 167 SR value of watermarked image after Salt & Pepper attack

PSNR value = 35,176721 PSNR value after Intensity Attack = 15,214227

Figure 168 PSNR values original and intensity attack images

SR Intensity Attack = 0, 9750

Figure 169 SR value of watermarked image after Intensity attack

PSNR value = 35,176721 PSNR value after Speckle Attack = 22,901300

Figure 170 PSNR values original and speckle noise attack images

SR Noise (Speckle) Attack = 0, 2219

Figure 171 SR value of watermarked image after speckle noise attack

PSNR value = 35,176721 PSNR value after Jpeg(75) Attack = 13, 0239

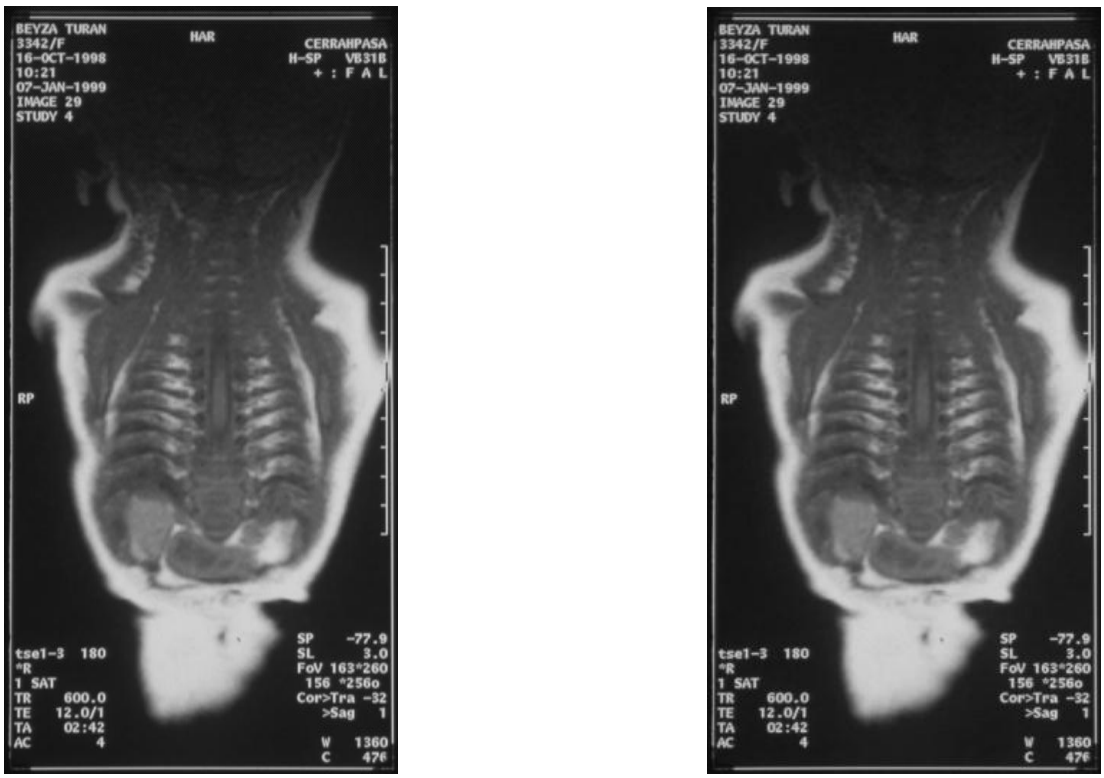


Figure 172 PSNR values original and jpeg (75) attack images

SR Jpeg (75) Attack = 0, 1338

Figure 173 SR value of watermarked image after jpeg (75) attack

PSNR value = 35,176721 PSNR value after Jpeg(50) Attack = 13, 1023

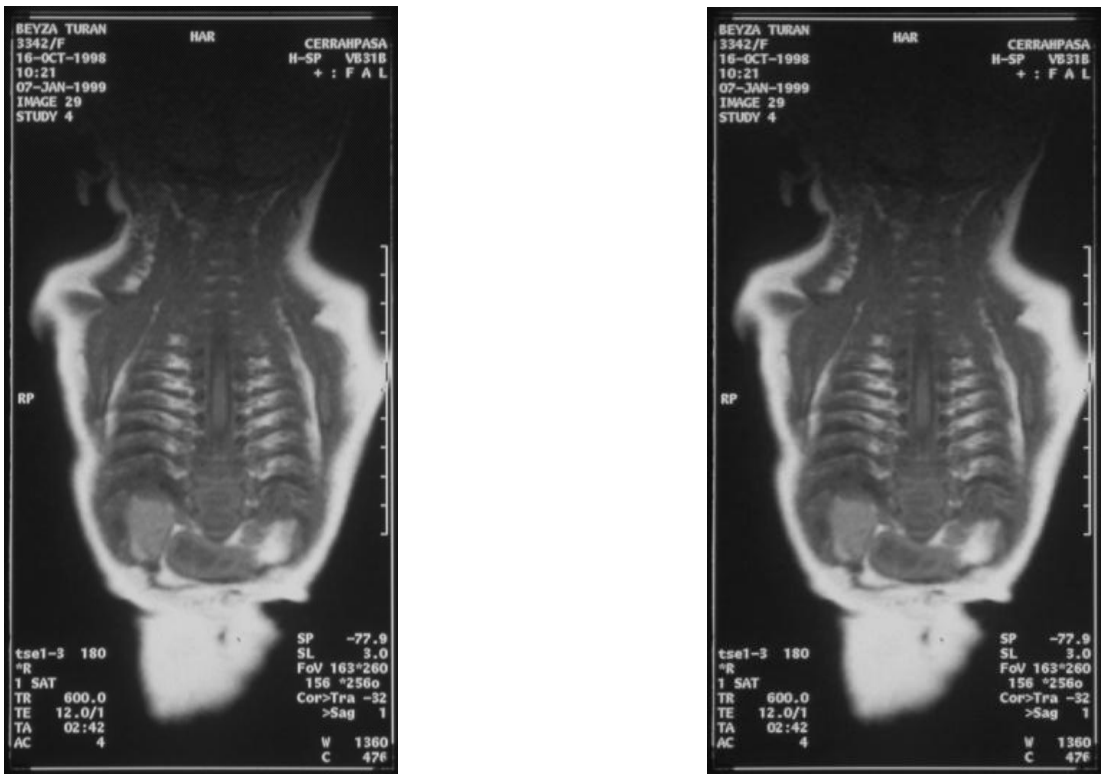


Figure 174 PSNR values original and jpeg (50) attack images

SR Jpeg(50) Attack = 0,1462

Figure 175 SR value of watermarked image after jpeg (50) attack

Table 5 PSNR and SR values after attacks

Attacks	PSNR	PSNR values after attacks	SR
Cropping	35,176721	10,810788	0,7312
Gaussian	35,176721	20,506922	0,1394
Rotate	35,176721	10,352137	0,1275
Gamma	35,176721	14,606989	0,2756
Histogram	35,176721	12,180470	0,8788
Intensity	35,176721	15,214227	0,9750
Salt & Pepper	35,176721	16,888130	0,1894
speckle noise	35,176721	22,901300	0,2219
Jpeg(75)	35,176721	13,023900	0,1338
Jpeg(50)	35,176721	13,102300	0,1462

Table 5 PSNR shows that PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. If PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For example PSNR value is 35,176721 before Salt & Pepper attack. After Salt & Pepper attack the PSNR value is 16,888130 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. The SR method compares pixel values of two watermark images. This values are between 0 and 1. If SR values close to 1, it means that recovered watermark image is in ideal optimum and preferred condition. Gaussian, Salt & Pepper, Gamma, Speckle Noise and Jpeg attacks' SR values are not good because they have the nearest values to 0. Other attack types' SR values are nearest to 1, as you can see in table 5. Best PSNR values are in Gaussian, Speckle Noise attacks. Rotate attack has the worst PSNR value

Figure 176 Original Image (Neck Mr) (Neck-MRI) by using Discrete Fourier Transform, the embedding process of watermark images is done. PSNR and SR values are calculated by applying attacks for watermark embedded images (Figure 177 Watermarked Image)

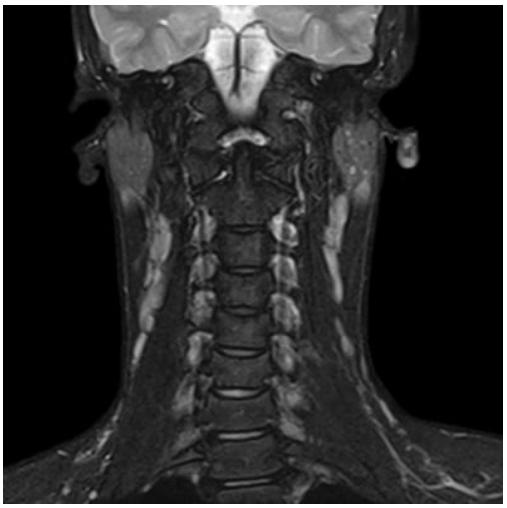


Figure 176 Original Image (Neck Mr)

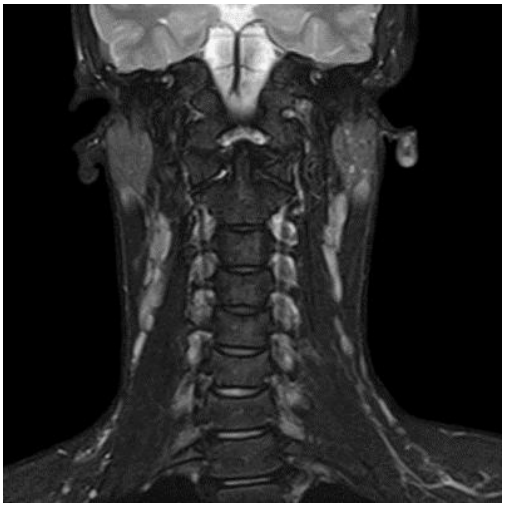


Figure 177 Watermarked Image

Figure 178 Watermark Image

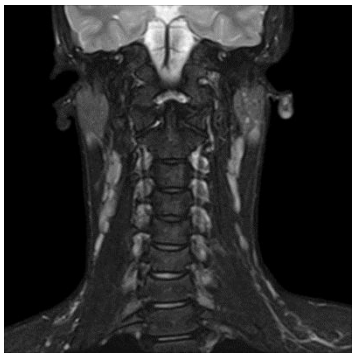


Figure 179 Filter Attack

Figure 180 Cropping Attack

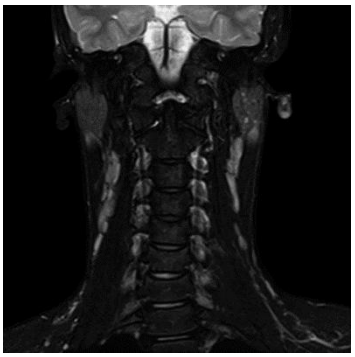


Figure 181 Gamma Attack

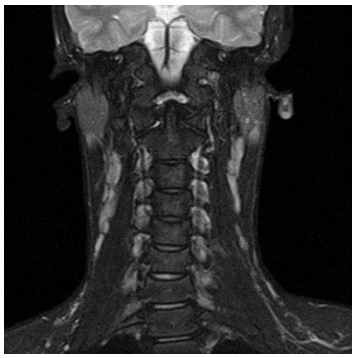


Figure 182 Gaussian Attack

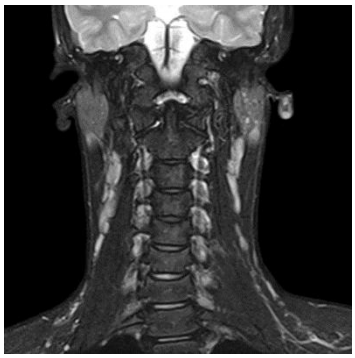


Figure 183 Intensity Attack

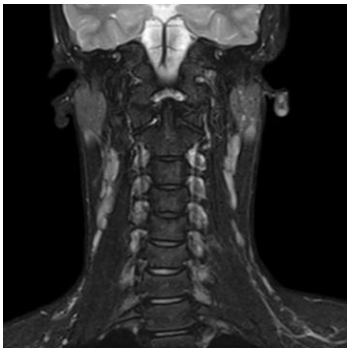
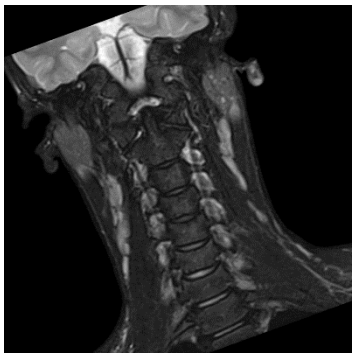


Figure 184 Resize Attack



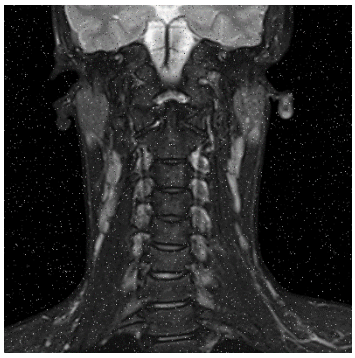


Figure 185 Rotate Attack **Figure 186** Salt & Pepper Attack **Figure 187** Speckle Attack

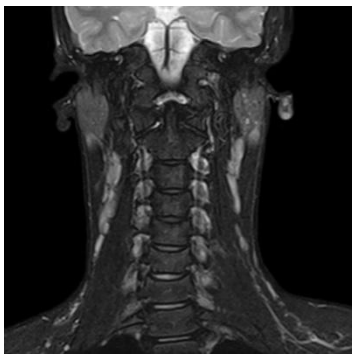


Figure 188 Jpeg (75) Attack

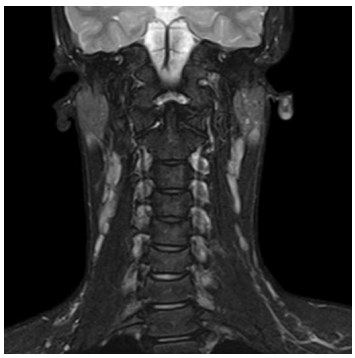
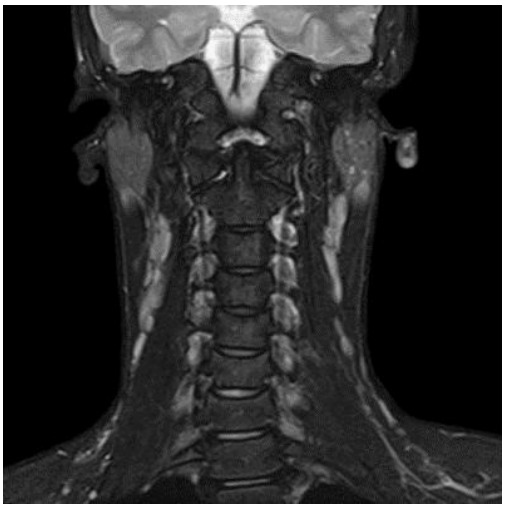


Figure 189 Jpeg (50) Attack

PSNR value watermarked images = 48, 1430



PSNR value after Filter Attack = 41, 7453

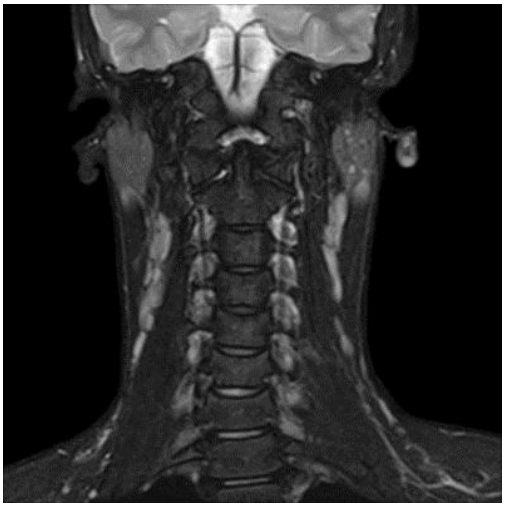


Figure 190 PSNR values original and Filter attack images

SR Filter Attack = 0,5781

Figure 191 SR value of watermarked image after filter attack

PSNR value after Cropping Attack = 22, 1004

Figure 192 PSNR values original and Cropping attack images

SR Cropping Attack = 0,8662

Figure 193 SR value of watermarked image after cropping attack

PSNR value after Gamma Attack = 21, 2767

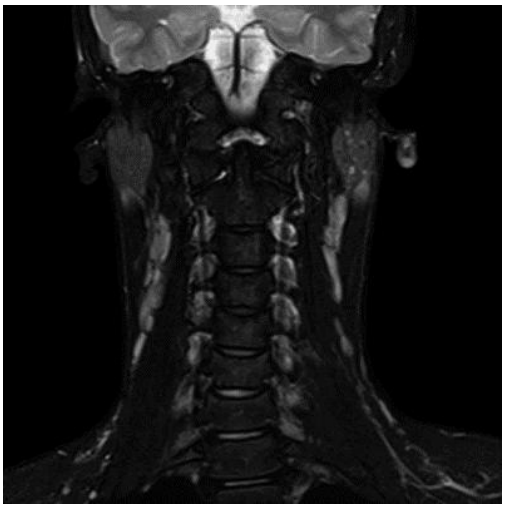


Figure 194 PSNR values original and Gamma attack images

SR Gamma Attack = 0,8956

Figure 195 SR value of watermarked image after gamma attack

PSNR value after Gaussian Attack = 30, 8571

Figure 196 PSNR values original and Gaussian attack images

SR Gaussian Attack = 0,5744

Figure 197 SR value of watermarked image after Gaussian attack

PSNR value after Intensity Attack = 25, 1287

Figure 198 PSNR values original and Intensity attack images

SR Intensity Attack = 0,8819

Figure 199 SR value of watermarked image after intensity attack

PSNR value after Resize Attack = 43, 1874

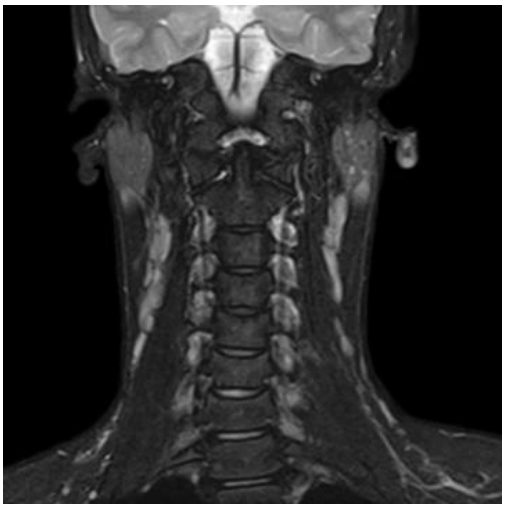


Figure 200 PSNR values original and Resize attack images

SR Resize Attack = 0,6062

Figure 201 SR value of watermarked image after resize attack

PSNR value after Rotate Attack = 14, 3982

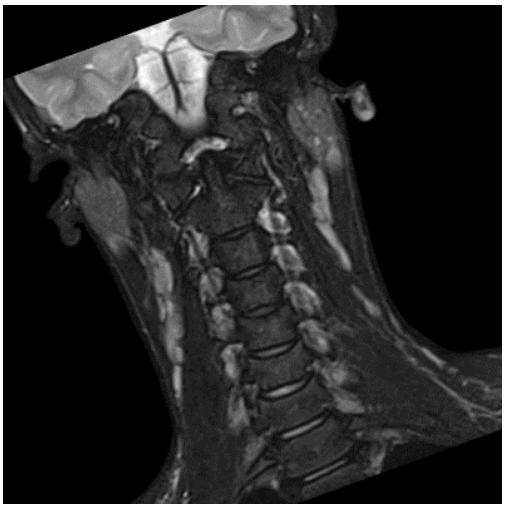


Figure 202 PSNR values original and rotate attack images

SR Rotate Attack = 0,6563

Figure 203 SR value of watermarked image after rotate attack

PSNR value after Salt & Pepper Attack = 20, 9357

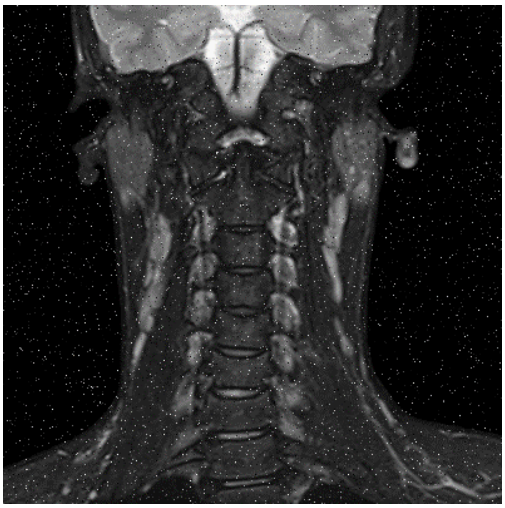


Figure 204 PSNR values original and Salt & Pepper attack images

SR Salt & Pepper Attack = 0,6887

Figure 205 SR value of watermarked image after salt & pepper attack

PSNR value after Speckle Attack = 26, 9029

Figure 206 PSNR values original and Speckle attack images

SR Speckle Attack = 0,5781

Figure 207 SR value of watermarked image after speckle attack

PSNR value after Jpeg (75) Attack =45, 7127

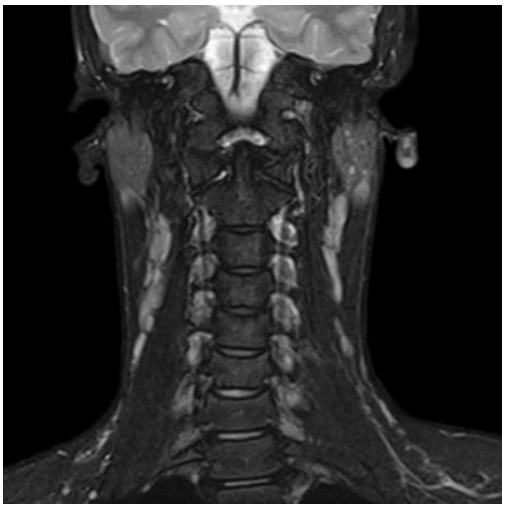


Figure 208 PSNR values original and Jpeg (75) attack images

SR Jpeg(75) Attack = 0,8969

Figure 209 SR value of watermarked image after jpeg (75) attack

PSNR value after Jpeg (50) Attack =42, 8370

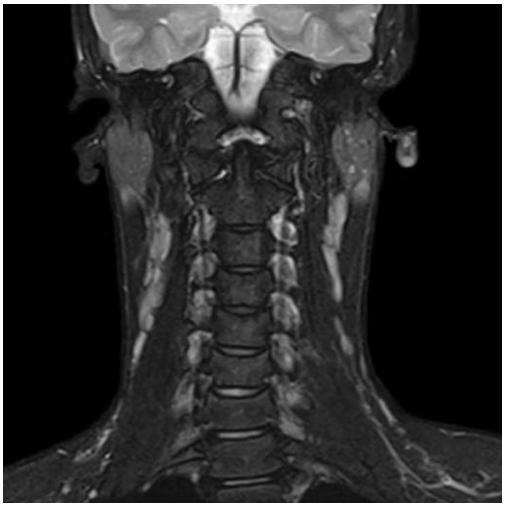


Figure 210 PSNR values original and Jpeg (50) attack images

SR Jpeg(50) Attack = 0,6438

Figure 211 SR value of watermarked image after jpeg (50) attack

Table 6 PSNR and SR values after attacks

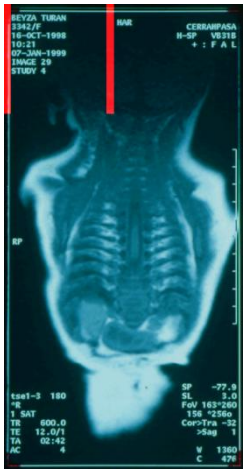
Attacks	PSNR	PSNR values after attacks	SR
Cropping	48,1430	22,1004	0,8662
Gaussian	48,1430	30,8571	0,5744
Rotate	48,1430	14,3982	0,6563
Gamma	48,1430	21,2767	0,8956
Histogram	48,1430	12,180471	0,2400
Intensity	48,1430	25,1287	0,8919
Salt & Pepper	48,1430	20,9357	0,6887
speckle noise	48,1430	26,9029	0,5781
Jpeg(75)	48,1430	45,7127	0,8969
Jpeg(50)	48,1430	42,8370	0,6438
Resize	48,1430	43,1874	0,6062
Filter	48,1430	41,7453	0,5781

Table 6 summarizes that PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. If PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For example PSNR value is 48, 1430 before Filter attack. After Filter attack the PSNR value is 41, 7453 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. The SR method compares pixel values of two watermark images. This values are between 0 and 1. If SR values close to 1, it means that recovered watermark image is in ideal optimum and preferred condition. Histogram and Gaussian attacks' SR values are not good because they have the nearest values to 0. Other attack types' SR values are nearest to 1, as you can see in table 6. Best PSNR values are in Jpeg (50), Jpeg (75), Resize and Filter attacks. Rotate attack has the worst PSNR value.

3.4. Least Significant Bit

In this part the attacks are applied by embedding encrypted message with LSB method. First of all patient info message prepared. After these message which is prepared first part is encrypted with RSA algorithm. And encrypted message embed medical image via LSB methods. Then calculating PSNR values of watermarked images after this process applied some attacks and calculating PSNR values images that is applied attacks. Extracting encrypted message in watermarked imaged and decrypted process is applied to reach patient info.

Figure 212 Gaussian Attack **Figure 213** Salt and Pepper Attack **Figure 214** Speckle Attack



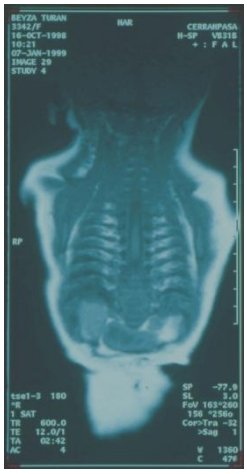


Figure 215 Crop Attack **Figure 216** Gamma Attack **Figure 217** Intensity Attack

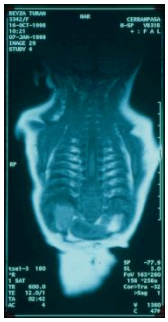


Figure 218 Resize Attack

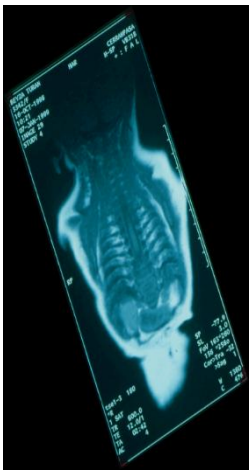


Figure 219 Rotate Attack

Table 7 PSNR values after attacks

Attacks	PSNR	PSNR values after attacks
Cropping	34,8826	27,9149
Gaussian	34,8826	24,1162
Rotate	34,8826	8,96044
Gamma	34,8826	17,6797
Intensity	34,8826	23,1189
Salt & Pepper	34,8826	20,8972
Speckle noise	34,8826	25,9120

Table 7 shows that PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. If PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For example PSNR value is 34, 8826 before cropping attack. After Cropping attack the PSNR value is 27, 9149 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. . Best PSNR values are in Cropping and Gaussian attacks. Rotate attack has the worst PSNR value.

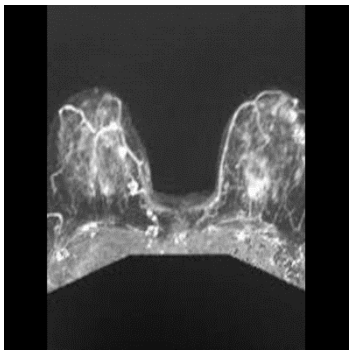
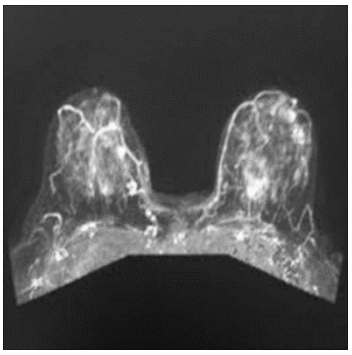
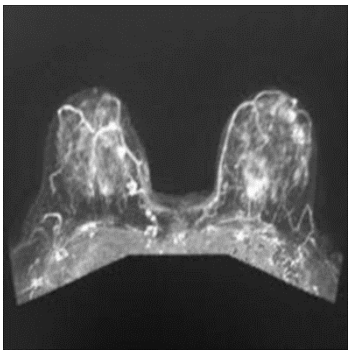




Figure 220 Cropping Attack **Figure 221** Filter Attack **Figure 222** Histogram Attack

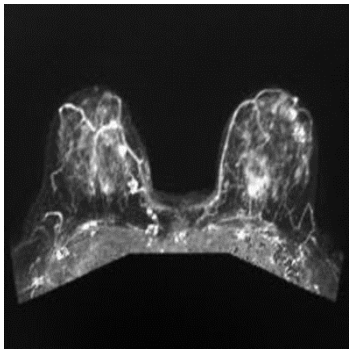
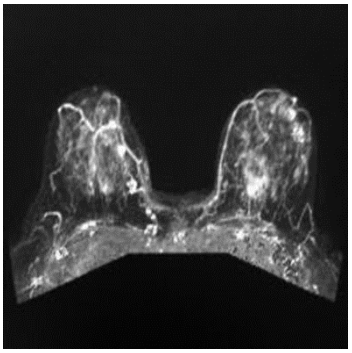
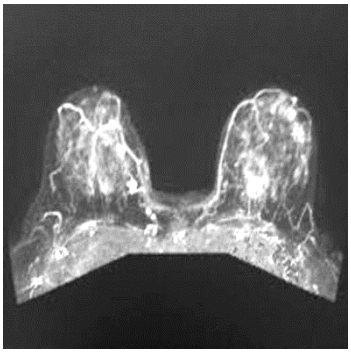




Figure 223 Gamma Attack **Figure 224** Gaussian Attack **Figure 225** Intensity Attack

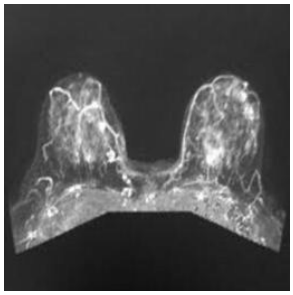
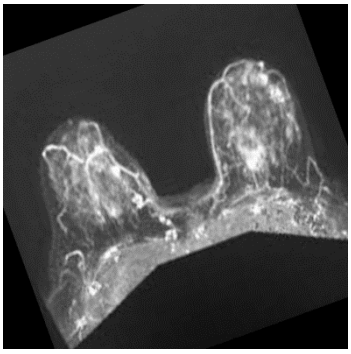
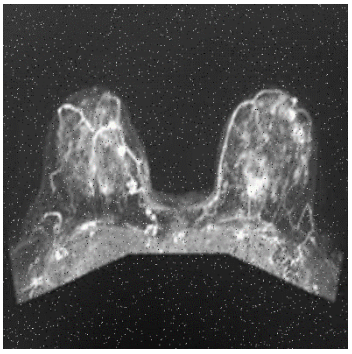




Figure 226 Resize Attack **Figure 227** Rotate Attack **Figure 228** Salt & Pepper Attack

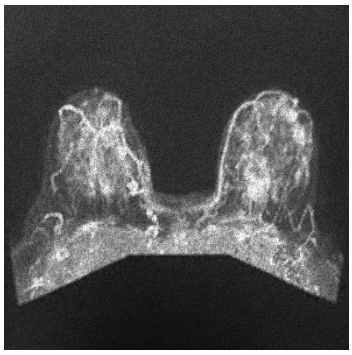


Figure 229 Speckle Attack

Table 8 PSNR values after attacks

Attacks	PSNR	PSNR values after attacks
Cropping	39,1895	15,2452
Gaussian	39,1895	33,5123
Filter	39,1895	27,6591
Rotate	39,1895	11,3695
Gamma	39,1895	20,1059
Histogram	39,1895	11,7125
Intensity	39,1895	23,1189
Salt & Pepper	39,1895	20,8972
speckle noise	39,1895	21,1147
Jpeg(75)	39,1895	35,2344
Jpeg(50)	39,1895	34,7563
Resize	39,1895	32,0367

Table 8 PSNR shows that PSNR values of watermarked image and PSNR values of after attacked watermarked image and SR values of watermark image. If PSNR values are higher, it shows us much better quality of the compressed or reconstructed image. If PSNR value is infinity, it means that two images are identically same and at this reason PSNR value result is infinity. For example PSNR value is 39, 1895 before Intensity attack. After Intensity attack the PSNR value is 23, 1189 as can be seen the PSNR values were changed. As noticed, this image is not original watermarked image because PSNR values is different. . Best PSNR values are in Jpeg (50), Jpeg (75), Resize and Gaussian attacks. Rotate and Histogram attacks have the worst PSNR values.

At the results of attacks, when the encrypted message that is embedded as text is extracted, the encrypted message is seen corrupted. However, any encrypted text message could not be found in Gamma and Rotate attacks.

CHAPTER 4

INTERPRETATION OF RESULTS

In this thesis, DWT, DCT, DFT, and LSB has been analysed as watermarking methods. LSB uses a spatial domain whereas other methods use transform domain. Every method was applied to insert watermark image in medical images for watermarking except LSB method. After this process watermarked image has been achieved and attacks have been applied to watermarked image. LSB method was used to hide encrypted patient info message in medical images. After all processes, we have calculated the PSNR and SR values. PSNR values after attacks are given on Table-9. In this work transform domain has been found as more successful than spatial domain when we compare PSNR values. Results show us, encrypted message was destroyed when attacked watermarked images that is used LSB algorithm. When we compare DWT, DCT and DFT which are transform domain methods through experimental results observed DWT and DFT PSNR values are better than DCT PSNR values. Extracted watermark image, which was extracted in watermarked image after attacks, was calculated SR value. These SR values show us DFT has worst SR values. DCT and DWT SR values are almost closer each other and these values around 1. Also some cases have remained outside it, such as Salt & Pepper and Speckle Noise attack because these values are closer to 0.

To sum up experiments show the DWT algorithm has robustness for attacks while still keeping the quality of the image. DCT algorithm also has robustness but PSNR values are worse than DWT and DFT algorithms. DFT algorithm keeping the quality but the SR values are worse than DCT and DWT algorithms. This means that DFT algorithm is not robust in this work like DCT and DWT algorithms because of DFT SR values. For medical images algorithm should ensure good quality for image. Because; if image quality changes, it can effect of patient treatment. At the same time watermark image must be robust. And results show us DWT is more suitable for medical images as a result.

Table 9 PSNR values after attack

PSNR values after attack	**DWT**	**DCT**	**DFT**	**LSB**
Cropping	23,14363	18,1172	22,1004	15,2452
Gaussian	31,01152	36,6585	30,8571	33,5123
Filter	42,25647	29,244117	41,7453	27,6591
Rotate	10,357190	13,4593	14,3982	11,3695
Gamma	20,154851	19,0065	21,2767	20,1059
Histogram	10,035300	11,9156	12,180471	11,7125
Intensity	22,583412	21,4528	25,1287	23,1189
Salt&Pepper	22,888509	23,2045	20,9357	20,8972
Speckle noise	44,270100	23,2045	26,9029	21,1147
Jpeg(75)	41,706500	37,5233	45,7127	35,2344
Jpeg(50)	30,044500	36,9072	42,8370	34,7563

CHAPTER 5

CONCLUSION

In this work, watermarking in medical images has been analysed by using DWT, DCT, DFT and LSB algorithms. The purpose of this study is calculating PSNR and SR values on medical images via different algorithms and comparing results. Watermarking is performed by hiding a logo in the original image. In this proposal, logo images are inserted into the medical images (MRI) utilizing DCT, DWT and DFT methods and different attacks are connected on the subsequent images. Embedding watermarking is divided three approaches: transform domain, spatial domain and compressed domain. In this work, transform domain and spatial domain are used with DCT, DWT, DFT and LSB. Three different MRI images are used. DFT method has been found as the best PSNR value (48, 1430). DCT, DFT and LSB values are almost same. Their PSNR values are around 35. When compares DCT, DFT and DWT methods SR values, DFT SR values are worst SR values. In future work Region of Interest (ROI) of the medical image and Region of Non Interest (RONI) of the medical image area will be used and watermarking process will be applied respectively ROI and RONI areas. PSNR and SR values will be calculated and compared

REFERENCES

[1] **Akar F., Yalman Y., Varol H.S., (2012)** "*Data Hiding in Digital Images Using A Partial Optimization Technique Based on Classical LSB Method*", Turkish Journal Of Electrical Engineering and Computer Sciences, doi: 10.3906/elk-1205-58.

[2] **Zhang Q., Li Y., Wei X., (2012)** "*An Improved Robust and Adaptive Watermarking Algorithm Based on DCT*", Journal of Applied Research and Technology, Vol. 10,
pp. 405-415.

[3] **Jane O., Elbaşi E., (2013)** "*A new approach in non-blind watermarking method Based on DWT and SVD via LU decomposition*", Turkish Journal of Electrical Engineering and Computer Sciences.

[4] **Kannammal A., Subha Rani S., (2014)** "*Two Level Security for Medical Images Using Watermarking/Encryption Algorithms*", International Journal of Imaging Systems and Technology Volume 24, Issue 1, pages 111–120.

[5] **Giakoumaki A., Pavlopoulos S., Koutsouris D., (2003)** "*A medical image watermarking scheme based on wavelet transform*", Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE

[6] **Miao S., Li J., Bai Y., Chen Y., (2012)** "*Robust Watermarking for Medical Images Based on Arnold Scrambling and DWT-DFT*", Computing and Convergence Technology (ICCCT) 7th International Conference.

[7] **Baiying L., Ee-Leng T., Siping C., Dong N., Tianfu W., (2014)** "*Reversible watermarking scheme for medical image based on differential evolution*", Expert Systems with Applications: An International Journal archive Volume 41 Issue 7, Pages 3178-3188

[8] **Pritesh P, S. Selvakumar., (2014)** "*Blind Image Steganalysis of JPEG images using feature extraction through the process of dilation*", Digital Investigation 11(1): 67-77.

[9] **Minamoto T., Ohura R.**, **(2014)** "*A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic*", Applied Mathematics and Computation 226: 306-319.

[10] **Khayam S. A.**, **(2012)** "*The Discrete Cosine Transform*",

[11] **Bultheel A. (1995)** MATH. SOC 2.

[12] **Chang S. G., Yu B., Vetterli M., (2000)** "*Trans. Image Processing*", 9 p. 1532

[13] **Hartung F., Kutter M., (1999),** "*Multimedia Watermarking Techniques*", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103.

[14] **Sharma P. K., Rajni, (2012)** "*Analysis of Image Watermarking Using Least Significant Bit Algorithm International*" Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4.