ÇANKAYA UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
COMPUTER ENGINEERING

MASTER THESIS

DIGITAL IMAGE WATERMARKING BY FINDING CORNER POINTS BASED ON DWT ALGORITHM

NAİM ÖLÇER

SEPTEMBER 2013

Title of the Thesis: **Digital Image Watermarking By Finding Corner Points Based On DWT Algorithm**

Submitted by **Naim ÖLÇER**

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 of Philosophy.

Yrd. Doç. Dr. Murat SARAN
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 of Philosophy.

Dr. Ersin ELBAŞI
Co-Supervisor

Yrd. Doç. Dr. Abdül Kadir GÖRÜR
Supervisor

Examination Date: September 16, 2013

Examining Committee Members

Yrd. Doç. Dr. Abdülkadir Görür (Çankaya Univ.)

Dr. Ersin Elbaşı (TÜBİTAK)

Yrd. Doç. Dr. Reza Zare Hassanpour (Çankaya Univ.)

STATEMENT OF NON-PLAGIARISM

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: Naim Ölçer

Signature:

Date: 16.09.2013

ABSTRACT

DIGITAL IMAGE WATERMARKING BY FINDING CORNER POINTS BASED ON DWT ALGORITHM

ÖLÇER, Naim

M.S.c., Department of Computer Engineering

Supervisor: Yrd. Doç. Dr. Abdülkadir Görür

Co-Supervisor: Dr. Ersin Elbaşı

September 2013, 80 pages

Nowadays digital watermarking is one of the popular research areas. Watermarking is an information hiding technique used to hide a mark. In the thesis, proposed a novel robust image watermarking with finding corner point based on DWT method. Harris corner detector is used to find feature points. By finding corners, compute square regions around feature point. In digital watermarking, processes are embedding, detection and extraction. After computing square region crop it and embed the watermarking. Attacks are applied to watermarked image and then detect and extract watermarking. Main goal of study is showing variations of PSNR and SR values on different attacks on different square regions and comparing SR, PSNR and PSNR after attacks.

Keywords: Digital watermarking, Discrete Wavelet Transform, Peak Signal-to-Noise Ratio, Similarity Ratio, Corner Point Detection

ÖZ

KÖŞE NOKTALARININ BULUNMASI İLE DWT ALGORİTMASINA DAYALI İMGELERDE DAMGALAMA METODU

ÖLÇER, Naim

Yüksek lisans, Bilgisayar Mühendisliği Anabilim Dalı

Tez Yöneticisi: Yrd. Doç. Dr. Abdülkadir Görür

Ortak Tez Yöneticisi: Dr. Ersin Elbaşı

Eylül 2013, 80 sayfa

Günümüzde dijital damgalama popüler araştırma alanlarından biridir. Damgalama logo gizlemek için kullanılan bir bilgi gizleme tekniğidir. Tezde, köşe noktaları bulunarak DWT yöntemine göre yeni ve sağlam bir damgalama metodu önerilmektedir. Noktaları bulmak için Harris köşe detektörü yöntemi kullanılır. Köşeler bulunarak, nokta etrafındaki kare bölgeler hesaplanır. Dijital damgalamada ki işlemler damga ekleme, damga detektörü ve damga çıkarmadır. Kare bölge hesaplandıktan sonra orijinal resimden çıkarılarak damga eklenir. Saldırılar damgalı resme uygulanır ve sonrasında damga tespit edilir ve çıkarılır. Çalışmanın temel amacı, farklı kare bölgelerinde farklı saldırılar uygulanarak PSNR ve SR değerleri değişimini göstermek ve saldırılardan sonraki SR ve PSNR değerlerini karşılaştırmaktır.

Anahtar Kelimeler: Dijital Damgalama, Ayrık Dalgalı Dönüşüm, Yoğun Sinyal Gürültü Oranı, Benzerlik Oranı, Köşe Noktası Bulma

ACKNOWLEDGMENTS

The author would like to acknowledge the contributions of the following groups and individuals to the development of this study.

Yrd. Doç. Dr. Abdülkadir Görür (supervisor) and Dr. Ersin Elbaşı (co-supervisor) for their invaluable direction and steadfast encouragement to complete this study…

Yrd. Doç. Dr. Reza Zare Hassanpour, for his comments and suggestions…

Special thanks to my wife and my family, for their reliance and giving me the strength in order to achieve everything of my life...

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Digital watermarking is an information hiding technique used to hide a mark such as image, audio signal, serial number or text in a given protected image. Also other digital watermarking application areas are apart from copy control and copyright protection; broadcast monitoring, fingerprinting, medical applications and content authentication are other application areas of digital watermarking. In real world, watermarking techniques can be implemented to many different areas, such as photograph, audio, and video. The hidden object is the watermark while the carrier is the marked object. There are three types of watermarks; Fragile, Robust, and Invertible. Fragile watermarks are destroyed, if the carrier image is subject to considerable modifications. Robust watermarks cannot be removed from the image unless the image is totally destroyed. Robust watermarks resist all types of known modifications. Invertible watermarks can be recovered from the carrier image using a given key, while non-invertible watermarks can be detected but not recovered.

There are basically three approaches to embed a watermark: spatial domain, transform domain and compressed domain watermarking. In the spatial domain, the watermark is embedded by modifying the pixel values in the original image. The simplest spatial domain watermarking technique is to embed the bits of the message directly into the least significant bit plane of the cover image [1]. Transform domain watermarking is similar to spatial domain watermarking; in this case, the coefficients of transforms such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT) are modified [2]. Compressed domain watermarking is only for audio or video files.

The Harris corner detector is mathematical operator that finds feature points. The algorithm relies on the image intensity and should change largely in multiple directions at a corner point. Looking though a small window, the Harris corner detector recognizes the point. This will be formulated with changes of intensity due to shifting in a local window. The Harris detector is based on the second moment matrix which reflects the local distribution of gradients in the image [3].

In this thesis a novel robust image watermarking by finding corner point based on DWT algorithm is proposed. A square region around feature point is computed. Watermark image is embedded to image and attacks are applied to image and watermark image is extracted.

Main point of the thesis is showing variations of PSNR and SR values on different attacks and comparing SR, PSNR and PSNR after attacks.

1.1. Previous Work and Objective of the Study

In the literature survey stage of this study, a number of references about digital image watermarking have been studied and some sample works are investigated. 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 [4].

FANG and TIAN had a study that is about improved blind watermarking algorithm based on two dimensional DWT. They used Arnold scrambling before embedding the watermark to improve security. In the extracting process, they had used only relevant key without the original image. Their algorithm were applicable for grayscale and color images. [5]

QI and QI had present content based digital image watermarking. They applied various image processing attacks and geometric distortions. They adopted embedded scheme is applied discrete Fourier transform (DFT). Their purpose was to developing reliable feature extraction method under some geometric distortions and efficient triangle generation and matching method. [6]

LU and et al. presented digital image watermarking based on DWT and sub-sampling. Sub-image sequences are constructed as a video segment and watermark is embedded in DWT domain of each sub-image by using video watermarking techniques. [7]

LIU and ZHAO proposed a watermarking method based on feature points detected by using adaptive threshold and it satisfied to decide on most robust feature points. Vertexes of triangle was found by modified Harris corner detection and watermark embedded in this triangle. They used Human Visual System to guarantee the image quality. [8]

To protect copyrights MADANE and SHAH applied an algorithm of digital image watermarking by using DWT. They used principle component analysis (PCA) to learn of low dimensional representation in the context of image. With their algorithm the PCA algorithm is able to detect all types of watermark images. [9]

ZHANG and CHANG proposed an algorithm suitable for blind detection based on DWT. Points are extracted by means features of image from low frequency sub-band of wavelet coefficients. Watermarking is embedded and extracted on these points. They were carried for locating and embedding operation separately and watermarking detection operation needs no participation of original image for information hiding and copyright protection. [10]

YANG et al. also studied with content based watermarking technique that robust geometry attacks. They proposed Multi-scale Curvature Product (MSCP) corner detection algorithm which detect corners from the low frequency components of the images after 3-level lifting wavelet transformation. They compared their second-generation digital image watermarking algorithm with the algorithms of the first generation watermarking. [11]

For watermarking embedding YONGPING proposed watermarking positioning algorithm that uses features of lower frequency sub-band of wavelet coefficient. Positions were used as watermarking embedded indexes. With this algorithm watermarking detection was free from original image. This algorithm could be used for wide spread image transmission. [12]

ZHANG et al. had a study about a new geometric distortion correcting algorithm for wavelet-based watermarked image. To extract feature points used for image correcting they modified Harris-Laplace detector. The algorithm was robust against to geometric attacks and common signals processing methods. [13]

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. [14]

AL-HAJ proposed an algorithm that combine DWT and DCT algorithms. In the first and second level DWT sub-bands of the original image watermarking were embedded, on the selected DWT sub-bands DCT application was embedded. Combination of these transforms algorithms improved the performance that are based only on the DWT. [15]

SHARMA and SAXENA presented watermarking technique for Joint Photographic Expert Group 2000 (JPEG 2000) image with using DWT. [16]

ABDULFETAH et al. proposed an algorithm based on DWT and DCT for copyright protection by adaptive invisible digital watermarking algorithms. Corporation of human visual system (HVS) model into proposed algorithm was effective for protection. [17]

TRIPATHI et al. presented DWT algorithm based on both blind and non-blind embedded algorithms used. They embedded two watermarks into one image for authenticate source image and protect watermark. Their study was different from others in that they protect both original image and watermark. They used pseudo random generator based on the mathematical constant that applying in selecting the watermark pixels, which makes the process more resistant to attacks. [18]

For video copyright protection MASOUMI and AMIRI delivered an algorithm based on DWT. Watermark image is embedded in video I-frames. This algorithm, besides maintaining the high transparency of video stream leads to resist the watermark against a variety of attacks. [19]

Another study of ZHANG et al. is dynamic robust multiple blind watermarking algorithm based on DWT and HVS. They used Arnold transform to transform watermark image. Original image was decomposed to blocks and watermark was embedded into these blocks by adopting just noticeable changes to HVS. [20]

YONGQIANG et al. studied digital watermark properties that are security, imperceptibility and robustness. They proposed their scheme according to these properties. They used two-dimensional chaotic stream encryption; genetic algorithm is used for selecting and modifying the wavelet coefficients and synergetic neural network is used for identifying the owner of extracted watermark. [21]

NA et al. studied on semi-blind watermarking. They improved Kundur quantization algorithm with Arnold scrambling transformation embedding hidden watermarks by decomposing three-level wavelet of image and decomposing bit-plane. [22]

VISWANATHAM and et al. presented a hybrid algorithm combining DWT and DCT. Extraction of watermark information was not needed for the original image, it was blind watermarking. They evaluated their study with PSNR value looking at the correlation between the original and the watermarked image. [23]

1.2. Organization of Thesis

Watermark embedding and extracting algorithms, attacks on watermarked image such as filter attack, scaling attack, Gaussian attack, histogram attack, gamma attack etc. and evaluation of watermarking techniques are explained in the second chapter.

In the third chapter, used methodology and the experimental results are illustrated. Conclusion of this work is explained in the fourth chapter.

In the thesis, digital image watermarking by finding corner point based on DWT algorithm is applied to original image. Cameraman and Lena are standard images that have been used for tests to compare the strength of the algorithm.

CHAPTER 2

DIGITAL WATERMARKING

A huge amount of data increases daily over the Internet. Multimedia data are also stored and copied from the Internet easily. Therefore, intellectual property right protection becomes a very important issue on the Internet. Many techniques are used to protect data such as encryption; however, it does not guarantee that the encrypted data can be decrypted. Digital image watermarking is a copyright protection technology. It is an information hiding technique to protect original image used to hide a mark such as image, audio signal, serial number or text. Also other digital watermarking application areas are apart from copy control and copyright protection; broadcast monitoring, fingerprinting, medical applications and content authentication are other application areas of digital watermarking. Copy Control is controlling the copy protection of images with embedded information in the original multimedia. A given watermark represents copy protected bits in embedding, and detection. Copyright Protection is a technique to protect ownership of data. Owner can embed a watermark representings some invisible copyright information. Broadcast Monitoring is checking the delivery of commercials or TV programs. If watermarks are embedded in commercial advertisements, an automated monitoring system can verify whether advertisements are broadcast as contracted. After embedding multimedia, it should be detected whenever transmitted. Fingerprinting is tracing illegal copies. With fingerprinting, the owner can embed watermarks in the copies of the data that is supplied to different person. Some definitions of digital image watermarking are introduced as follows:

“Digital watermarking is a technique that is used to prevent copy-protected content from re-entering the compliant world after having been copied or transmitted by noncompliant devices [24].”

“Watermarking is the process of encoding hidden copyright information into digital data by making small modifications to the data samples, e.g., pixels [25].”

“Digital watermarking is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object [26].”

In digital watermarking, visible watermark can be seen by eyes, other hand invisible watermarked image cannot visible. Invisible watermarked image is usually used for protection. To detect watermark if original image is used, is non-blind watermarking. If original image is not required, this is blind watermarking. Semi-blind watermark requires seed and watermarked document to detect the watermark.

In digital watermarking, terms that are used watermark embedding, detection and extraction. Watermark embedding is the process of hiding an info or image in the original image. When embedding info in image, it is called embedded or watermarked image. Watermark detection is the process of checking the watermark is in existence or not. Watermark extraction is the process of getting out the info embedded in the image from watermarked image. A watermarking technique should be secure making detection and extraction processes impossible. It should be strong against any type of attacks. It should use invisible watermark.

2.1. Watermarking Methods

There are three watermarking methods in multimedia: spatial domain watermarking, transform domain watermarking and compressed domain watermarking. Spatial domain watermarking embeds a watermark directly to selected pixels in the original image. Transform domain watermarking is inserted into transformed coefficients of image. Discrete wavelet transform, discrete cosine transform and discrete Fourier transform are used to transform domain watermarking technique. Transform domain is more robust than spatial domain watermarking. Compressed domain watermarking is only for audio or video files.

In the thesis transform domain watermarking is used. DCT or DWT can give better results for some different images. DWT, DCT and DFT are explained in detail in the following.

- **Discrete Wavelet Transform:** DWT separates image into four components. These components are approximate (LL), horizontal (HL), vertical (LH) and diagonal sub bands (HH). In the lowest bands (LL) the magnitude of coefficients are larger at decomposition. Embedding watermark in higher level of sub bands (HL, LH, HH) provide efficient robustness of watermark. Figure 1 shows the first level of DWT decomposition. Figure 2 shows the second level of DWT decomposition.

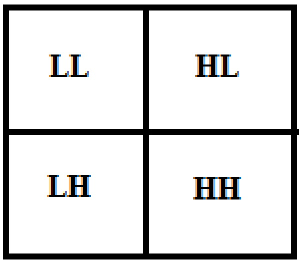


Figure 1. First Level of DWT decomposition

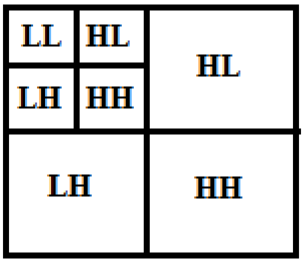


Figure 2. Second Level of DWT decomposition

- **Discrete Cosine Transform:** DCT separates 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 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.

2.2. Attacks on Watermarked Image

One of the digital watermarking issues is that watermark should be robust against several attacks. There are several attacks such as direct or indirect, geometric, and statistical attacks. Some attacks are defined below:

- **Filter Attack:** Filtering attacks are linear filtering such as high pass, low pass filtering midpoint, local median etc.
- **Scaling Attack:** Scaling is a geometric attack. Changing the size of the image, and bringing it back to the original size. For instance, if a watermarked image size is 256x256, it is resized to 128 x 128 and back to 256 x 256.
- **Gaussian Attack:** Gaussian attack is a signal processing attack that should detect watermark after signal processing.
- **Histogram Equalization Attack:** Histogram equalization attack is a signal processing attack. It is a technique for increasing the details of an image that is lacking in contrast. This technique changes the intensity levels in the image to cause the image to conform to some desired histogram.
- **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.
- **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. This increases the contrast of the output image.
- **Noise (Pepper & Salt) Attack:** Adding salt and pepper noise to the image with noise density. This affects the pixels.

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

2.3. Evaluation of Watermarking

Measurement of image quality is a challenging problem in many applications to attacks. Objective measures of images are mean square error, peak signal to noise ratio and similarity ratio.

- **Mean Square Error:** MSE is a measure of control and quality. The MSE is defined as follows

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

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

- **Peak Signal to Noise Ratio:** The PSNR is used as a measure of quality of reconstruction in image watermarking. It is a ratio between the maximum value of a signal and the magnitude of background noise [27]. It is most easily defined via MSE for an 8-bit gray scale image as shown

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

- **Similarity Ratio:** SR is used in evaluation of non-blind watermark extraction. SR provides high precision for binary image watermarks. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR is defined as

$$SR = S/(S + D)$$

where S and D represent the number of matching pixel values in compared images and the number of different pixel values in compared images respectively.

CHAPTER 3

METHODOLOGY

In this thesis, employing corner detector, watermark embedding, several images attacks watermark extracting algorithm were used.

Firstly, corners of image were found with Harris corner detector. Then, one corner point from found corners was elected. After that, a square with edge 70 was drawn and this square was cropped from the original image.

Then, the watermark image was embedded to this cropping image Watermark embedding procedure is as input is a cropped image (A) and binary image watermark (W), output is watermarked image (AW). First, using DWT, decompose the cover work, A, into four sub bands: LL, LH, HL, and HH. Then, decompose LL band into LU factorization with its components L, D and U. Apply SVD to D and apply SVD to W. after this applying, modify SDw, the singular values of D component, by adding the singular values of the watermark, W, with the scaling factor α. Since the singular value of the watermark image is directly added to the singular values of D with the scaling factor, it is wise to reconstruct D by updated coefficient Dw. Because the diagonal matrix (D) of LL sub band is updated, it is time to gather L, Dww and U to obtain LL1w. After that, compute the inverse DWT to obtain the watermarked cover image, AW. Finally, store the locations of 1's in W in order to use them as a key in the extracting algorithm [4].

After that, several image attacks were applied on the original image, which are "Filter Attacks", "Scaling, Gaussian Attacks", "Histogram Equalization Attacks", "Gamma correction Attacks"," JPEG Compression Attacks", "Rotation Attacks", "Intensity Adjustment Attacks", "Noise Attack Pepper & Salt", "Speckle Noise Attacks", "Decoding Attacks", to watermark image.

Finally, watermark extracting algorithm procedure is as input is attacked watermarked image (AW*) that shows same corner point cropped image and the output is extracted watermark (W*). First, using DWT, watermarked and possibly attacked image, AW* is decomposed, into four sub bands: LLw, LHw, HLw, and HHw. Then LLw is decomposed into LU factorization with its components and SVD is applied to D*. After that, extract the singular values of the watermark Sw* and the watermark with its SVD components are extracted. Finally, the key which is the location of pixels stored in the embedding algorithm is used. If the mean value of pixels in the key (TH) for W* is positive, assign that pixel value to binary 0, otherwise to binary 1. After the extract image, MSE, PSNR and SR are calculated and compared for each attacks.

Steps of proposed algorithm are shown in Figure 3.

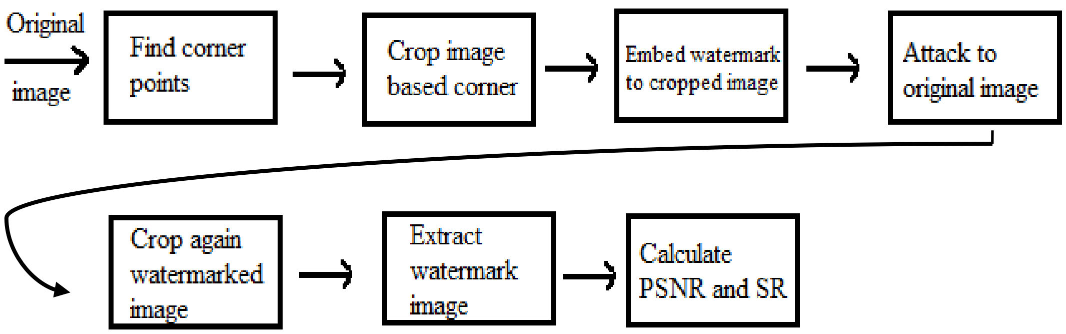


Figure 3. Steps of proposed algorithm

3.1. Experiments

First image used is shown in Figure 4 that is Cameraman image respectively are 8 bit 256x256 gray scale images.

Figure 4. Cameraman

Image shown in Figure 5 is used as the watermark is a binary image in size 36x36.

Figure 5. Watermark Image

Two hundred corner points are detected with Harris corner method that finds feature points. All corner points are shown in Figure 6.

Figure 6. 200 corner points

One example of the corner point that is detected with Harris method is shown in Figure 7. In this study two hundred different corner points and square region are used. However, 157 numbers of result were taken because of some points not being in the region of the cropped image. While the corner point being detected, crop image 70 x 70 and embed the watermark. After that, ten different attacks are applied for each corner point.

Figure 7. One corner point example of image

Image that watermark applied and original image shown in Figure 8. Used invisible watermarking that watermark is not visible as shown.

a. b.

Figure 8. a. Original image, b. Watermarked image

Using DWT, decompose the original image into four bands that are LL, LH, HL, and HH. Figure 9 shows that one level of DWT on example corner. Apply SVD to sub band LL. Apply SVD to watermark image.

Figure 9. One level DWT for cropped image

MATLAB was used for all ten different attacks these are filter attack, scaling, Gaussian attacks, histogram equalization attacks, gamma correction attack, JPEG compression attacks, rotation attack, intensity adjustment attack, noise attack Pepper & Salt, speckle noise attacks.

These attacks parameters are filter attack used window size is 3x3 with using two dimensional correlation, scaling attack resized image 256 to 128, Gaussian attack mean is zero, variance is 0.001, histogram equalization attack used automatic, Gamma attack used gamma is 1.5 that mapping is weighted toward lower output values, JPEG compression used quality is 25, rotation attack used 20^{o} angle, intensity adjustment used low and high intensities 0 and 1, pepper & salt noise attack used noise density 0.2, speckle noise attack used variance 0.2. The attacked images are shown in Figures 10-19.

Figure 10. Filter Attack

Figure 11. Scaling Attack

Figure 12. Gaussian Attack

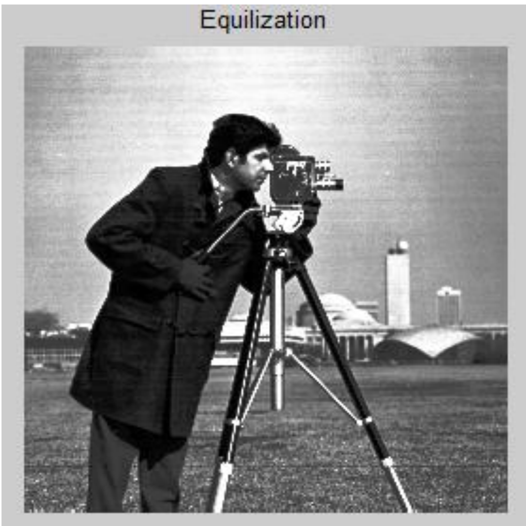


Figure 13. Histogram Equalization Attack

Figure 14. Gamma Correction Attack

Figure 15. JPEG Compression Attack

Figure 16. Rotation Attack

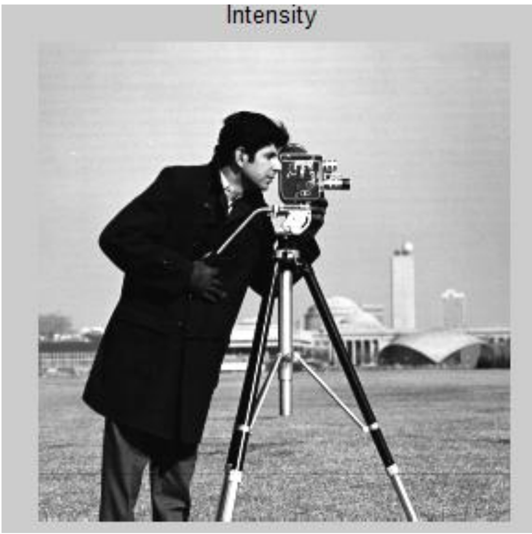


Figure 17. Intensity Adjustment Attack

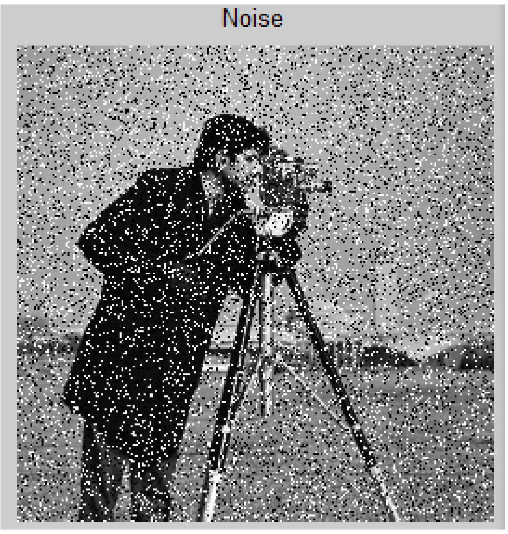


Figure 18. Pepper & Salt Noise Attack

Figure 19. Speckle Noise Attack

In this thesis, some quality measures were used to find measurement of image quality. These are MSE that is proven measure of control and quality, PSNR that is used as a measure of quality of reconstruction in image watermarking, and SR that is a division of representing the number of matching pixel values in compared images and the number of different pixel values in compared images respectively.

For Filter Attack, Figure 20 shows PSNR values of original and attacked image and Figure 21 shows SR value of attacked image.

Figure 20. PSNR values of original and filter attacked image

Figure 21. SR value of watermarked image after filter attack

For Scaling Attack, Figure 22 shows PSNR values of original and attacked image and Figure 23 shows SR value of attacked image.

Figure 22. PSNR values of original and scaling attacked image

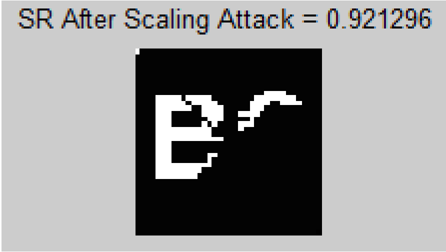


Figure 23. SR value of watermarked image after scaling attack

For Gaussian Attack, Figure 24 shows PSNR values of original and attacked image and Figure 25 shows SR value of attacked image.

Figure 24. PSNR values of original and Gaussian attacked image

Figure 25. SR value of watermarked image after Gaussian attack

For Histogram Equalization Attack, Figure 26 shows PSNR values of original and attacked image and Figure 27 shows SR value of attacked image.

Figure 26. PSNR values of original and histogram equalization attacked image

Figure 27. SR value of watermarked image after histogram equalization attack

For Gamma Correction Attack, Figure 28 shows PSNR values of original and attacked image and Figure 29 shows SR value of attacked image.

Figure 28. PSNR values of original and gamma correction attacked image

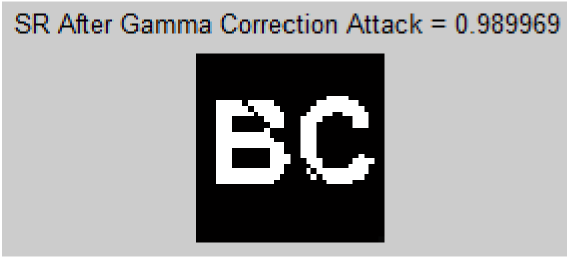


Figure 29. SR value of watermarked image after gamma correction attack

For JPEG Compression Attack, Figure 30 shows PSNR values of original and attacked image and Figure 31 shows SR value of attacked image.

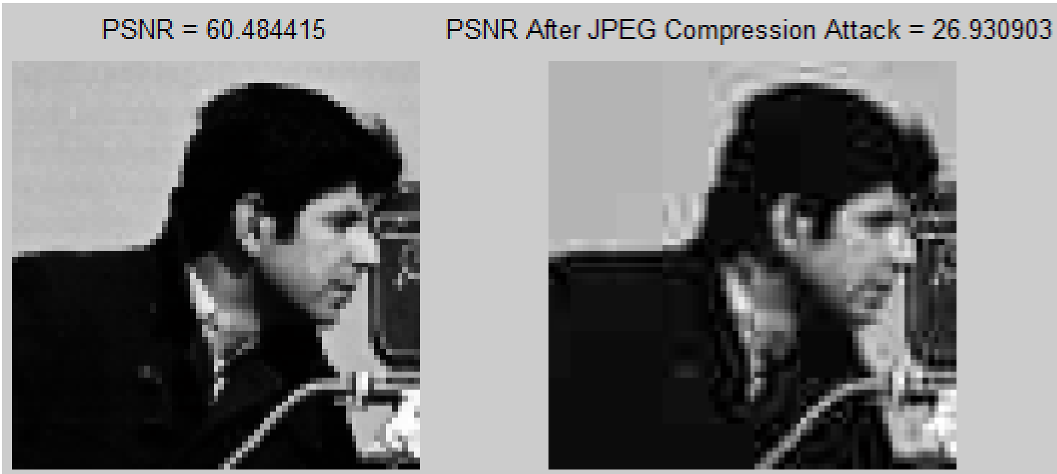


Figure 30. PSNR values of original and JPEG compression attacked image

Figure 31. SR value of watermarked image after JPEG compression attack

For Rotation Attack, Figure 32 shows PSNR values of original and attacked image and Figure 33 shows SR value of attacked image.

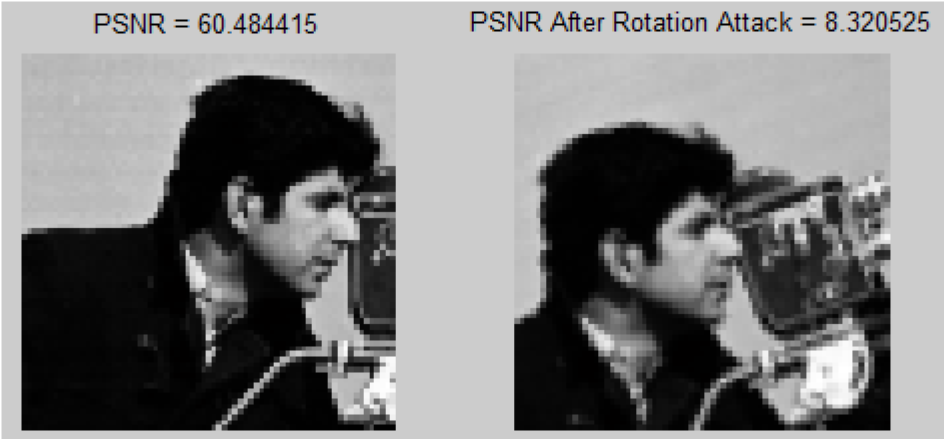


Figure 32. PSNR values of original and rotation attacked image

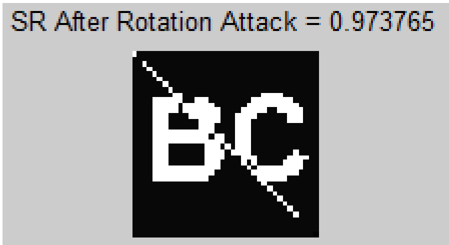


Figure 33. SR value of watermarked image after rotation attack

For Intensity Adjustment Attack, Figure 34 shows PSNR values of original and attacked image and Figure 35 shows SR value of attacked image.

Figure 34. PSNR values of original and intensity adjustment attacked image

Figure 35. SR value of watermarked image after intensity adjustment attack

For Noise Pepper & Salt Attack, Figure 36 shows PSNR values of original and attacked image and Figure 37 shows SR value of attacked image.

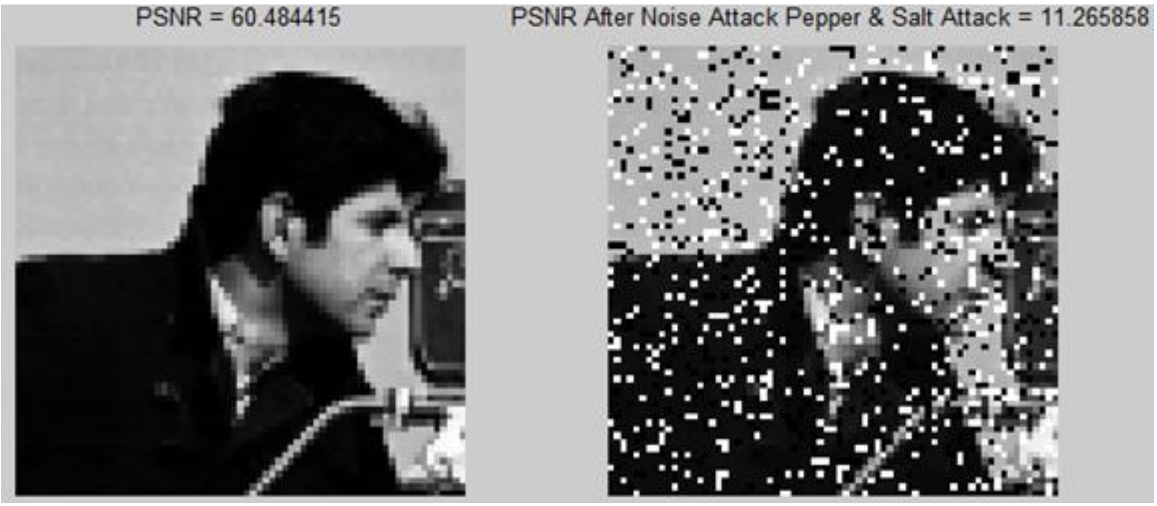


Figure 36. PSNR values of original and pepper & salt noise attacked image

Figure 37. SR value of watermarked image after pepper & salt noise attack

For Speckle Noise Attack, Figure38 shows PSNR values of original and attacked image and Figure 39 shows SR value of attacked image.

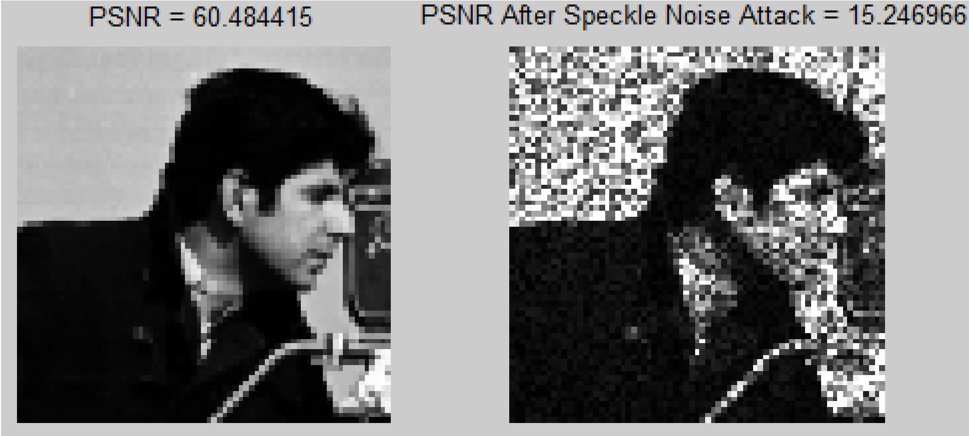


Figure 38. PSNR values of original and speckle noise attacked image

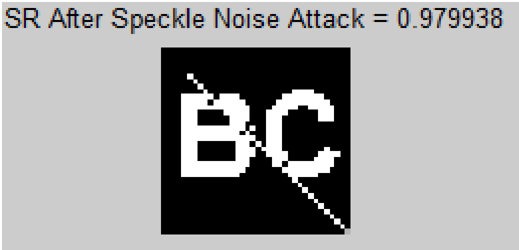


Figure 39. SR value of watermarked image after speckle noise attack

Table 1. PSNR, PSNR_After and SR Values of First Corner Point

Attacks	PSNR	PSNR_After	SR
Filter Attack	60,484415	23,239781	0,957562
Scaling Attack	60,484415	21,813470	0,921296
Gaussian Attack	60,484415	30,304466	0,981481
Histogram Equalization Attack	60,484415	17,522895	0,975309
Gamma Correction Attack	60,484415	21,197943	0,989969
Jpeg Correction Attack	60,484415	26,930903	0,986883
Rotation Attack	60,484415	8,320525	0,973765
Intensity Adjustment Attack	60,484415	19,285868	0,986883
Noise Attack	60,484415	11,265858	0,980710
Speckle Noise Attack	60,484415	15,246966	0,979938

In Table 1 the PSNR and SR values are calculated for image and respectively presented. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images; original and watermarked image. The higher the PSNR shows the better the quality of the compressed or reconstructed image. For two images that are perfect copies of each other PSNR value is infinity. Since PSNR is in logarithmic scale slight improvements are sufficient. For instance, PSNR before histogram equalization attack is 60.484415; this value is watermarked image's PSNR value. But its PSNR value changed after histogram equalization attack. It could be 17.522895. This difference between PSNR values, show us, this image not an original watermarked image. So, original watermarked images had some change. The SR between two images is used as quality measurement; it is calculated similarity between watermark images after and before attack. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR for original watermark image is 1. Recovered watermarks quality under the above attacks is assessed based on subjective evaluation of SR. In all attacked cases the SR value is more than 0.92. If the original watermarked image, PSNR and SR values are same or similar before attack and after attack.

Second example of corner point is shown in Figure 40.

Figure 40. Second corner point example

Image that watermark applied and original image shown in Figure 41. Used invisible watermarking that watermark is not visible as shown.

a. b.

Figure 41. a. Original image, b. Watermarked image

Using DWT, decompose the original image into four bands that are LL, LH, HL, and HH. Figure 42 shows that one level of DWT on example corner. Apply SVD to sub-band LL. Apply SVD to watermark image.

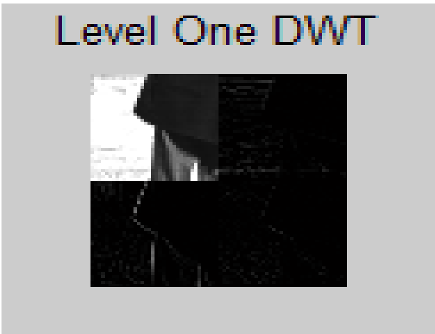


Figure 42. One level DWT for second corner point example

For Filter Attack, Figure 43 shows PSNR values of original and attacked image and Figure 44 shows SR value of attacked image.

Figure 43. PSNR values of original and filter attacked image

Figure 44. SR value of watermarked image after filter attack

For Scaling Attack, Figure 45 shows PSNR values of original and attacked image and Figure 46 shows SR value of attacked image.

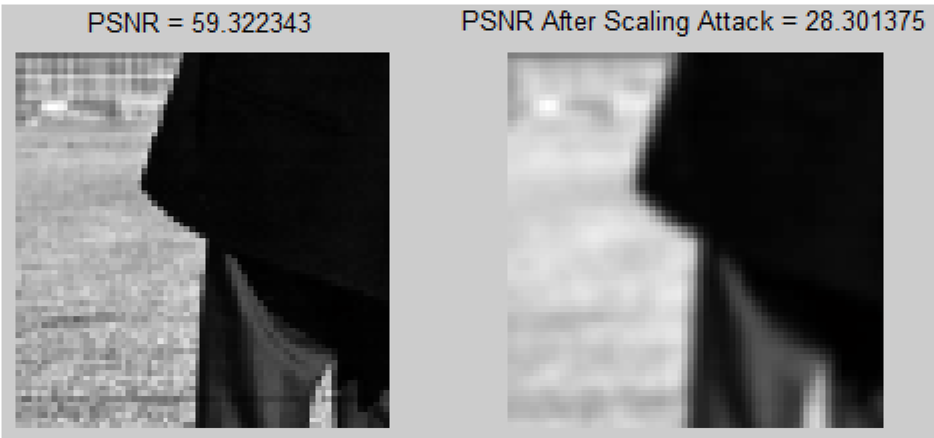


Figure 45. PSNR values of original and scaling attacked image

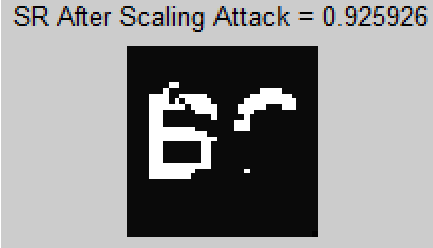


Figure 46. SR value of watermarked image after scaling attack

For Gaussian Attack, Figure 47 shows PSNR values of original and attacked image and Figure 48 shows SR value of attacked image.

Figure 47. PSNR values of original and Gaussian attacked image

Figure 48. SR value of watermarked image after Gaussian attack

For Histogram Equalization Attack, Figure 49 shows PSNR values of original and attacked image and Figure 50 shows SR value of attacked image.

Figure 49. PSNR values of original and histogram equalization attacked image

Figure 50. SR value of watermarked image after histogram equalization attack

For Gamma Correction Attack, Figure 51 shows PSNR values of original and attacked image and Figure 52 shows SR value of attacked image.

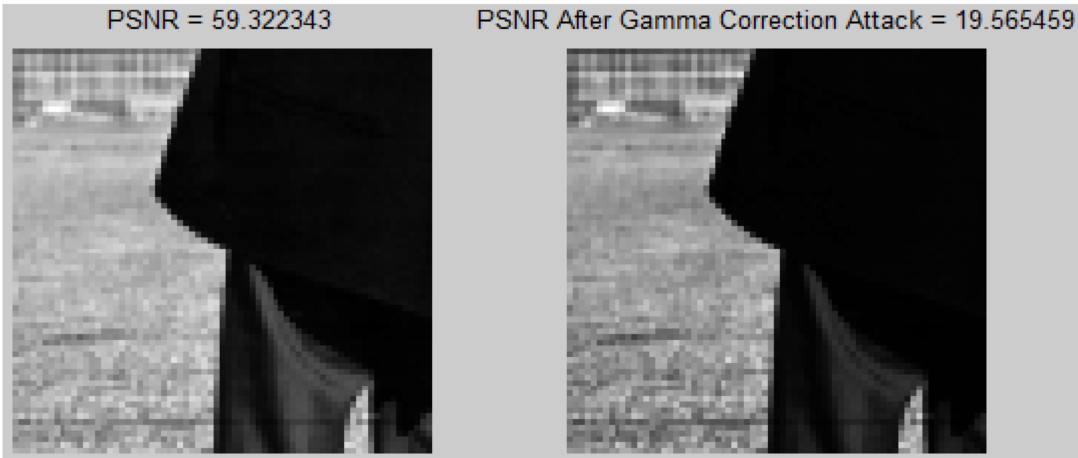


Figure 51. PSNR values of original and gamma correction attacked image

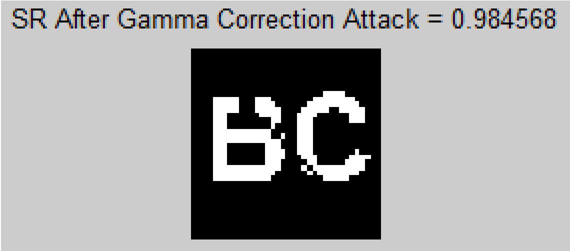


Figure 52. SR value of watermarked image after gamma correction attack

For JPEG Compression Attack, Figure 53 shows PSNR values of original and attacked image and Figure 54 shows SR value of attacked image.

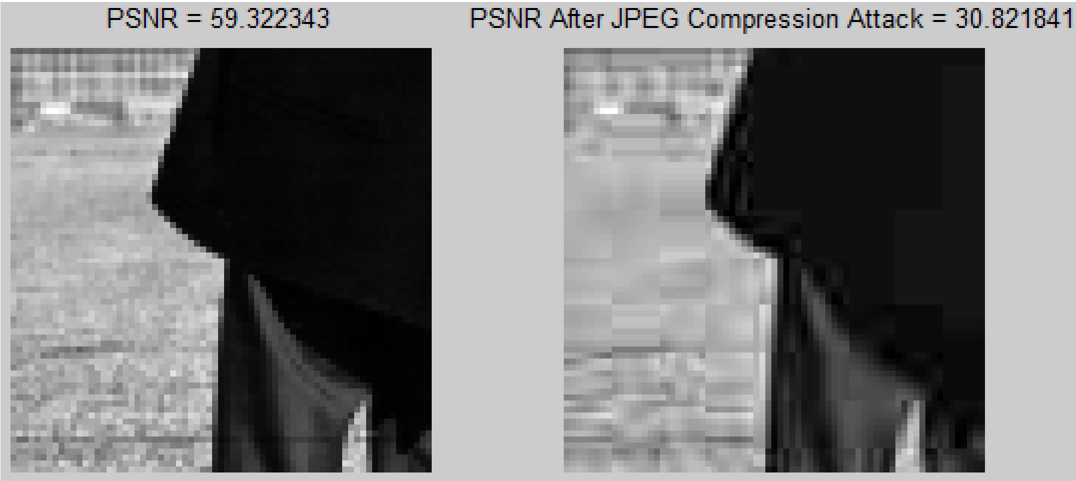


Figure 53. PSNR values of original and JPEG compression attacked image

Figure 54. SR value of watermarked image after JPEG compression attack

For Rotation Attack, Figure 55 shows PSNR values of original and attacked image and Figure 56 shows SR value of attacked image.

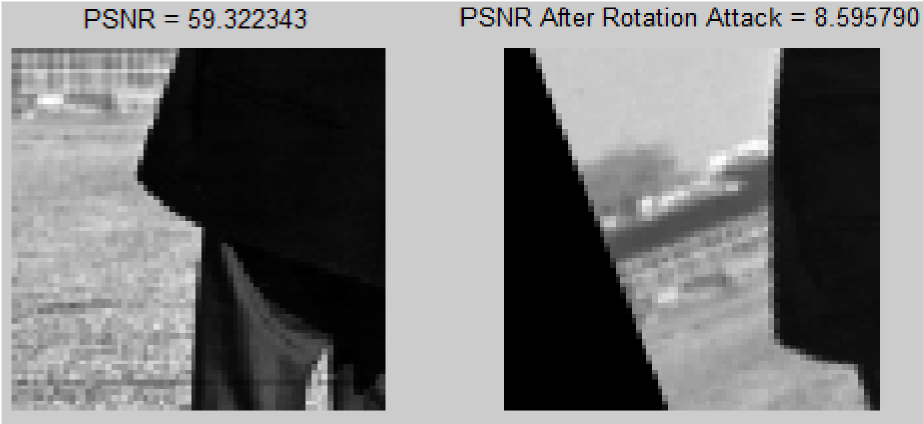


Figure 55. PSNR values of original and rotation attacked image

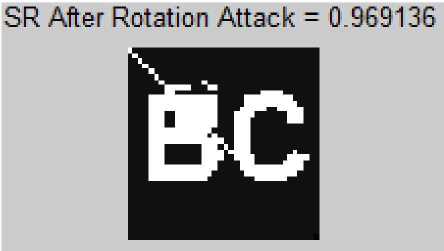


Figure 56. SR value of watermarked image after rotation attack

For Intensity Adjustment Attack, Figure 57 shows PSNR values of original and attacked image and Figure 58 shows SR value of attacked image.

Figure 57. PSNR values of original and intensity adjustment attacked image

Figure 58. SR value of watermarked image after intensity adjustment attack

For Noise Pepper & Salt Attack, Figure 59 shows PSNR values of original and attacked image and Figure 60 shows SR value of attacked image.

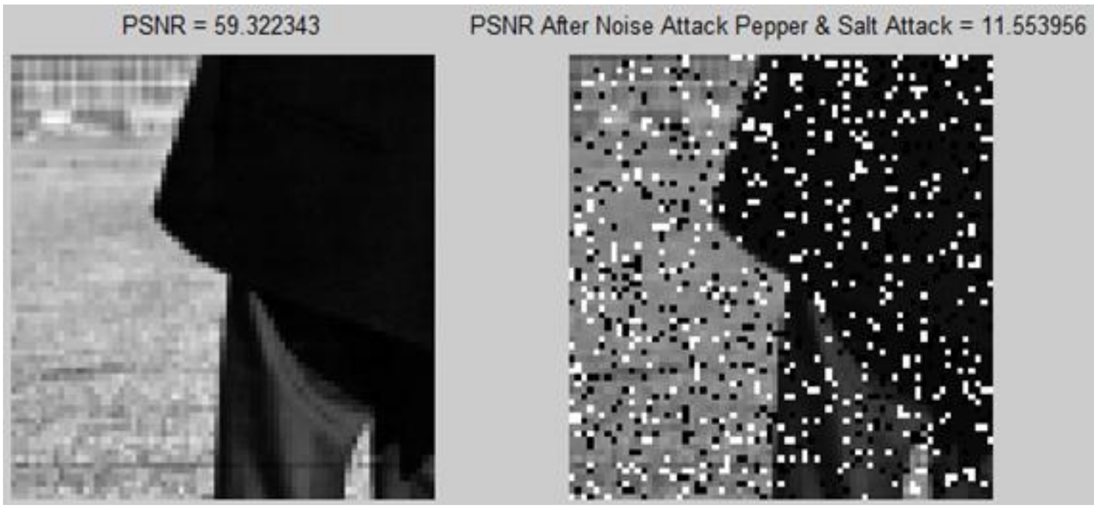


Figure 59. PSNR values of original and pepper & salt noise attacked image

Figure 60. SR value of watermarked image after pepper & salt noise attack

For Speckle Noise Attack, Figure 61 shows PSNR values of original and attacked image and Figure 62 shows SR value of attacked image.

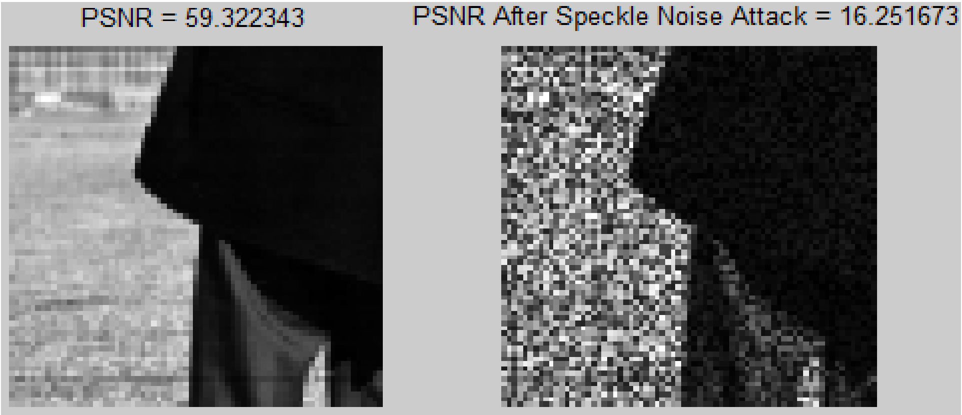


Figure 61. PSNR values of original and speckle noise attacked image

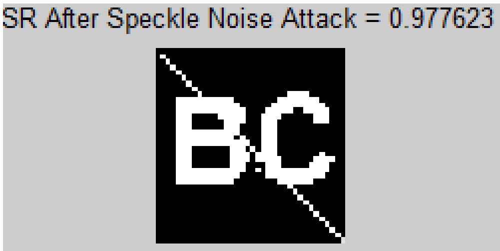


Figure 62. SR value of watermarked image after speckle noise attack

Table 2. PSNR, PSNR_After and SR Values of Second Corner Point

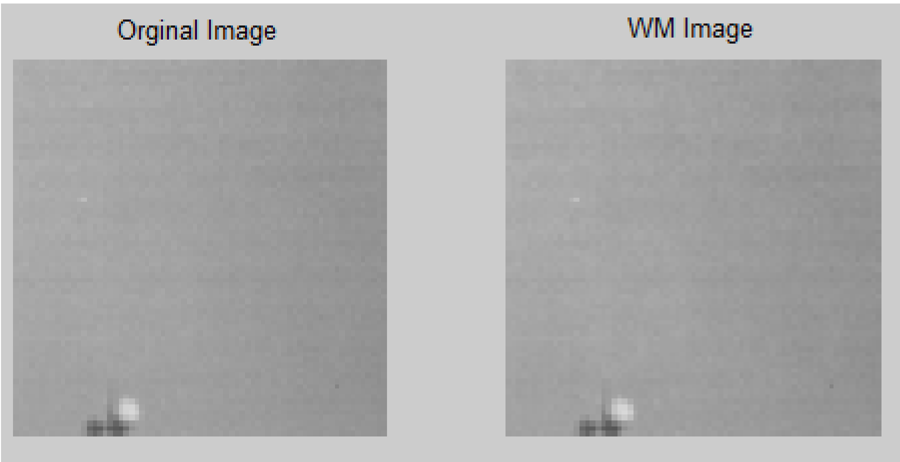
Attacks	PSNR	PSNR_After	SR
Filter Attack	59,322343	28,166853	0,958333
Scaling Attack	59,322343	28,301375	0,925926
Gaussian Attack	59,322343	30,190835	0,976852
Histogram Equalization Attack	59,322343	22,781750	0,979938
Gamma Correction Attack	59,322343	19,565459	0,984568
Jpeg Correction Attack	59,322343	30,821841	0,990741
Rotation Attack	59,322343	8,595790	0,969136
Intensity Adjustment Attack	59,322343	21,105403	0,982253
Noise Attack	59,322343	11,553956	0,979167
Speckle Noise Attack	59,322343	16,251673	0,977623

In Table 2 the PSNR and SR values are calculated for image and respectively presented. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images; original and watermarked image. The higher the PSNR shows the better the quality of the compressed or reconstructed image. For two images that are perfect copies of each other PSNR value is infinity. Since PSNR is in logarithmic scale slight improvements are sufficient. For instance, PSNR before rotation attack is 59,322343; this value is watermarked image's PSNR value. But its PSNR value changed after rotation attack. It could be 8,595790. This difference between PSNR values, show us, this image not an original watermarked image. So, original watermarked images had some change. The SR between two images is used as quality measurement; it is calculated similarity between watermark images after and before attack. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR for original watermark image is 1. Recovered watermarks quality under the above attacks is assessed based on subjective evaluation of SR. In all attacked cases the SR value is more than 0.92. If the original watermarked image, PSNR and SR values are same or similar before attack and after attack.

To compare PSNR and SR values, also studied with non-corner point. 140 different points that were not equal to corners selected randomly. One of the non-corner point examples is shown Figure 63.

Figure 63. Non-corner point example

Image that watermark applied and original image shown in Figure 64. Used invisible watermarking that watermark is not visible as shown.



a. b.

Figure 64. a. Original image, b. Watermarked image

Using DWT, decompose the original image into four bands that are LL, LH, HL, and HH. Figure 65 shows that one level of DWT on example corner. Apply SVD to sub-band LL. Apply SVD to watermark image.

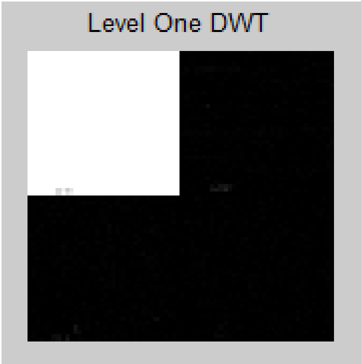


Figure 65. One level DWT for non-corner point example

For Filter Attack, Figure 66 shows PSNR values of original and attacked image and Figure 67 shows SR value of attacked image.

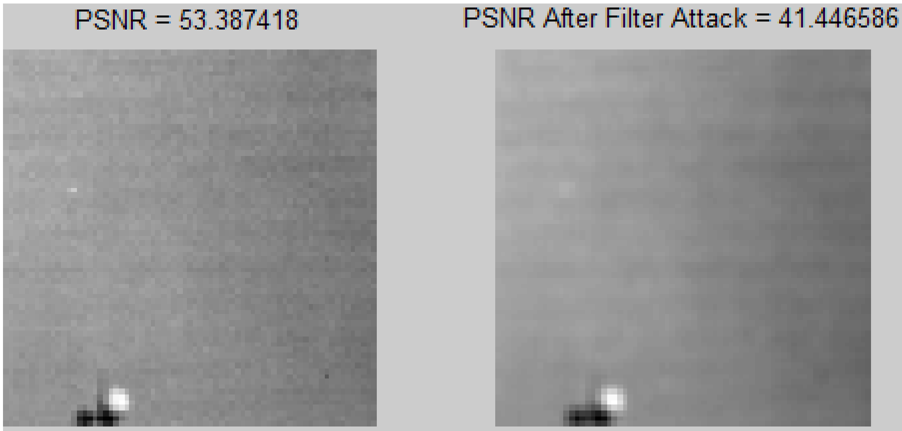


Figure 66. PSNR values of original and filter attacked image

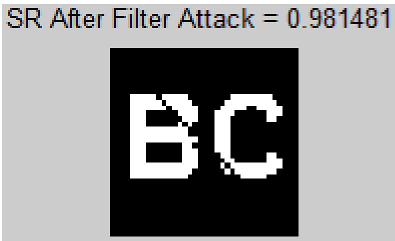


Figure 67. SR value of watermarked image after filter attack

For Scaling Attack, Figure 68 shows PSNR values of original and attacked image and Figure 69 shows SR value of attacked image.

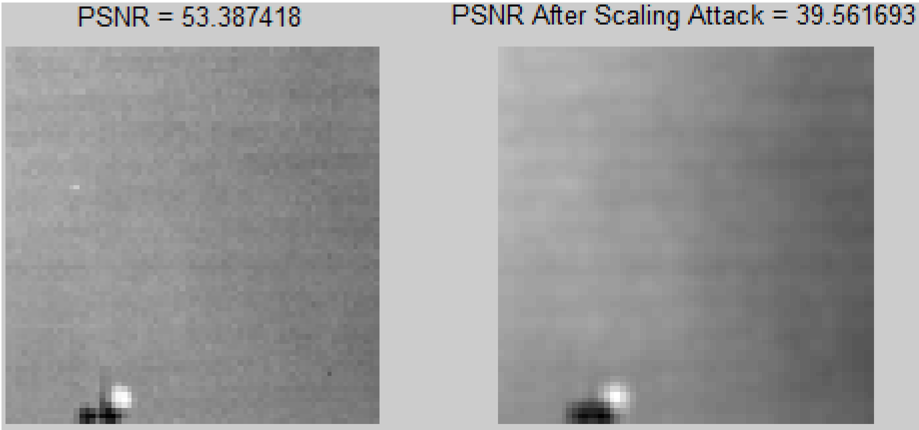


Figure 68. PSNR values of original and scaling attacked image

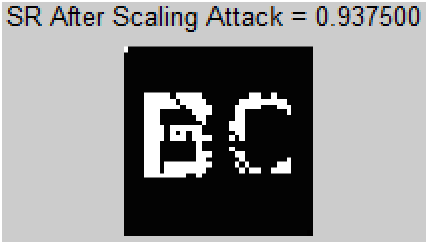


Figure 69. SR value of watermarked image after scaling attack

For Gaussian Attack, Figure 70 shows PSNR values of original and attacked image and Figure 71 shows SR value of attacked image.

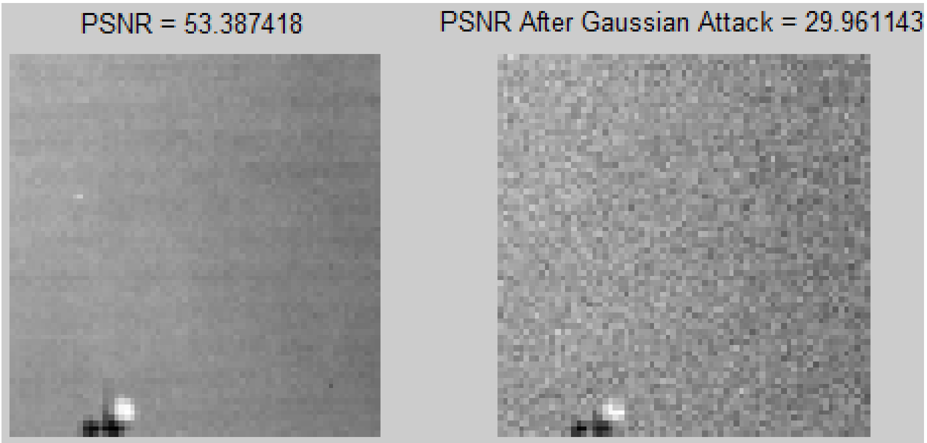


Figure 70. PSNR values of original and Gaussian attacked image

Figure 71. SR value of watermarked image after Gaussian attack

For Histogram Equalization Attack, Figure 72 shows PSNR values of original and attacked image and Figure 73 shows SR value of attacked image.

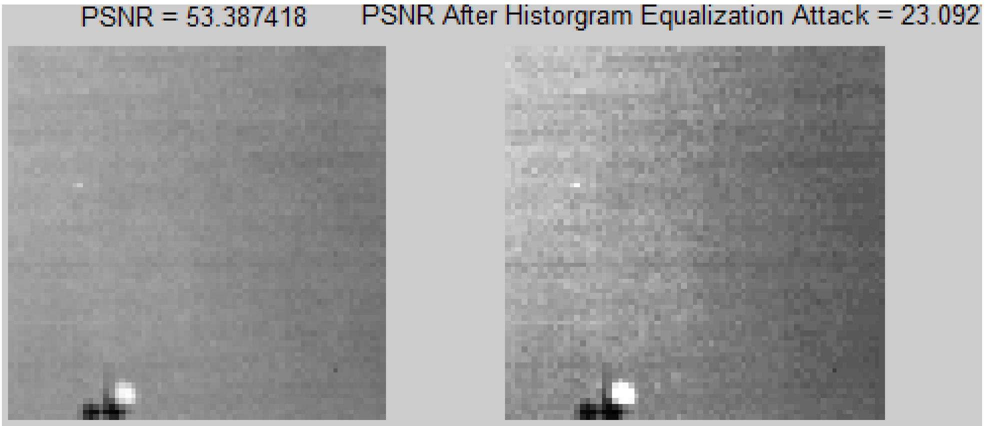


Figure 72. PSNR values of original and histogram equalization attacked image

Figure 73. SR value of watermarked image after histogram equalization attack

For Gamma Correction Attack, Figure 74 shows PSNR values of original and attacked image and Figure 75 shows SR value of attacked image.

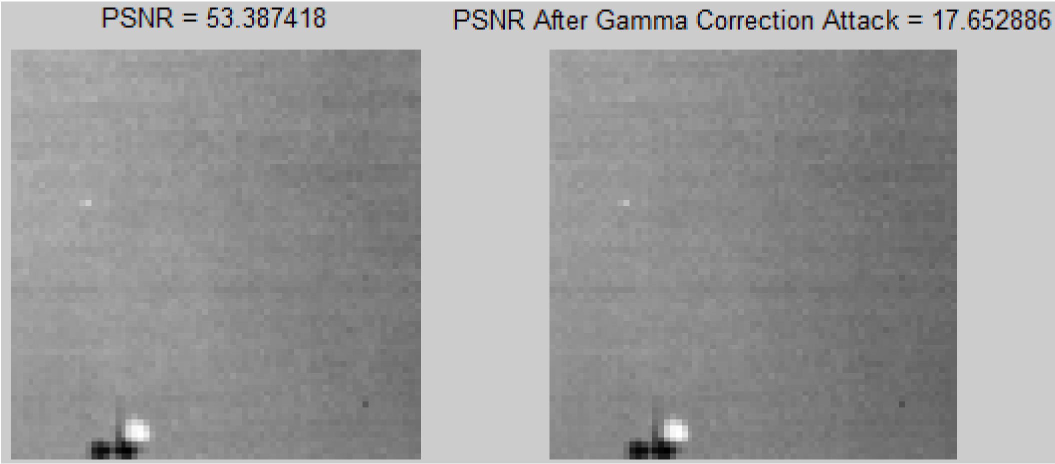


Figure 74. PSNR values of original and gamma correction attacked image

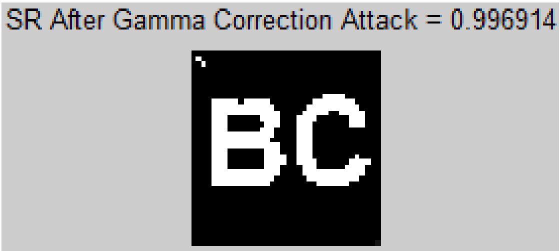


Figure 75. SR value of watermarked image after gamma correction attack

For JPEG Compression Attack, Figure 76 shows PSNR values of original and attacked image and Figure 77 shows SR value of attacked image.

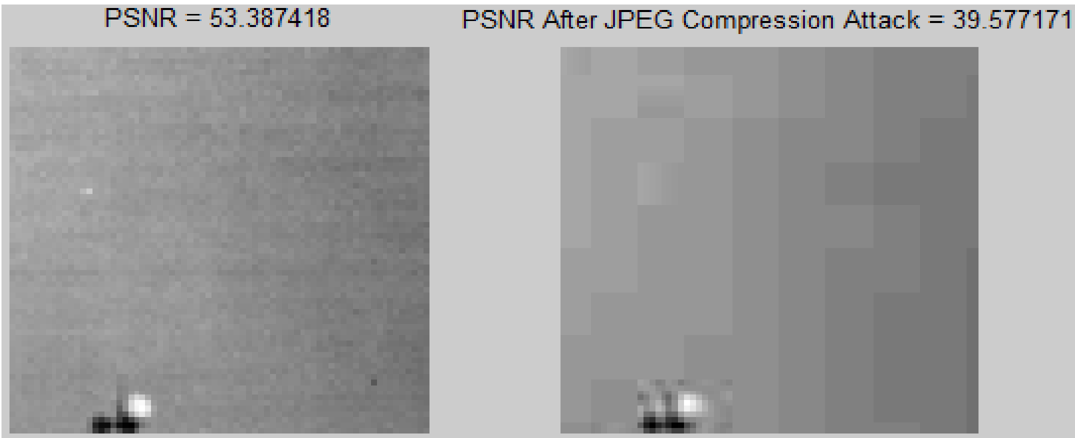


Figure 76. PSNR values of original and JPEG compression attacked image

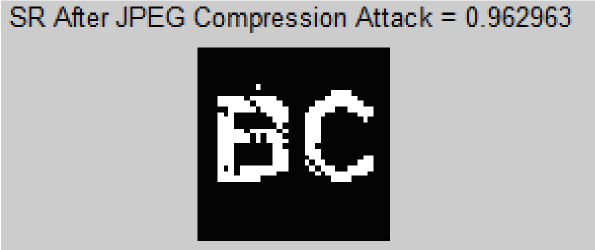


Figure 77. SR value of watermarked image after JPEG compression attack

For Rotation Attack, Figure 78 shows PSNR values of original and attacked image and Figure 79 shows SR value of attacked image.

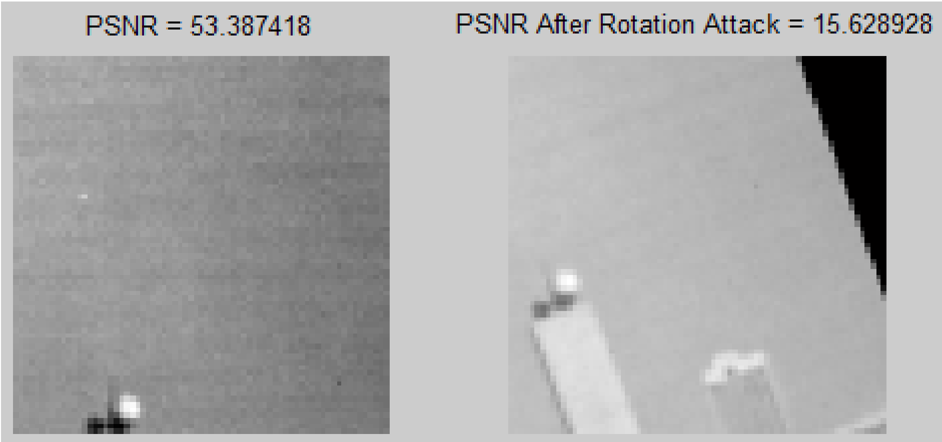


Figure 78. PSNR values of original and rotation attacked image

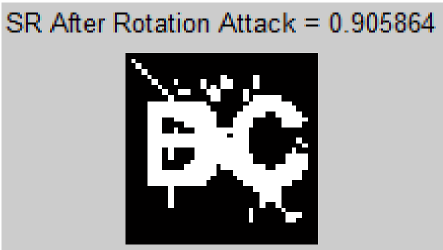


Figure 79. SR value of watermarked image after rotation attack

For Intensity Adjustment Attack, Figure 80 shows PSNR values of original and attacked image and Figure 81 shows SR value of attacked image.

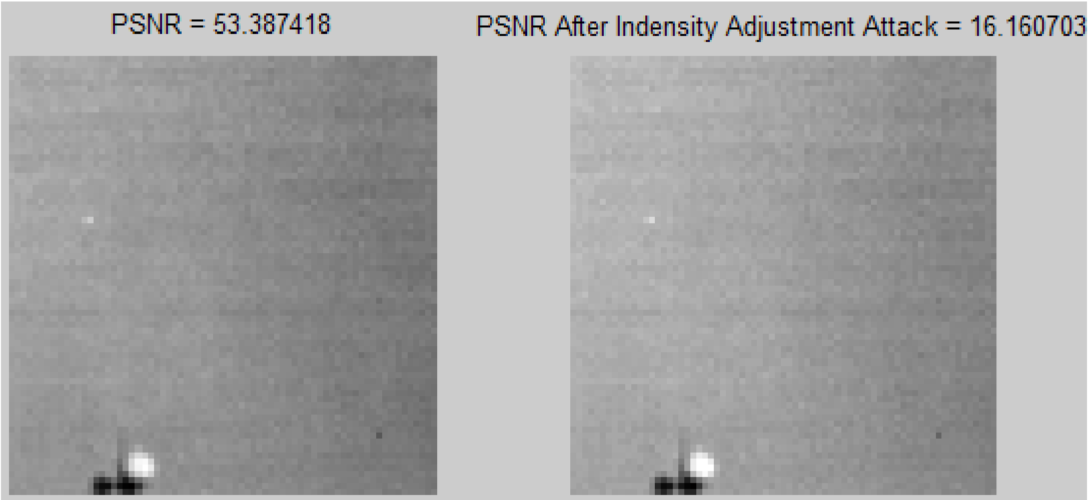


Figure 80. PSNR values of original and intensity adjustment attacked image

Figure 81. SR value of watermarked image after intensity adjustment attack

For Noise Pepper & Salt Attack, Figure 82 shows PSNR values of original and attacked image and Figure 83 shows SR value of attacked image.

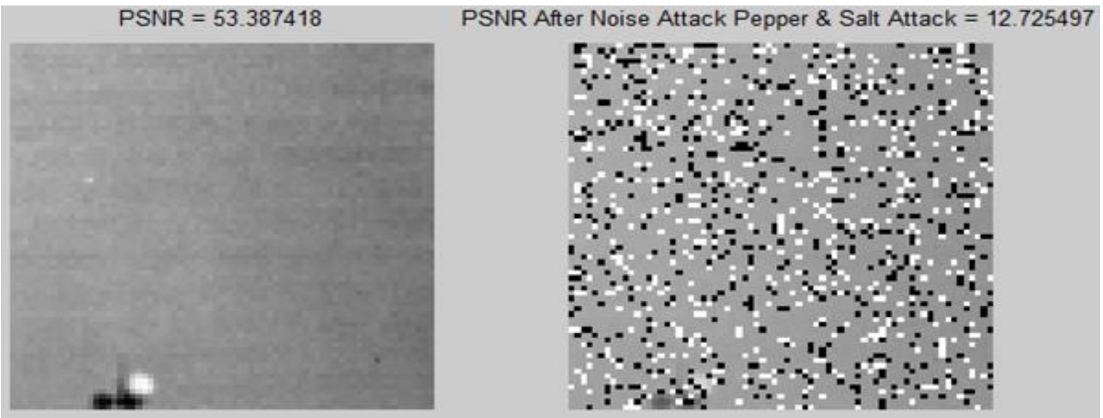


Figure 82. PSNR values of original and pepper & salt noise attacked image

Figure 83. SR value of watermarked image after pepper & salt noise attack

For Speckle Noise Attack, Figure 84 shows PSNR values of original and attacked image and Figure 85 shows SR value of attacked image.

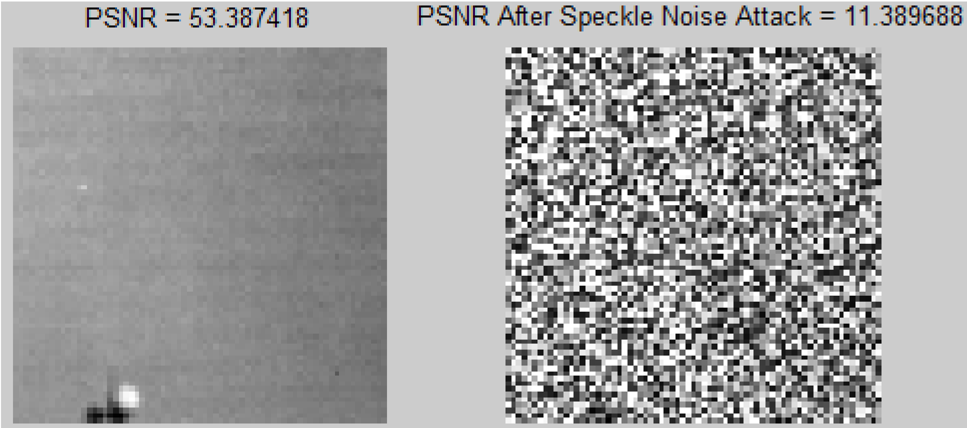


Figure 84. PSNR values of original and speckle noise attacked image

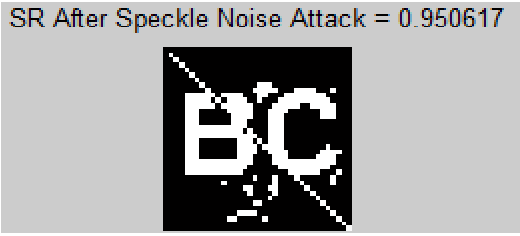


Figure 85. SR value of watermarked image after speckle noise attack

Table 3. PSNR, PSNR_After and SR Values of Non Corner Point

Attacks	PSNR	PSNR_After	SR
Filter Attack	53.387418	41.446586	0.981481
Scaling Attack	53.387418	39.561693	0.937500
Gaussian Attack	53.387418	29.961143	0.973765
Histogram Equalization Attack	53.387418	23.092000	0.979938
Gamma Correction Attack	53.387418	17.652886	0.996914
Jpeg Correction Attack	53.387418	39.577171	0.962963
Rotation Attack	53.387418	15.628928	0.905864
Intensity Adjustment Attack	53.387418	16.160703	0.996914
Noise Attack	53.387418	12.725497	0.964506
Speckle Noise Attack	53.387418	11.389688	0.950617

In Table 3 the PSNR and SR values are calculated for image and respectively presented. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images; original and watermarked image. The higher the PSNR shows the better the quality of the compressed or reconstructed image. For two images that are perfect copies of each other PSNR value is infinity. Since PSNR is in logarithmic scale slight improvements are sufficient. For instance, PSNR before gamma correction attack is 53.387418; this value is watermarked image's PSNR value. But its PSNR value changed after gamma correction attack. It could be 17.652886. This difference between PSNR values, show us, this image not an original watermarked image. So, original watermarked images had some change. The SR between two images is used as quality measurement; it is calculated similarity between watermark images after and before attack. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR for original watermark image is 1. Recovered watermarks quality under the above attacks is assessed based on subjective evaluation of SR. In all attacked cases the SR value is more than 0.9. If the original watermarked image, PSNR and SR values are same or similar before attack and after attack.

Moreover, proposed algorithm is also used for different image named Lena. Lena image respectively 8 bit and 256x256 gray scale images. Same watermark image is used.

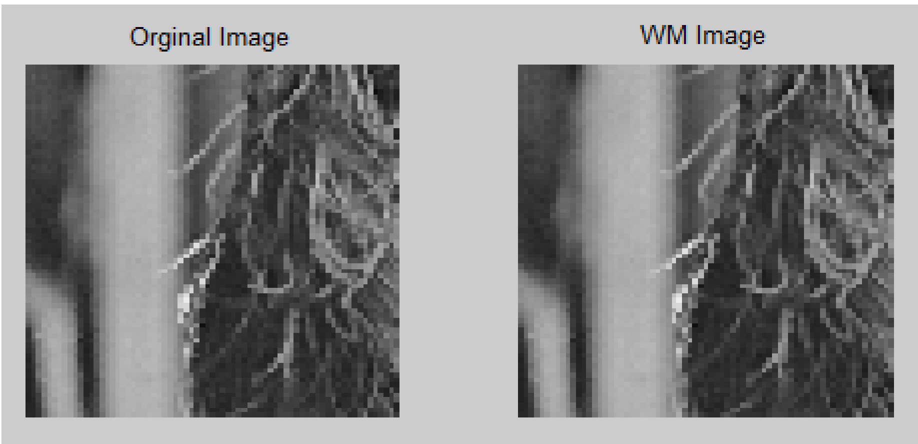
Figure 86. Lena

Figure 87. 200 corner points of Lena

One example of the corner point that is detected with Harris method is shown in Figure 88. For Lena image again used two hundred different corner points and square region. However, taked 134 numbers of result because of some points not in region of cropped image. While corner point is detecting, crop image 70 x 70 and embed the watermark. After that, ten different attacks applied for each corner point.

Figure 88. One corner point example of Lena image

Image that watermark applied and original image shown in Figure 89. Used invisible watermarking that watermark is not visible as shown.



a. b.

Figure 89. a. Original image, b. Watermarked image

Using DWT, decompose the original image into four bands that are LL, LH, HL, and HH. Figure 90 shows that one level of DWT on example corner. Apply SVD to sub-band LL. Apply SVD to watermark image.

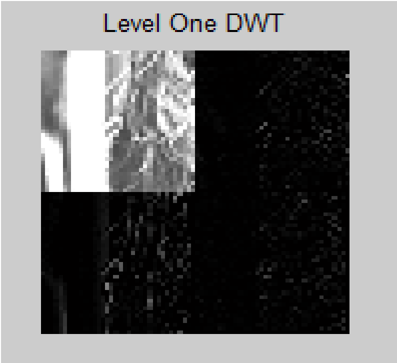


Figure 90. One level DWT for cropped image

Same ten different attacks also applied to Lena image. Measurement values PSNR and SR values shown in following.

For Filter Attack, Figure 91 shows PSNR values of original and attacked image and Figure 92 shows SR value of attacked image.

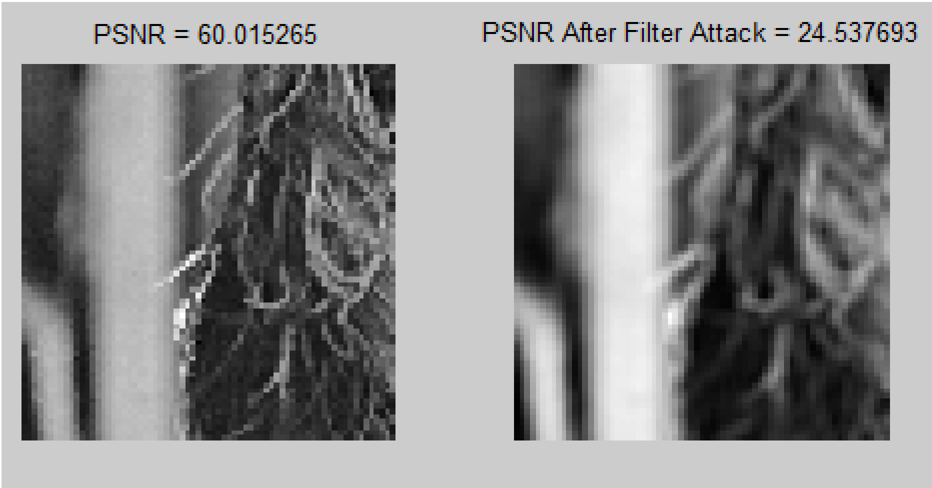


Figure 91. PSNR values of original and filter attacked image

Figure 92. SR value of watermarked image after filter attack

For Scaling Attack, Figure 93 shows PSNR values of original and attacked image and Figure 94 shows SR value of attacked image.

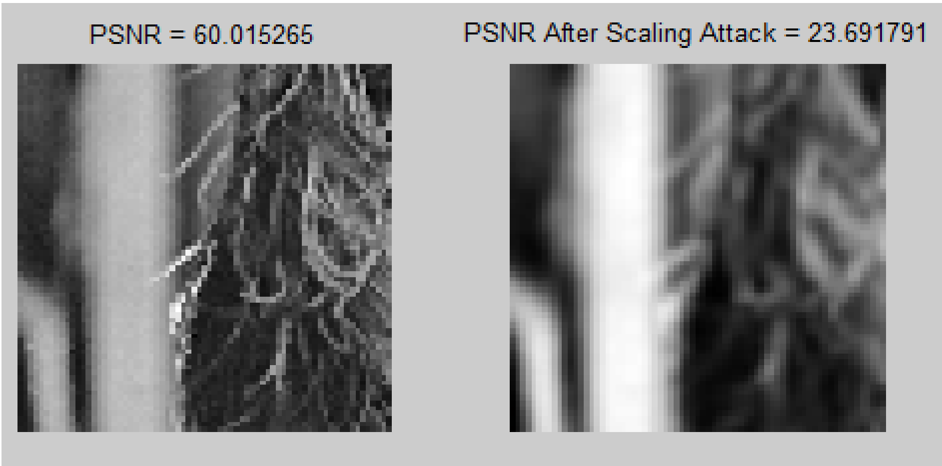


Figure 93. PSNR values of original and scaling attacked image

Figure 94. SR value of watermarked image after scaling attack

For Gaussian Attack, Figure 95 shows PSNR values of original and attacked image and Figure 96 shows SR value of attacked image.

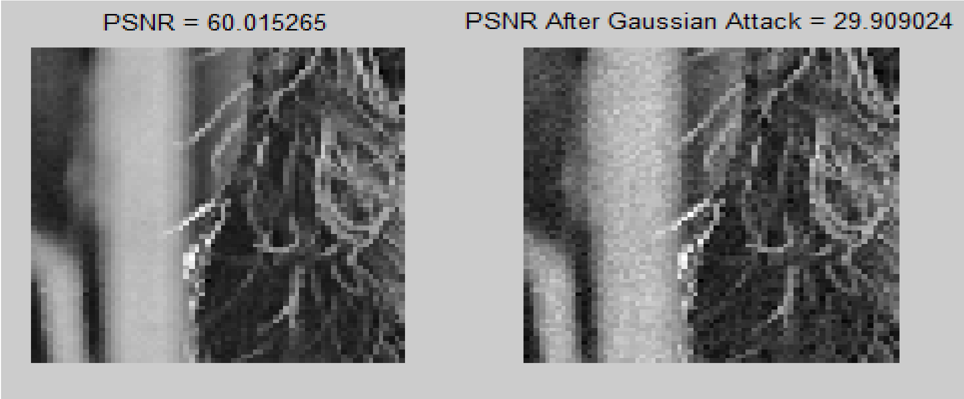


Figure 95. PSNR values of original and Gaussian attacked image

Figure 96. SR value of watermarked image after Gaussian attack

For Histogram Equalization Attack, Figure 97 shows PSNR values of original and attacked image and Figure 98 shows SR value of attacked image.

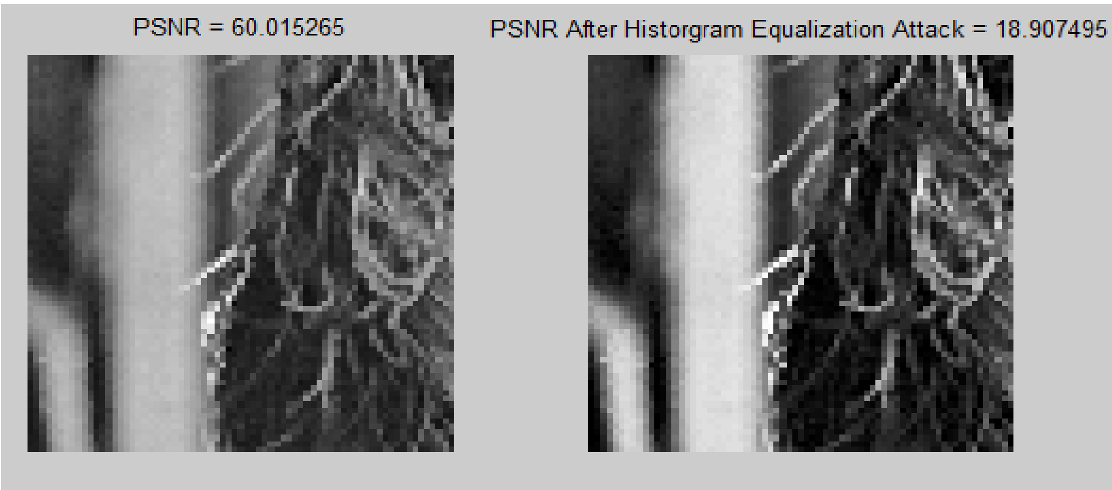


Figure 97. PSNR values of original and histogram equalization attacked image

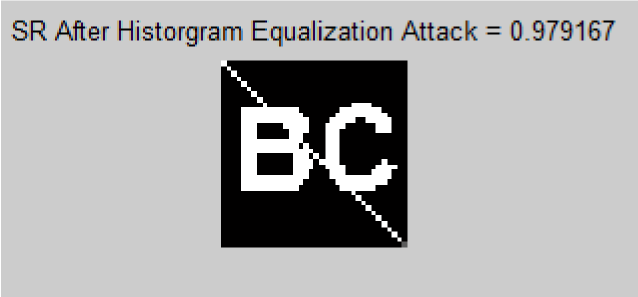


Figure 98. SR value of watermarked image after histogram equalization attack

For Gamma Correction Attack, Figure 99 shows PSNR values of original and attacked image and Figure 100 shows SR value of attacked image.

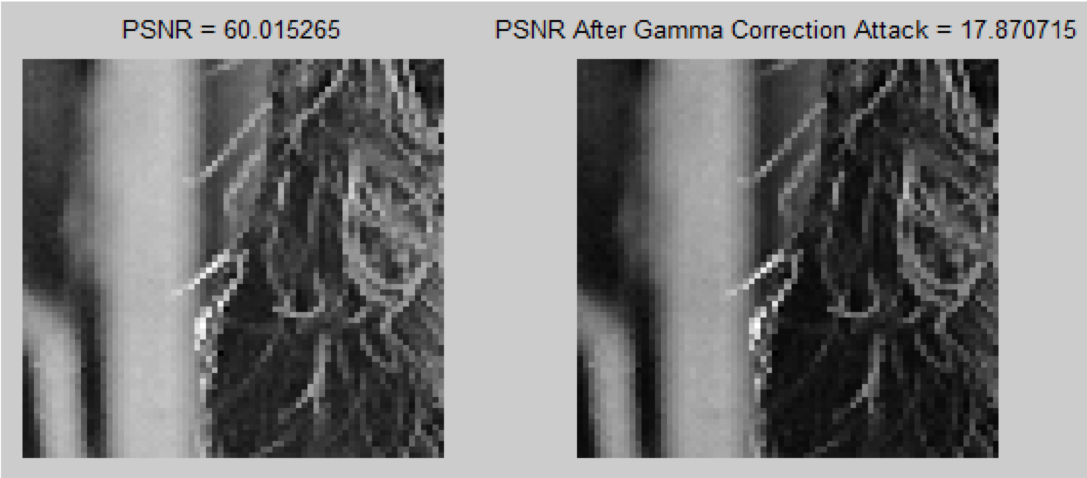


Figure 99. PSNR values of original and gamma correction attacked image

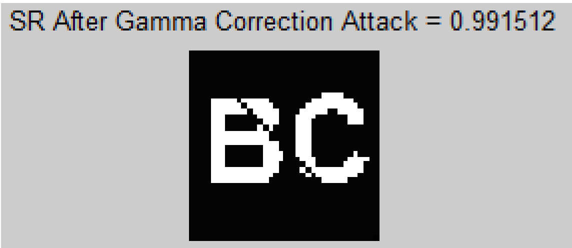


Figure 100. SR value of watermarked image after gamma correction attack

For JPEG Compression Attack, Figure 101 shows PSNR values of original and attacked image and Figure 102 shows SR value of attacked image.

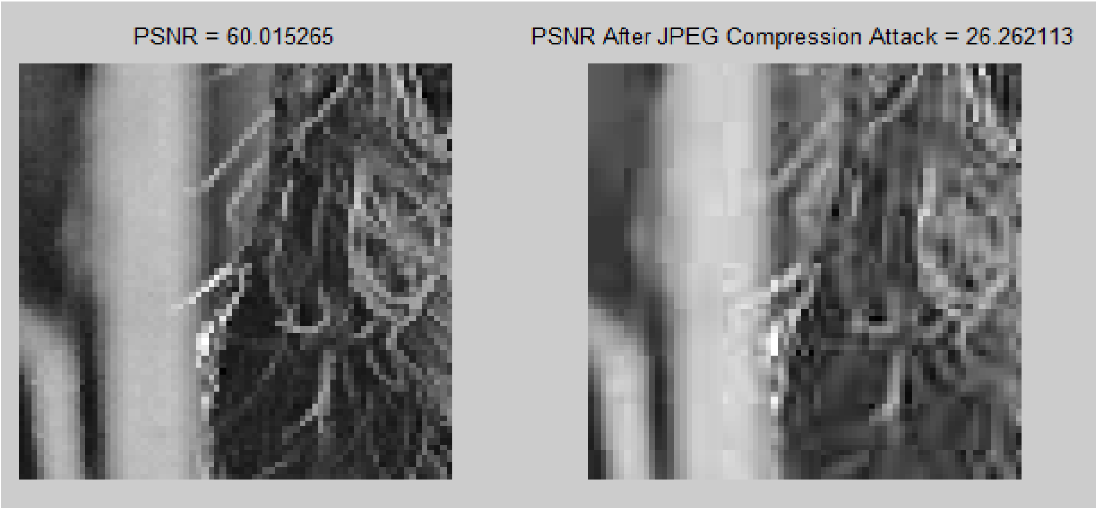


Figure 101. PSNR values of original and JPEG compression attacked image

Figure 102. SR value of watermarked image after JPEG compression attack

For Rotation Attack, Figure 103 shows PSNR values of original and attacked image and Figure 104 shows SR value of attacked image.

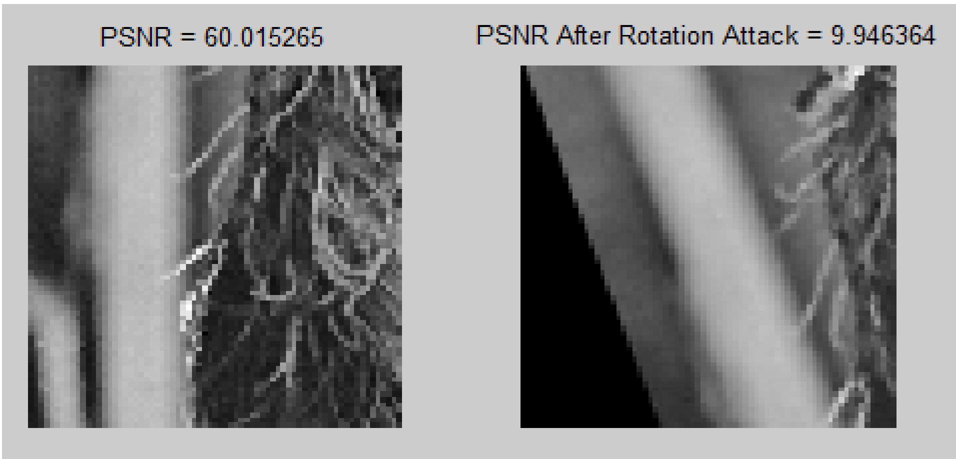


Figure 103. PSNR values of original and rotation attacked image

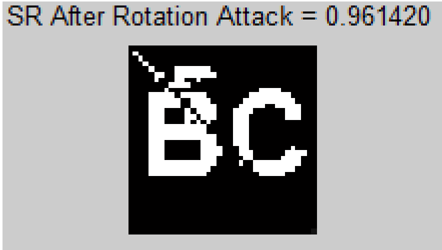


Figure 104. SR value of watermarked image after rotation attack

For Intensity Adjustment Attack, Figure 105 shows PSNR values of original and attacked image and Figure 106 shows SR value of attacked image.

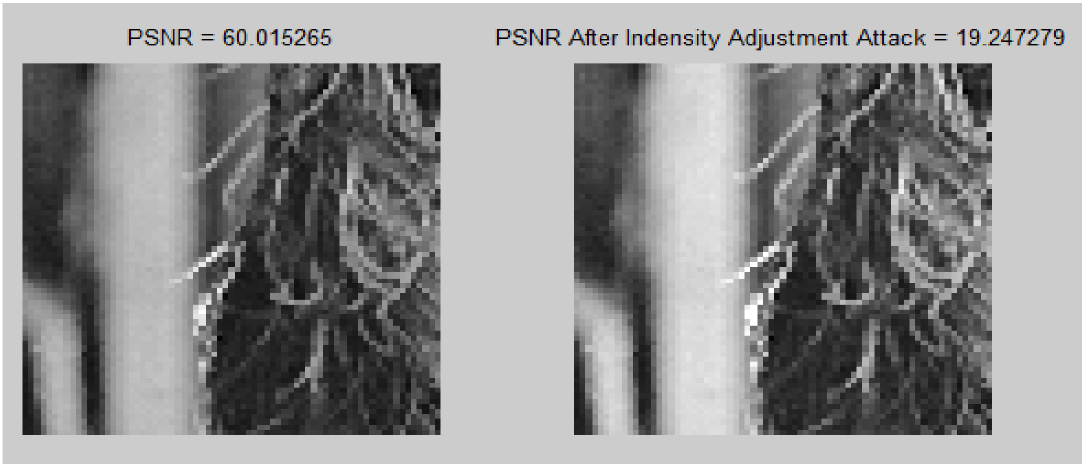


Figure 105. PSNR values of original and intensity adjustment attacked image

Figure 106. SR value of watermarked image after intensity adjustment attack

For Noise Pepper & Salt Attack, Figure 107 shows PSNR values of original and attacked image and Figure 108 shows SR value of attacked image.

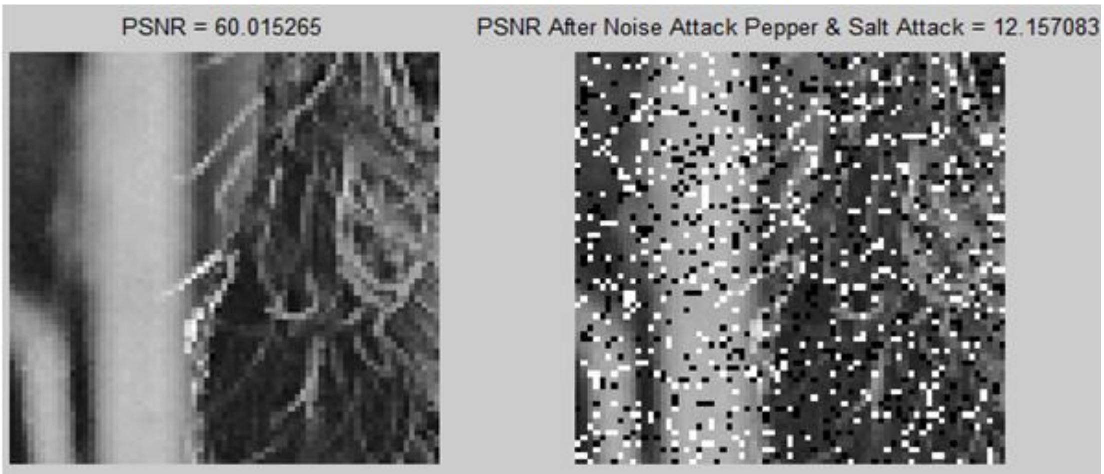


Figure 107. PSNR values of original and pepper & salt noise attacked image

Figure 108. SR value of watermarked image after pepper & salt noise attack

For Speckle Noise Attack, Figure 109 shows PSNR values of original and attacked image and Figure 110 shows SR value of attacked image.

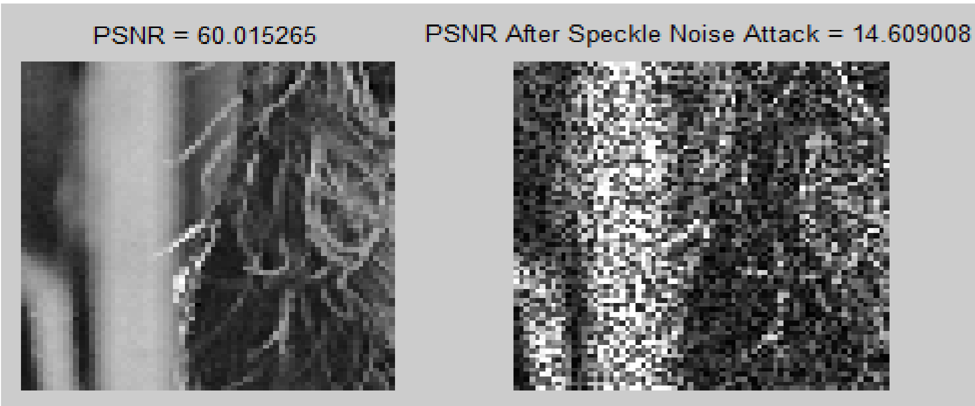


Figure 109. PSNR values of original and speckle noise attacked image

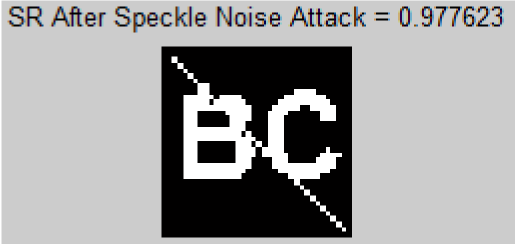


Figure 110. SR value of watermarked image after speckle noise attack

Table 4. PSNR, PSNR_After and SR Values of Corner Point of Lena

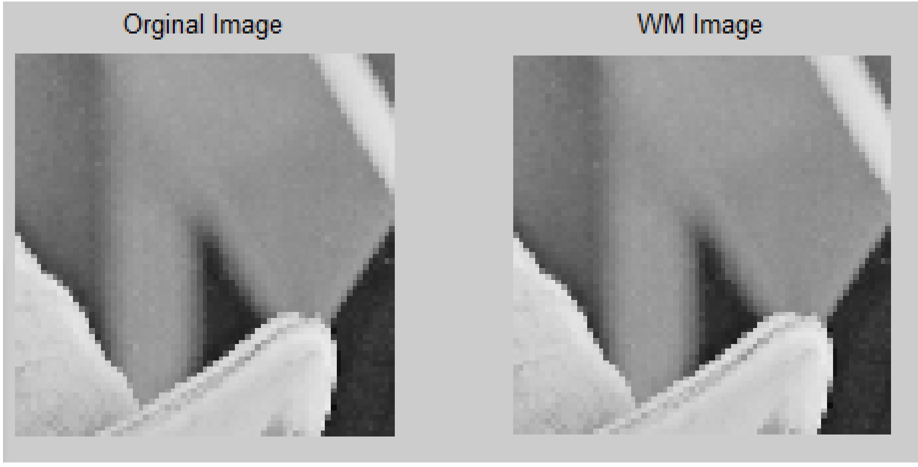
Attacks	PSNR	PSNR_After	SR
Filter Attack	60.015265	24.537693	0.954475
Scaling Attack	60.015265	23.691791	0.897377
Gaussian Attack	60.015265	29.909024	0.983025
Histogram Equalization Attack	60.015265	18.907495	0.979167
Gamma Correction Attack	60.015265	17.870715	0.991512
Jpeg Correction Attack	60.015265	26.262113	0.986111
Rotation Attack	60.015265	9.946364	0.961420
Intensity Adjustment Attack	60.015265	19.247279	0.982253
Noise Attack	60.015265	12.157083	0.977623
Speckle Noise Attack	60.015265	14.609008	0.977623

In Table 4 the PSNR and SR values are calculated for image and respectively presented. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images; original and watermarked image. The higher the PSNR shows the better the quality of the compressed or reconstructed image. For two images that are perfect copies of each other PSNR value is infinity. Since PSNR is in logarithmic scale slight improvements are sufficient. For instance, PSNR before filter attack is 60.015265; this value is watermarked image's PSNR value. But its PSNR value changed after filter attack. It could be 24.537693. This difference between PSNR values, show us, this image not an original watermarked image. So, original watermarked images had some change. The SR between two images is used as quality measurement; it is calculated similarity between watermark images after and before attack. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR for original watermark image is 1. Recovered watermarks quality under the above attacks is assessed based on subjective evaluation of SR. In all attacked cases the SR value is more than 0.9. If the original watermarked image, PSNR and SR values are same or similar before attack and after attack.

Second example of corner point is shown in Figure 111.

Figure 111. Second corner point example of Lena image

Image that watermark applied and original image shown in Figure 112. Used invisible watermarking that watermark is not visible as shown.



a. b.

Figure 112. a. Original image, b. Watermarked image

Using DWT, decompose the original image into four bands that are LL, LH, HL, and HH. Figure 113 shows that one level of DWT on example corner. Apply SVD to sub-band LL. Apply SVD to watermark image.

Figure 113. One level DWT for cropped image

For Filter Attack, Figure 114 shows PSNR values of original and attacked image and Figure 115 shows SR value of attacked image.

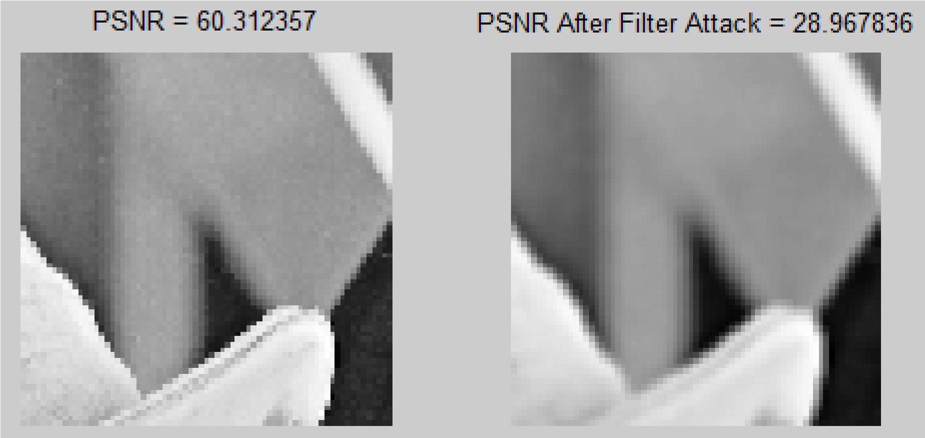


Figure 114. PSNR values of original and filter attacked image

Figure 115. SR value of watermarked image after filter attack

For Scaling Attack, Figure 116 shows PSNR values of original and attacked image and Figure 117 shows SR value of attacked image.

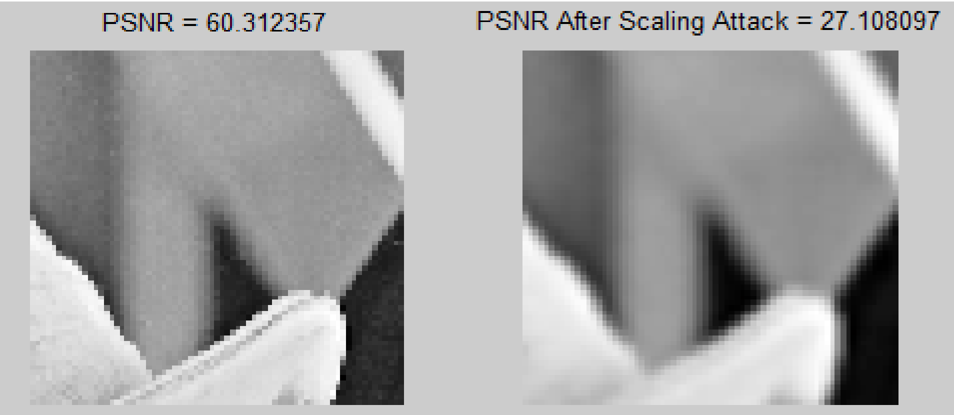


Figure 116. PSNR values of original and scaling attacked image

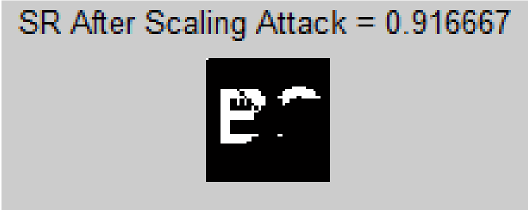


Figure 117. SR value of watermarked image after scaling attack

For Gaussian Attack, Figure 118 shows PSNR values of original and attacked image and Figure 119 shows SR value of attacked image.

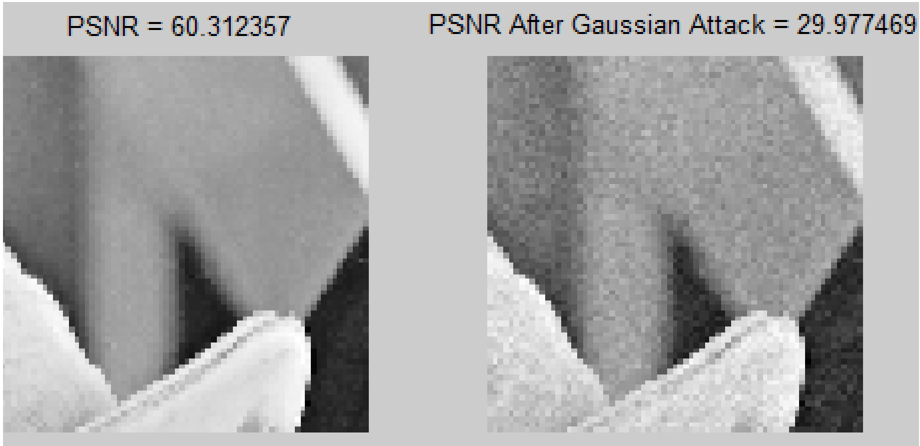


Figure 118. PSNR values of original and Gaussian attacked image

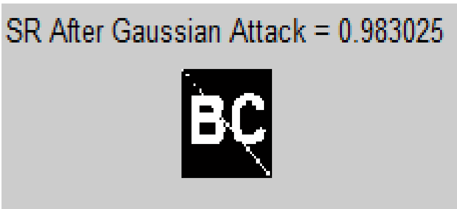


Figure 119. SR value of watermarked image after Gaussian attack

For Histogram Equalization Attack, Figure 120 shows PSNR values of original and attacked image and Figure 121 shows SR value of attacked image.

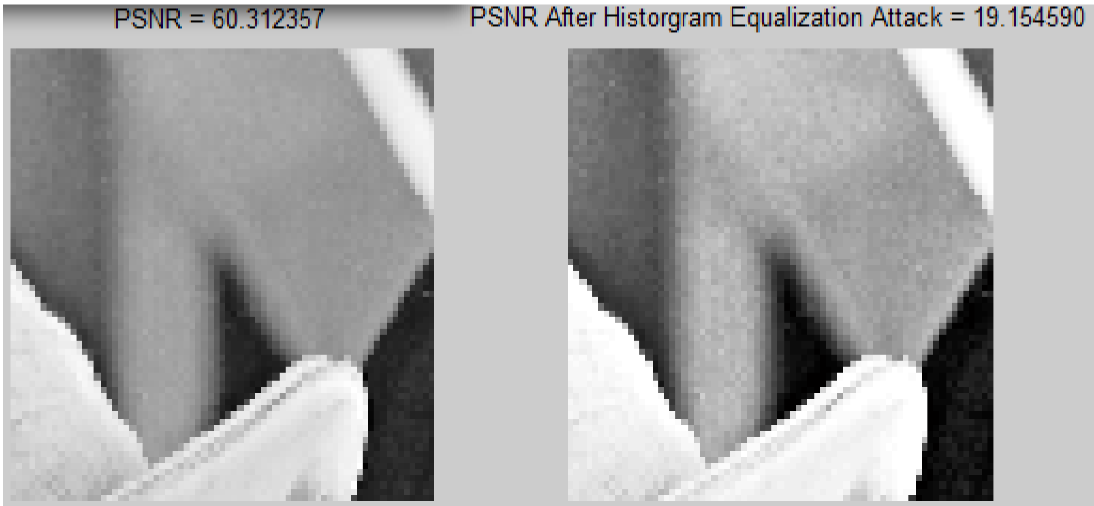


Figure 120. PSNR values of original and histogram equalization attacked image

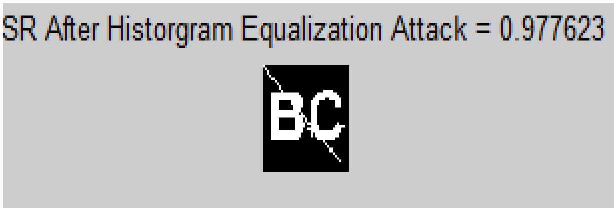


Figure 121. SR value of watermarked image after histogram equalization attack

For Gamma Correction Attack, Figure 122 shows PSNR values of original and attacked image and Figure 123 shows SR value of attacked image.

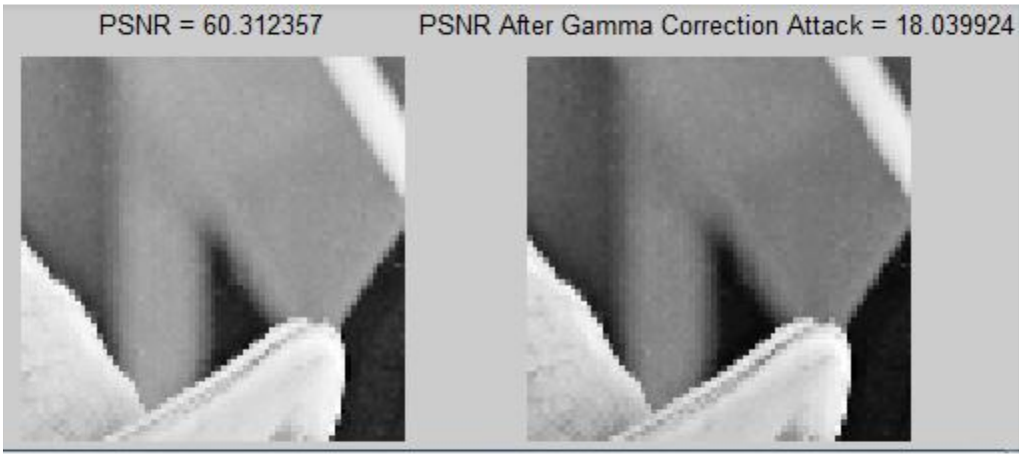


Figure 122. PSNR values of original and gamma correction attacked image

Figure 123. SR value of watermarked image after gamma correction attack

For JPEG Compression Attack, Figure 124 shows PSNR values of original and attacked image and Figure 125 shows SR value of attacked image.

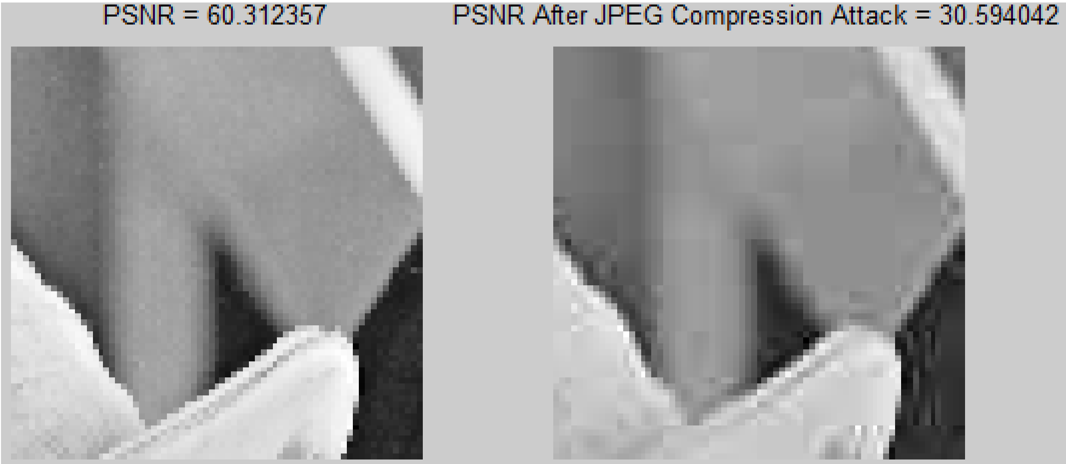


Figure 124. PSNR values of original and JPEG compression attacked image

Figure 125. SR value of watermarked image after JPEG compression attack

For Rotation Attack, Figure 126 shows PSNR values of original and attacked image and Figure 127 shows SR value of attacked image.

Figure 126. PSNR values of original and rotation attacked image

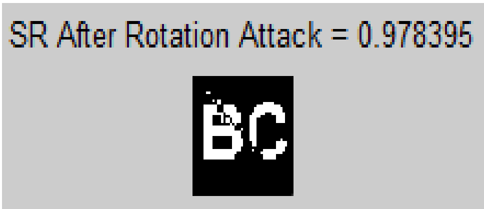


Figure 127. SR value of watermarked image after rotation attack

For Intensity Adjustment Attack, Figure 128 shows PSNR values of original and attacked image and Figure 129 shows SR value of attacked image.

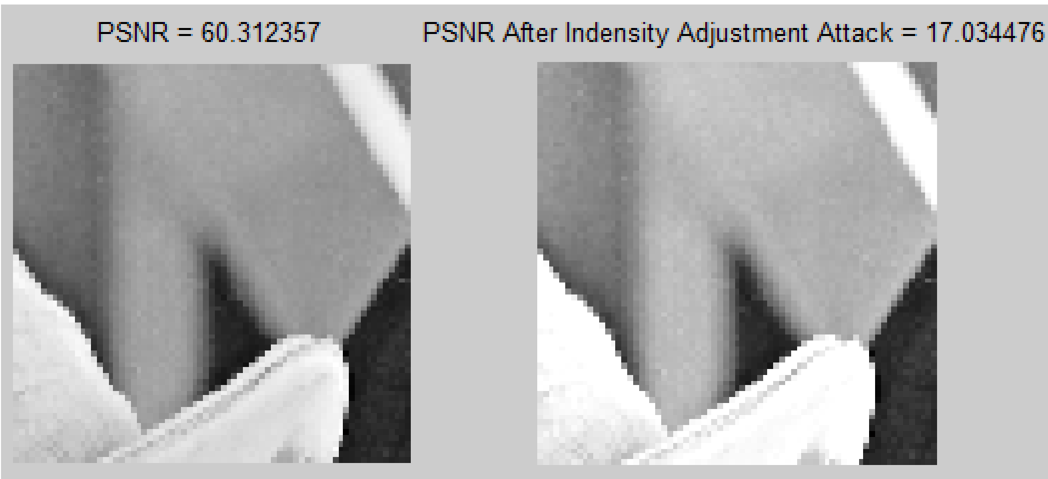


Figure 128. PSNR values of original and intensity adjustment attacked image

Figure 129. SR value of watermarked image after intensity adjustment attack

For Noise Pepper & Salt Attack, Figure 130 shows PSNR values of original and attacked image and Figure 131 shows SR value of attacked image.

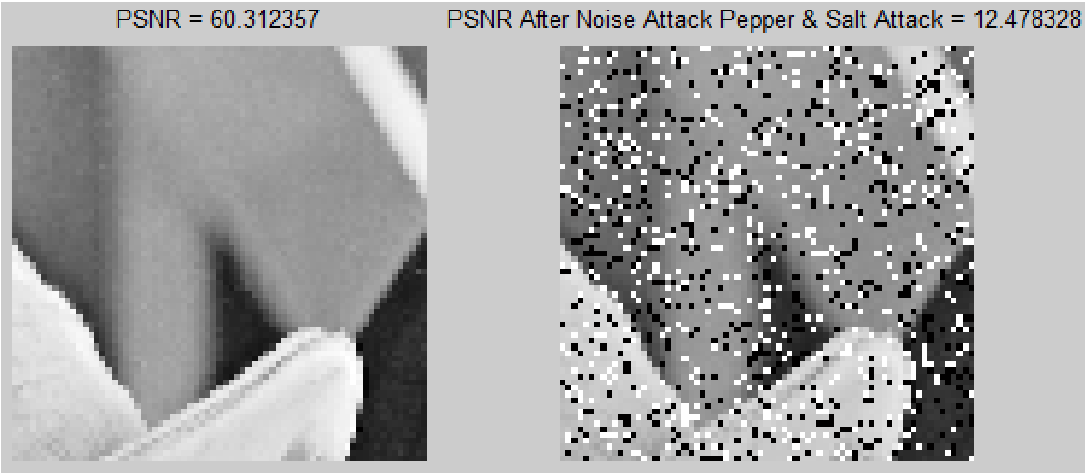


Figure 130. PSNR values of original and pepper & salt noise attacked image

Figure 131. SR value of watermarked image after pepper & salt noise attack

For Speckle Noise Attack, Figure 132 shows PSNR values of original and attacked image and Figure 133 shows SR value of attacked image.

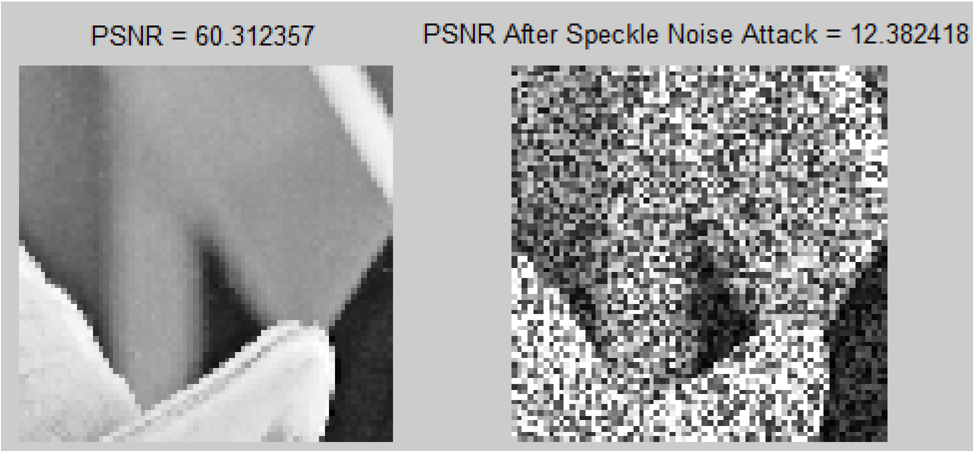


Figure 132. PSNR values of original and speckle noise attacked image

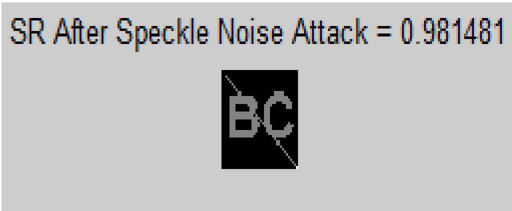


Figure 133. SR value of watermarked image after speckle noise attack

Table 5. PSNR, PSNR_After and SR Values of Second Corner Point of Lena

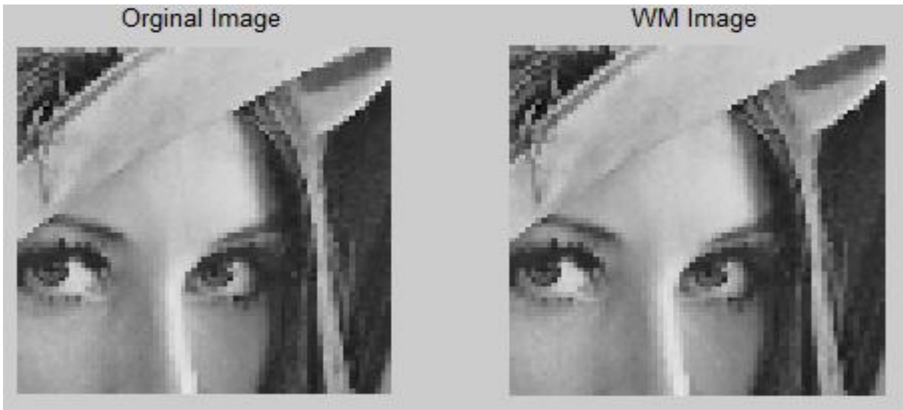
Attacks	PSNR	PSNR_After	SR
Filter Attack	60.312357	28.967836	0.962963
Scaling Attack	60.312357	27.108097	0.916667
Gaussian Attack	60.312357	29.977469	0.983025
Histogram Equalization Attack	60.312357	19.154590	0.977623
Gamma Correction Attack	60.312357	18.039924	0.986883
Jpeg Correction Attack	60.312357	30.594042	0.989198
Rotation Attack	60.312357	10.592376	0.978395
Intensity Adjustment Attack	60.312357	17.034476	0.980710
Noise Attack	60.312357	12.478328	0.982253
Speckle Noise Attack	60.312357	12.382418	0.981481

In Table 5 the PSNR and SR values are calculated for image and respectively presented. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images; original and watermarked image. The higher the PSNR shows the better the quality of the compressed or reconstructed image. For two images that are perfect copies of each other PSNR value is infinity. Since PSNR is in logarithmic scale slight improvements are sufficient. For instance, PSNR before noise attack is 60.312357; this value is watermarked image's PSNR value. But its PSNR value changed after noise attack. It could be 12.478328. This difference between PSNR values, show us, this image not an original watermarked image. So, original watermarked images had some change. The SR between two images is used as quality measurement; it is calculated similarity between watermark images after and before attack. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR for original watermark image is 1. Recovered watermarks quality under the above attacks is assessed based on subjective evaluation of SR. In all attacked cases the SR value is more than 0.9. If the original watermarked image, PSNR and SR values are same or similar before attack and after attack.

To compare PSNR and SR values, also studied with non-corner point. 166 different points that were not equal to corners selected randomly. One of the non-corner point examples is shown Figure 134.

Figure 134. Non corner point example of Lena image

Image that watermark applied and original image shown in Figure 135. Used invisible watermarking that watermark is not visible as shown.



a. b.

Figure 135. a. Original image, b. Watermarked image

Using DWT, decompose the original image into four bands that are LL, LH, HL, and HH. Figure 136 shows that one level of DWT on example corner. Apply SVD to sub-band LL. Apply SVD to watermark image.

Figure 136. One level DWT for cropped image

For Filter Attack, Figure 137 shows PSNR values of original and attacked image and Figure 138 shows SR value of attacked image.

Figure 137. PSNR values of original and filter attacked image

Figure 138. SR value of watermarked image after filter attack

For Scaling Attack, Figure 139 shows PSNR values of original and attacked image and Figure 140 shows SR value of attacked image.

Figure 139. PSNR values of original and scaling attacked image

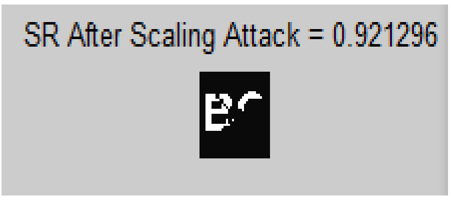


Figure 140. SR value of watermarked image after scaling attack

For Gaussian Attack, Figure 141 shows PSNR values of original and attacked image and Figure 142 shows SR value of attacked image.

Figure 141. PSNR values of original and Gaussian attacked image

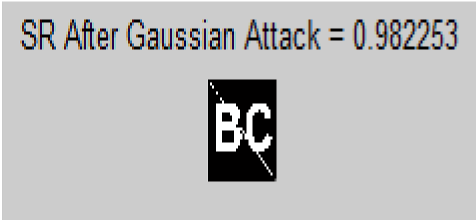


Figure 142. SR value of watermarked image after Gaussian attack

For Histogram Equalization Attack, Figure 143 shows PSNR values of original and attacked image and Figure 144 shows SR value of attacked image.

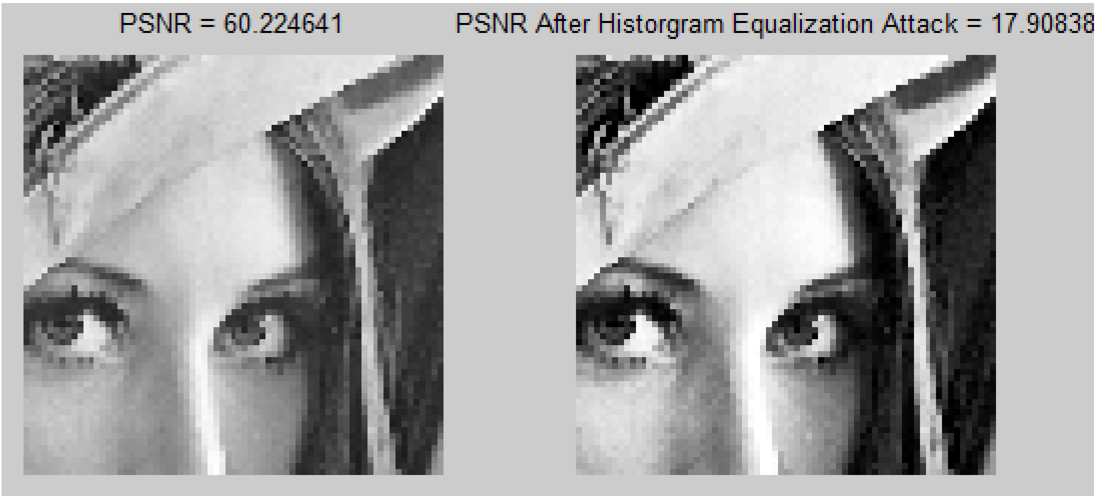


Figure 143. PSNR values of original and histogram equalization attacked image

Figure 144. SR value of watermarked image after histogram equalization attack

For Gamma Correction Attack, Figure 145 shows PSNR values of original and attacked image and Figure 146 shows SR value of attacked image.

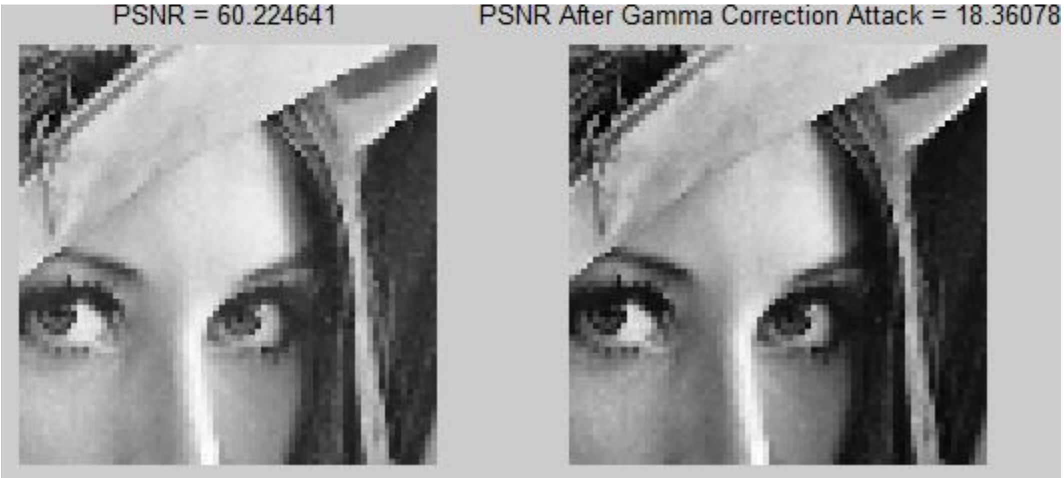


Figure 145. PSNR values of original and gamma correction attacked image

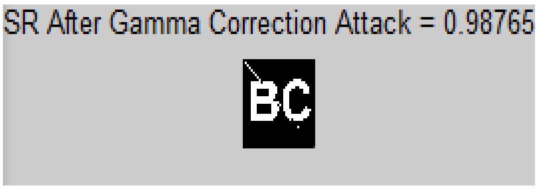


Figure 146. SR value of watermarked image after gamma correction attack

For JPEG Compression Attack, Figure 147 shows PSNR values of original and attacked image and Figure 148 shows SR value of attacked image.

Figure 147. PSNR values of original and JPEG compression attacked image

Figure 148. SR value of watermarked image after JPEG compression attack

For Rotation Attack, Figure 149 shows PSNR values of original and attacked image and Figure 150 shows SR value of attacked image.

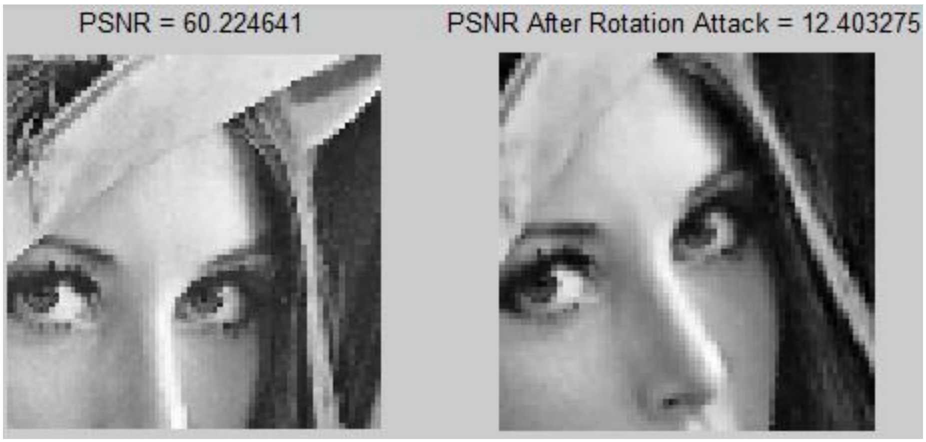


Figure 149. PSNR values of original and rotation attacked image

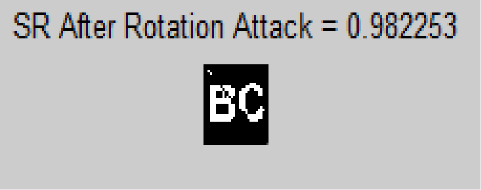


Figure 150. SR value of watermarked image after rotation attack

For Intensity Adjustment Attack, Figure 151 shows PSNR values of original and attacked image and Figure 152 shows SR value of attacked image.

Figure 151. PSNR values of original and intensity adjustment attacked image

Figure 152. SR value of watermarked image after intensity adjustment attack

For Noise Pepper & Salt Attack, Figure 153 shows PSNR values of original and attacked image and Figure 154 shows SR value of attacked image.

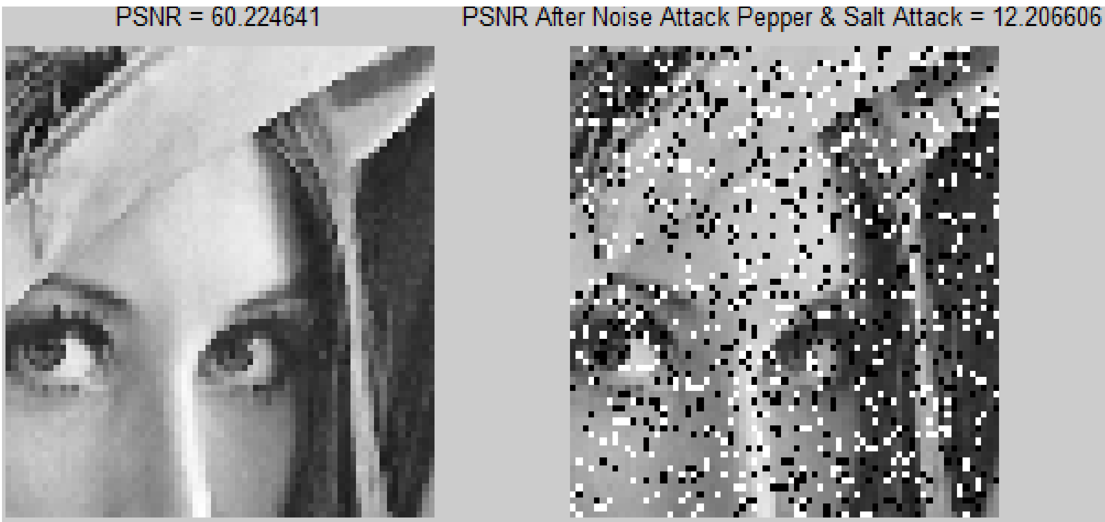


Figure 153. PSNR values of original and pepper & salt noise attacked image

Figure 154. SR value of watermarked image after pepper & salt noise attack

For Speckle Noise Attack, Figure 155 shows PSNR values of original and attacked image and Figure 156 shows SR value of attacked image.

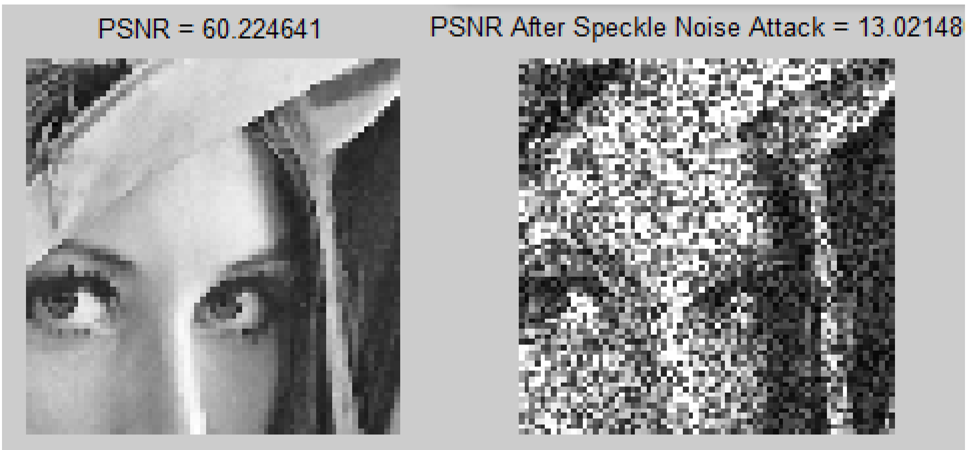


Figure 155. PSNR values of original and speckle noise attacked image

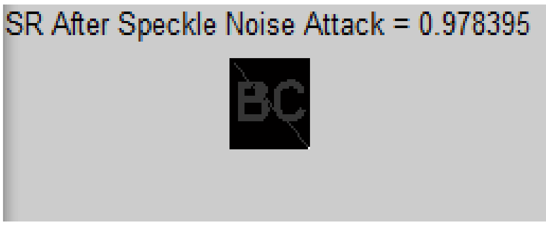


Figure 156. SR value of watermarked image after speckle noise attack

Table 6. PSNR, PSNR_After and SR Values of Non Corner Point of Lena

Attacks	PSNR	PSNR_After	SR
Filter Attack	60.224641	25.239493	0.955247
Scaling Attack	60.224641	23.874577	0.921296
Gaussian Attack	60.224641	29.901480	0.982253
Histogram Equalization Attack	60.224641	17.908380	0.982253
Gamma Correction Attack	60.224641	18.360780	0.987650
Jpeg Correction Attack	60.224641	26.993723	0.989198
Rotation Attack	60.224641	12.403275	0.982253
Intensity Adjustment Attack	60.224641	17.233285	0.982253
Noise Attack	60.224641	12.206606	0.979938
Speckle Noise Attack	60.224641	13.021480	0.978395

In Table 6 the PSNR and SR values are calculated for image and respectively presented. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images; original and watermarked image. The higher the PSNR shows the better the quality of the compressed or reconstructed image. For two images that are perfect copies of each other PSNR value is infinity. Since PSNR is in logarithmic scale slight improvements are sufficient. For instance, PSNR before Gaussian attack is 60.224641; this value is watermarked image's PSNR value. But its PSNR value changed after Gaussian attack. It could be 29.901480. This difference between PSNR values, show us, this image not an original watermarked image. So, original watermarked images had some change. The SR between two images is used as quality measurement; it is calculated similarity between watermark images after and before attack. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. SR for original watermark image is 1. Recovered watermarks quality under the above attacks is assessed based on subjective evaluation of SR. In all attacked cases the SR value is more than 0.9. If the original watermarked image, PSNR and SR values are same or similar before attack and after attack.

CONCLUSION

In the study, digital image watermarking with finding corner point based on DWT method is proposed. Digital watermarking is an information hiding technique which is used to hide a mark such as image to protected information. There are three approaches to embed a watermark: spatial domain, transform domain and compressed domain watermarking. In this study, transform domain watermarking is used with DWT. Invisible watermarked is used. Harris corner detector is used to find feature points. By finding corners, square regions around feature points are computed. After computing square region, it is cropped and the watermark is embedded. Ten different attacks are applied to watermarked image and then watermarking is detected and extracted. This technique is applied to many corner points. Two different images are used Cameraman and Lena. When looking to variations of PSNR and SR values on different attacks on different square regions, it is seen that SR and PSNR values are changing. Mostly, the SR value is more than 0.9 in all attack cases.

The objective of this study is embedding small watermark images to original image and showing the results.

In the thesis, experiments show the proposed watermarking algorithm has robustness for attacks while still keeping the quality of the image.

As an extension of the thesis, second level of DWT will be applied on same images and compare results of one level and second level.

REFERENCES

[1] **F. AKAR, Y. YALMAN, H.S. VAROL**, "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, 2012.

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

[3] **K. MIKOLAJCZYK AND C. SCHMID,** "Scale and affine invariant interest point detector", Int. J. Comput. Vis., vol. 60, no. 1, pp.63-86, Oct. 2004.

[4] **O.JANE, E. ELBAŞI,** "A new approach in non-blind watermarking method based on DWT and SVD via LU decomposition", Turkish Journal of Electrical Engineering and Computer Sciences, 2013

[5] **Y. FANG AND L.TIAN**, "An Improved Blind Watermarking Algorithm for Image Based On Dwt Domain", Journal of Theoretical and Applied Information Technology, Vol. 45 No.1, pp 168-173, Nov. 2012.

[6] **X. QI AND J. QI,** "A robust content-based digital image watermarking scheme", Signal Processing 87 (2007) 1264–1280.

[7] **W. LU, W. SUN AND H. LU**, "Novel robust image watermarking based on subsampling and DWT", Multimed Tools Appl (2012) 60:31–46

[8] **Y. LIU AND J. ZHAO**, "A Robust image watermarking based on Adaptive Feature Points Detection", International Conference on Communications, Circuits and Systems Proceedings, 2006

[9] **A.R. MADANE AND M.M. SHAH**, "Watermark Image Recognition Using Principle Component Analysis", First International Conference on Emerging Trends in Engineering and Technology, 2008

[10] **Y. ZHANG AND N. CHANG,** "DWT-Based feature Locating Digital Watermark Technique", International Conference on Computational Intelligence and Software Engineering, 2009

[11] **J. YANG, D. YANG, X. ZHOU AND Y. GE**, "A robust content-based digital image watermarking technique", Chinese Conference on CCPR, 2010.

[12] **Z. YONGPING,** "Digital Watermarking Technique for Images Based on DWT", Conference on Multimedia Computing and Systems - ICMCS, pp. 1-6, 2011

[13] **J. ZHANG, M. SUN, M. GE, Z. YANG, J. XUE, L. WANG** "Robust Watermarking Of Digital Image Based On Feature And Dwt", Proceedings of the 2012 International Conference on Machine Learning and Cybernetics, July, 2012

[14] **S. MIAO, J. LI, Y. BAI AND Y. CHEN**, "Robust Watermarking for Medical Images Based on Arnold Scrambling and DWT-DFT", Computing and Convergence Technology (ICCCT) 7th International Conference, 2012

[15] **A. AL-HAJ**, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science 3 (9): 740-746, 2007

[16] **R. G. SHARMA AND V. SAXENA**, "DWT-Based Watermarking for JPEG2000 Images", The Icfai University Journal of Information Technology, Vol. V, No. 2, 2009

[17] **A.A.ABDULFETAH, X. SUN, H. YANG AND N. MOHAMMED**, " Robust Adaptive Image Watermarking using Visual Models in DWT and DCT Domain", Information Tech. Journal 9(3): 460-466, 2010

[18] **S. TRIPATHI, N. RAMESH, B. A, AND N.K. J**, "A DWT based dual image watermarking technique for authenticity and watermark protection", Signal and Image Processing: An International Journal, Vol 1 No.2, Dec. 2010

[19] **M. MASOUMI AND S. AMIRI**, "Copyright Protection of Color Video Using Digital Watermarking ",IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012

[20] **L. ZHANG, X. YAN, H. LI AND M. CHEN**, "A Dynamic Multiple Watermarking Algorithm Based on DWT and HVS ",Int. J. Communications, Network and System Sciences, 2012, 5, 490-495

[21] **C. YONGQIANG, Z. YANQING AND P. LIHUA**, "A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network", Proceedings of the 2009 International Symposium on Information Processing, August 21-23, 2009, pp. 298-301

[22] **Z. C. NA, Z.Y. YONG, M. CHI AND L. Y. RAN**, " A Self-Adaptive Digital Watermarking Algorithm Based On Wavelet Transform", Journal of Theoretical applied Information Technology, Vol. 49 No.2, March 2013

[23] **V.M. VISWANATHAM, G.S. REDDY AND P.JAGADEESH**, "A Hybrid Digital Watermarking Algorithm for Color Images Based on DWT and DCT", Anale Seria Informatică. Vol. 10 No. 2, 2012

[24] **M. MAES, T. KALKER, J. LINNARTZ, J. TALSTRA, G. DEPOVERE, J. HAITSMA**, "Digital Watermarking for DVD Video Copy Protection: What Issues Play a Role in Designing an Effective System?", IEEE Signal Processing Magazine, September 2000.

[25] **M. D. SWANSON, B. ZHU, A. H. TEWFIK**, "Multiresolution Scene-Based Video Watermarking Using Perceptual Models," IEEE Journal on Selected Areas in Communications, Vol. 16, No.4, May 1998.

[26] **S. P. MOHANTY, N. RANGANATHAN, AND R. K. NAMBALLA**, "VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder," Proceedings of the IEEE Workshop on Signal Processing System (SIPS), pp. 183-188, 2003.

[27] **H. WANG, Z. LU, J. PAN, S. SUN,** "Robust Blind Video Watermarking with Adaptive Embedding Mechanism", International Journal of Innovative Computing, Information and Control Volume 1, Number 2, June 2005.

APPENDIX A

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Ölçer, Naim

Nationality: Turkish (TC)

Date and Place of Birth: 01 January 1984, Hatay

Marital Status: Married

E-mail: naimolcer@gmail.com

EDUCATION

Çankaya University, Department of Computer Engineering, 2009

WORK EXPERIENCE

2013 - Present	EnerjiSA	Information System Specialist
2011 - 2013	Innova Bilişim	Senior Software Developer
2011 - 2011	Halıcı Yazılım Evi	Senior Software Developer
2009 - 2011	LST Yazılım	Senior Software Developer

PUBLICATIONS

N.Olcer, E.Elbasi,"Petrol flow pattern identification via data mining techniques" Energy Education Science and Technology Part A