Robust Color Image Watermarking Techniques Based on DWT, DCT and SVD in Different Color Spaces

Asma Abdallah Alkraik

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Science
in
Electrical and Electronic Engineering

Eastern Mediterranean University
February 2016
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Cem Tanova
Acting Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Master of Science in Electrical and Electronic Engineering.

Prof. Dr. Hasan Demirel
Chair, Department of Electrical and
Electronic Engineering

We 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 in Electrical and Electronic Engineering.

Prof. Dr. Hasan Demirel
Supervisor

Examining Committee

1. Prof. Dr. Hasan Demirel
2. Assoc. Prof. Dr. Erhan A. İnce
3. Asst. Prof. Dr. Rasime Uyguroğlu

ABSTRACT

Within the last decade, with the development of communication technologies and the increasing growth in the internet has become insecure, so it created different techniques to solve this problem. One of these techniques is the digital watermark, which provides the protection of property rights.

In this thesis, we suggest new techniques of watermarking image aim to increase the degree of robustness of the watermark against various attacks and to increase the imperceptibility of the watermark image. Also these techniques aim to ensure the watermark image using Arnold transform where the watermark is available only to a legitimate user.

The proposed approaches of watermarking image based on DWT, DCT and SVD have been applied on gray and color images in different color spaces like RGB, YIQ and YCbCr. Therefore, we have seven proposed algorithms namely: a gray image watermarking technique, an image watermarking technique in RGB color space (using a gray watermark image), an image watermarking technique in RGB color space (using a color watermark image), an image watermarking technique in YIG color space (using a gray watermark image), an image watermarking technique in YIQ color space (using a color watermark image), an image watermarking technique in YCbCr color space (using a gray watermark image) and an image watermarking technique in YCbCr color space (using a color watermark image). The difference between these algorithms is the type of watermark and the colorspace used (gray or color image: RGB, YIQ or YCbCr). To test the performance of proposed approaches, we calculated the PSNR and the SSIM.

The best proposed approach which gives high robustness and imperceptibility of the watermark image against different attacks is an image watermarking technique in YIQ colour space (using a gray watermark image). And, the worst proposed approach which gives low robustness and low imperceptibility of the watermark image against different attacks is an image watermarking technique in YCbCr color space (using a color watermark image). In addition, our proposed approaches give high imperceptibility and high robustness of the watermark image when compared with other techniques [17][22][23].

Through the results, it has been verified superiority of our proposed approaches on many techniques. Our proposed approaches have high robustness of the watermark against various attacks with high quality for the watermarked image and security of the watermark image.

Keywords: Watermarking Image, robustness, imperceptibility, PSNR, SSIM.

ÖZ

Son on yıl içinde, iletişim teknolojilerinin gelişmesi ve artan büyüme ile İnternet güvensiz hale gelmiştir, dolayısıyla bu sorunu çözmek için farklı teknikler geliştirilmiştir. Bu tekniklerden biri de sayısal filigran tekniğidir. Sayısal filigran temelde mülkiyet haklarının korunmasını sağlamaktadır.

Bu tezde, yeni teknikler kullanarak farklı saldırılara karşı filigran sağlamlığını artırmak ve filigran görüntüsünün fark edilemezliğini artırmayı hedeflemekteyiz. Arnold dönüşümü kullanan bu teknikler ile filigran görüntüsüsün sadece meşru bir kullanıcı tarafından kullanılabilir olması sağlanmaktadır.

DWT , DCT ve SVD dayalı damgalama önerileri RGB , YIQ ve YCbCr gibi farklı renk uzaylarında gri ve renkli filigranlar kullanılarak uygulanmıştır. Bu çerçevede yedi farklı algoritma önerilmiştir. Bunlar, sırasıyla: gri görüntü filigran tekniği, RGB renk uzayında bir filigran görüntü tekniği (gri filigran kullanılarak), RGB renk uzayında bir filigran görüntü tekniği (renkli filigran kullanılarak), YIG renk uzayında bir filigran görüntü tekniği (gri filigran kullanılarak), YIQ renk uzayında bir görüntü filigran tekniği (renkli filigran kullanılarak), YCbCr renk uzayında bir görüntü filigran tekniği (gri filigran kullanılarak) ve YCbCr renk uzayında bir görüntü filigran tekniği (renkli filigran kullanılarak). Bu algoritmalar arasındaki farkları renk uzaylarındaki (RGB , YIQ ya da YCbCr) farklarla filigran türü arasındaki farklar (gri ya da renkli) oluşturmaktadır. Önerilen yaklaşımların performansını test etmek için PSNR ve SSIM metrikleri kullanılmaktadır.

Önerilen yaklaşımlar arasında en yüksek sağlamlık ve farklı saldırılara karşı en kaliteli filigran fark edilemezliği sağlayan yaklaşım (gri filigran görüntü kullanılarak) YIQ renk uzayında elde edilmişti. Öte yandan, önerilen yaklaşımlar arasında en düşük sağlamlık ve farklı saldırılara karşı en düşük kalitede filigran fark edilemezliği sağlayan yaklaşım (renkli filigran kullanılarak) YCbCr renk uzayında elde edilmişti. Literatürdeki alternatif tekniklerle ([17] [22] [23]) karşılaştırıldığında, önerilen yaklaşımlar yüksek fark edilemezlik ve yüksek filigran sağlamlığı ortaya çıkarmaktadır.

Elde edilen sonuçlar, önerilen yaklaşımların literatürdeki yaklaşımlara göre olan üstünlüğü doğrulanmıştır. Önerilen yaklaşımlar filigranlı görüntünün yüksek kalitede olmasını ve faklı saldırılara karşı filigran sağlamlığının güvenlik açısından üst seviyede olduğunu göstermektedir.

Anahtar Kelimeler: Filigramlı görüntü, filigram sağlamlığı, fark edilemezlik, PSNR, SSIM.

DEDICATION

This thesis is dedicated to my lovely parents for their love. Further, I would like to dedicate this work to my husband and my sisters and my brothers for their encouragement and endless support and to my beloved children.

ACKNOWLEDGMENT

I would like to thank my supervisor and chairman Prof. Dr. Hasan Demirel for his endless support and guidance in the preparation of this study. I would also like to thank him for being an open person to ideas and help me in all stages of my master study.

I owe quit a lot to my family specially my husband who allowed me to complete my studies and supported me in all of my study. I also would like to express my appreciation to my parents and my brothers and sisters who have supported me in all of my life. In addition, I would like to thank my friends who has supported and encouraged me.

Last but not least, I would like to say to my father "I miss you so much in these times and I love you too much".

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS/ABBREVIATIONS

Alpha	Embedding coefficient
CC	Correlation Coefficient
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transformation
HH	Diagonal Sub-band
HL	Horizontal sub-band
LH	Vertical sub-band
LL	Approximate sub band
MSE	The Mean Square Error
PSNR	Peak Signal to Noise Ratio
SSIM	Structural similarity Index Measurement
SVD	Singular Value Decomposition
2-D DCT	Two-Dimensional Discrete Cosine Transform

Chapter 1

INTRODUCTION

1.1 Introduction

In recent years with the fast growth of technology and the increasing use of the internet for data transfer shall provide for the protection of communication systems. Where, the controlling and protecting sensitive or confidential documents and images has become next to impossible. Therefore, the world today is based on the provision of many of the techniques of information security, such as encryption and digital watermarking. Digital watermarking is one of the most influential techniques to detect misappropriated data and ensure copyright protection for the digital content like texts, images, audios and videos from illegal manipulations [1][2].

Digital watermarking refers to the process of embedding or hiding the digital data directly onto the digital content (multimedia) and that it can be extracted again. And It has many proprieties such as cryptography, watermark is imperceptible and does not affect the aesthetic of the digital content and robustness of the watermark against different attacks such as the compression, rotation and scaling for digital image watermarking [1][2][3].

Therefore, the quality of the technique is determined using some properties like robustness, transparency and capacity. The watermarking technique is robust, if the watermark is not significantly affected when exposed to various attacks like the compression, scaling, rotation and noises then watermarking scheme is robust. The transparency or imperceptibility means after embedding the watermark, the original data should not be distorted. The capacity means the size of watermark which is inserted into original data. More capacity means it can hide large size of information.

In this thesis, we suggest novel technique using digital image watermarking based on three techniques that are DCT, DWT and SVD to hide the watermark image into original image for the grayscale and color image in different space (RGB, YIQ and YCbCr).

Where, the security technique has been used to ensure the watermark image, so the watermark is available only to a legitimate user, using encryption technique which called Arnold transformation.

1.2 Objectives

The main objective of this thesis is to get the best results for the quality of the digital image watermarking technology for color image in different color spaces, which is divided into:

- The high robustness of watermark techniques against the various attacks like the compression, noise, cropping, rotation and scaling.
- The high transparency or imperceptibility for watermark image after insertion the watermark image into original image.
- The security of the watermark image using encryption technique (Arnold transformation).

1.3 Contributions

In this thesis, the main contributions can be specified as follows:

- Promotion of protection of data, our thesis suggests new techniques for protecting digital images, solving the problems of forgery and illegal manipulation. Therefore, people can do business electronically.
- Proficient image archiving and retrieval, our thesis uses the encryption technique which is Arnold transform to ensure the watermark.
- High robustness and imperceptibility of the watermark scheme, our thesis gives high robustness against different attacks like compression, noises and scaling, in the same time it gives high imperceptibility thereby high quality image.

1.4 Thesis Overview

Chapter 1 is the introduction of thesis includes brief review of digital watermarking and explaining the advantages of digital watermarking and the main aims from this thesis. Chapter 2 deals with definition of digital watermarking, properties and applications of digital image watermarking. Chapter 3 is talking about the grayscale image and different color spaces like RGB, YIQ and YCbCr. Chapter 4 is explanation the three domains or techniques the DWT, DCT and SVD for watermarking. Chapter 5 shows the embedding and extraction algorithms based on DWT-DCT-SVD for grayscale image and color image (in different color spaces). Chapter 6 there are experimental results for our techniques. The comparisons between the different techniques have been shown in tables and graphs clearly. Finally, chapter 7 is the conclusion of our proposed approaches based on results of approaches and suggest more efficient and accurate method for future works.

Chapter 2

DIGITAL WATERMARKING

2.1 Introduction

The digital multimedia like the image, video and audio, can be protected against copyright infringements using some techniques such as steganography and digital watermarking techniques. Digital Watermarking is a technique to insertion of data into digital multimedia, without affecting quality of the original multimedia. Therefore, this technique has become useful tool for steganography, copyright protection and content authentication [4].

Where, the digital watermarking technology plays an important role in preventing copyright violation as it allows to place an imperceptible or invisible watermark depending on the requirement in the multimedia data to detect malicious tampering of the multimedia or data identify the legitimate owner [2][4].

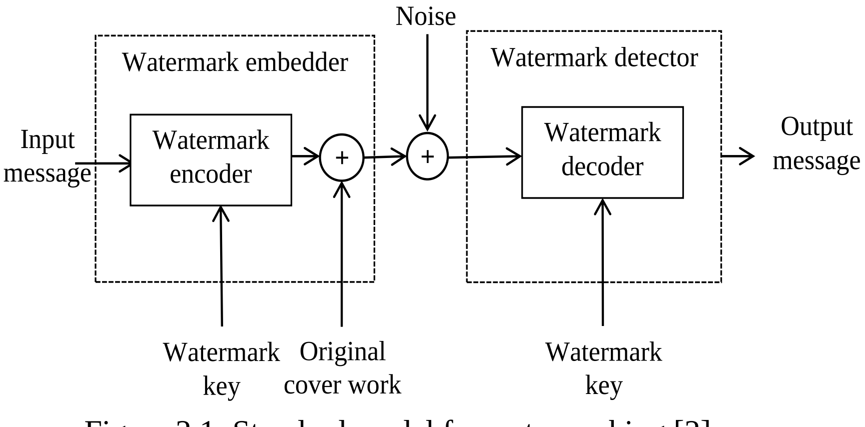


Figure 2.1: Standard model for watermarking [2]

As shown by Figure 2.1, in the watermark embedder, a watermark encoder encodes an input message using a watermark key. The encoded message or watermark will be embedded into the original cover work. In the watermark detector, a watermark decoder receives the noisy watermarked cover and decodes it using the same key to get the output message (extracted message).

2.2 Digital Image Watermarking

The scheme of digital image watermarking divides into two stages: the embedding process and the detection process as shown in following figures:

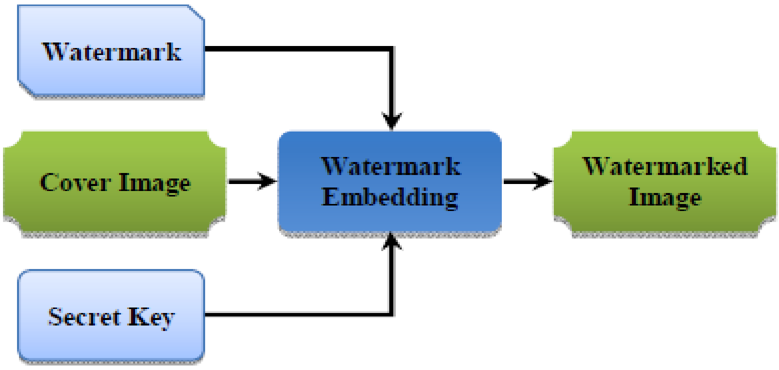


Figure 2.2: The embedding process [5]

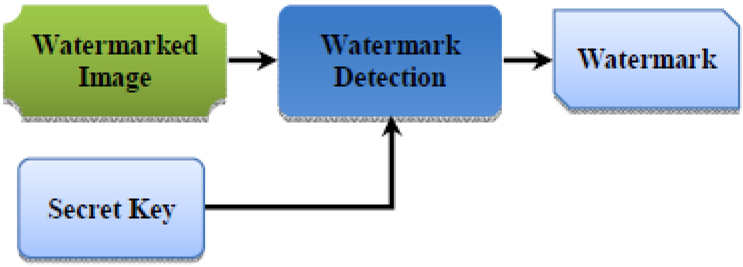


Figure 2.3: The detection process [5]

The embedding process is used for embedding the watermark image into the cover image with the secret key to secure the watermark image. The output of this process is the watermarked image. And, the detection process is used to recover the watermark by using the same secret key [5].

2.3 Proprieties of Digital Watermarking

Digital watermarking can be characterized on the basis of several properties which depend on the type of application. These properties include resistance of the watermarking scheme to malicious attacks, the capacity of bit information and the complexity of the watermarking scheme. In general, they are described as the robustness, capacity, imperceptibility, security and other restrictions [5]. The main properties of digital watermarking as following:

2.3.1 The robustness

The robustness is resilience of the watermark to the various attacks like the compression, scaling, rotation and printing. The robustness of the watermark scheme can be divided as following:

a) Robust:

The robust watermark schemes are ability to intentional or un-intentional attacks or signal processing operations. This type of watermarking scheme uses in copyright protection, copy control, fingerprinting, and broadcast monitoring.

b) Fragile:

In this type unlike robust watermark schemes, the watermark scheme can be distorted at any type of modification. In addition, this type of watermark scheme can be used in content authentication and integrity verification [2][4][5].

c) Semi-fragile:

This type of watermark scheme is fragile against malicious attacks, but robust against incidental modifications. In addition, it is used for image authentication [5].

2.3.2 Imperceptibility

Imperceptibility watermark scheme (also known as invisibility) is a measure of the similarity between the original image before watermarking process and the watermarked image. And the watermark should be invisible. However, the challenge is that imperceptibility could be achieved, but the robustness and the capacity will be reduced, and vice versa. In some applications, the watermark is preferred to be a visual watermark. Therefore, it is not always invisible [2][4][5].

2.3.3 Capacity (Payload)

The capacity watermark scheme is the size of data which will be embedded into the original image. In addition, the capacity can be different depending on the application that is designed for it. Where, in some applications need to one bit and another applications need to big capacity [4][5].

2.3.4 Security

Security watermark scheme is the ability to resist against hostile attacks. These kind of attacks aims to change the objective of embedding process. The kinds of attacks are classified as following:

a) Unauthorized embedding.

b) Unauthorized detection.

c) Unauthorized removal.

Depending on the use of watermark scheme, the certain feature should be available in the scheme to resist various attacks. So, the watermark must be fragile or semi fragile to detection any change for unauthorized embedding. And, it must be imperceptible watermark for unauthorized detection. Also, the watermark must be robust against the attacks for unauthorized removal [4][5].

2.4 Application of Digital Watermarking

Digital watermarking is used for the protection of ownership rights of digital media, like images, video, audio, and other multimedia objects. It can be applied to various applications such as content authentication, copyright protection, copy control, owner identification and secret communication [4]. The main applications of digital watermarking as following:

a) Copyright Protection

For intellectual property protection and copyright, the copyright data can be added into the new production as a watermark. Where, the watermark can be extracted to give the information about owner of this product. Copyright applications should be imperceptible, require a high degree of robustness and but may have low capacity [5].

b) Content Authentication

The objective of authentication applications is for detecting any modifications of the data. In other words, the digital watermark contains data which can be used for proving that the digital content has not been changed. This can be achieved with fragile watermarks which have a low robustness to certain attacks such as compression, but are destroyed by other attacks [2][4][5].

c) Owner Identification

The owner identification data can be embedded into image as a watermark that is a visual or visible watermark (traditional form). However, this can be overcome using some programs which modify the images. In order to overcome the problem, invisible watermarks are used [2][4][5].

Chapter 3

GRAY-SCALE AND COLOR IMAGE SPACES

3.1 Gray-scale Image

The gray-scale (sometimes also called the white space) is a range of monochromatic shades from pure white to pure black without apparent color. The intermediate shades of the gray are represented by equal brightness levels of the three primary colors red, green and blue, or equal amounts of the three primary pigments cyan, magenta and yellow. The gray space has a single dimension or component.

3.2 Color Image Spaces

The colors are created by the primary colors of pigment and these colors define a specific color space (also called as color models or color system). In other words, the color space is an abstract mathematical space that describes the range of colors as tuples of numbers such as RGB space which contains three color components. Each color in the system is represented by a single dot. There are a different of color spaces such as RGB, YIQ, CMY and YCbCr.

3.2.1 RGB Color Space

RGB color space uses the three primary red, green and blue additive colors, all possible colors can be made from mixing primary colors. RGB builds its space on different colors of light added together, where the mixture of all three colors produces white light as shown in Figure 3.1. RGB color uses in digital cameras and monitors display [6].

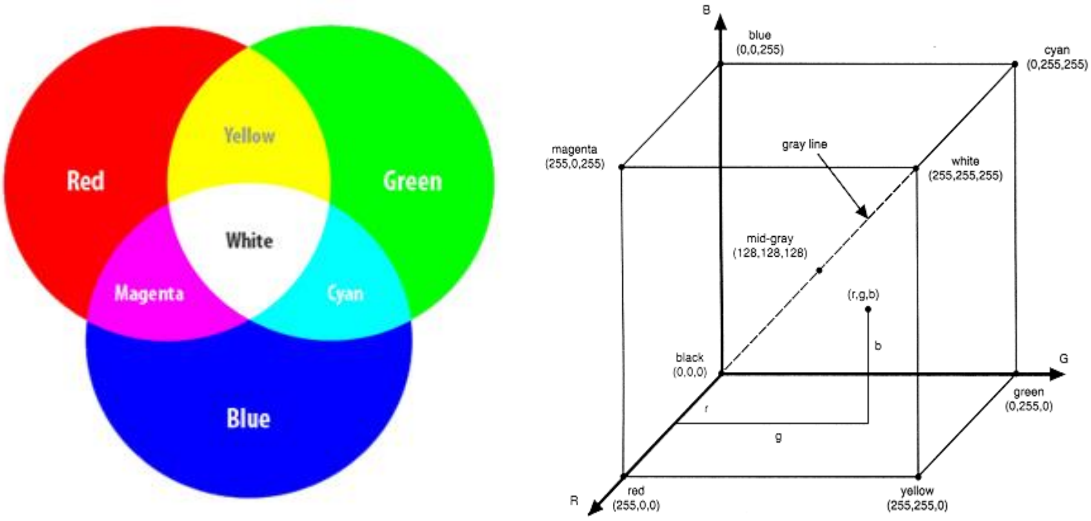


Figure 3.1: RGB color Space [7]

The conversion from RGB to Grayscale is given by formula:

$$\mathrm{Gray}_{\mathrm{scale}} = 0.2989 * \mathrm{R} + 0.587 * \mathrm{G} + 0.114 * \mathrm{B} \qquad (3.1)$$

3.2.1 YIQ Color Space

The YIQ color space is designed to separate chrominance from luminance. The Y-channel contains luminance information (or the brightness) while I and Q channels carried the color information. This space is used in a color television set then is converted into RGB space for display on a screen [8]. The conversion from RGB to YIQ is given by formula:

$$\begin{bmatrix} \mathrm{Y} \\ \mathrm{I} \\ \mathrm{Q} \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} \mathrm{R} \\ \mathrm{G} \\ \mathrm{B} \end{bmatrix} \qquad (3.2)$$

Also, the conversion from YIQ to RGB is given by formula:

$$\begin{bmatrix} \mathrm{R} \\ \mathrm{G} \\ \mathrm{B} \end{bmatrix} = \begin{bmatrix} 1 & 0.956 & 0.621 \\ 1 & -0.272 & -0.647 \\ 1 & -1.106 & 1.703 \end{bmatrix} \begin{bmatrix} \mathrm{Y} \\ \mathrm{I} \\ \mathrm{Q} \end{bmatrix} \qquad (3.3)$$

3.2.2 YCbCr Color Space

YCbCr color space is used in digital photography and video systems. Where, Y is the luminance (or light intensity) component and Cb and Cr are the blue-difference and red-difference chroma components.

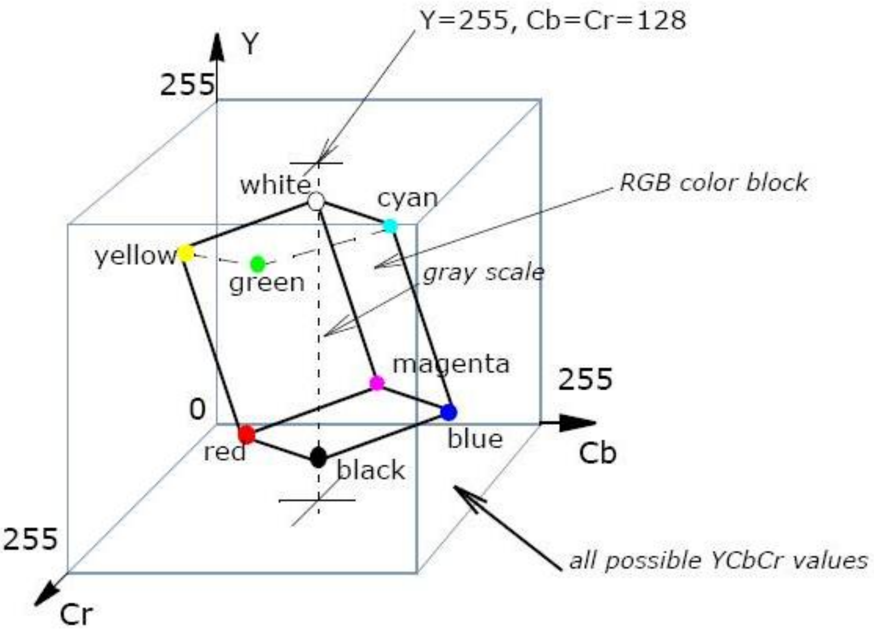


Figure 3.2: YCbCy Color Space [9]

The difference between RGB and YCbCr is that RGB represents the color as red, green and blue, while YCbCr represents the color as brightness and two color difference signals. where, the Y is the brightness or luma component, Cb is the difference between blue and luma component and Cr is the difference between red and luma component [9]. The conversion from RGB to YCbCr is given by formula:

$$\begin{bmatrix} \mathrm{Y} \\ \mathrm{Cb} \\ \mathrm{Cr} \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 65.481 & 128.553 & 24.966 \\ -37.797 & -74.203 & 112 \\ 112 & -93.786 & -18.214 \end{bmatrix} \begin{bmatrix} \mathrm{R} \\ \mathrm{G} \\ \mathrm{B} \end{bmatrix} \tag{3.4}$$

Also, the conversion from YCbCr to RGB is given by formula:

$$\begin{bmatrix} \mathrm{R} \\ \mathrm{G} \\ \mathrm{B} \end{bmatrix} = \begin{bmatrix} 0.00456621 & 0 & 0.00625893 \\ 0.00456621 & -0.00153632 & -0.00318811 \\ 0.00456621 & 0.00791071 & 0 \end{bmatrix} \begin{bmatrix} \mathrm{Y}-16 \\ \mathrm{Cb}-128 \\ \mathrm{Cr}-128 \end{bmatrix} \tag{3.5}$$

Chapter 4

DWT, DCT AND SVD FOR WATERMARKING

4.1 Introduction

In general, there are many domains to encode the watermark image. The most approach of watermarking is in spatial domain where the pixels are modified directly to encode the watermark. Another domain is in frequency where the image is converted into frequency domain and encode the watermark in low, median or high frequency. The frequency domain such as DCT and DFT. Other domains include the DWT, SVD and Hadamard domain.

For our proposed image watermarking scheme concepts of DWT, DCT, SVD and Arnold Transform are used. These tools are discussed in this chapter one by one.

4.2 Discrete Wavelet Transformation (DWT)

DWT is used to decompose the input image into sub bands of different resolutions that are low, middle and high frequency bands. The mean value of the filter is the low frequency coefficient while wavelet coefficients are the high frequency coefficients [10].

In one level DWT, an image is decomposed into four sub-bands which are approximate sub-band (LL1), horizontal sub-band (HL1), vertical sub-band (LH1), and diagonal Sub-band (HH1) [11][12]. One level DWT of an image as shown in following figure:

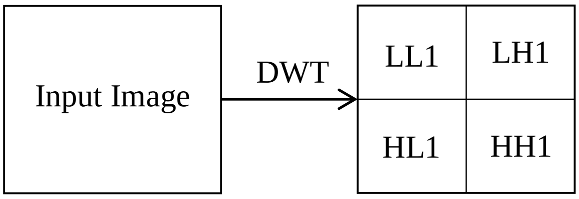


Figure 4.1: Decomposition structure "one level DWT" [15]

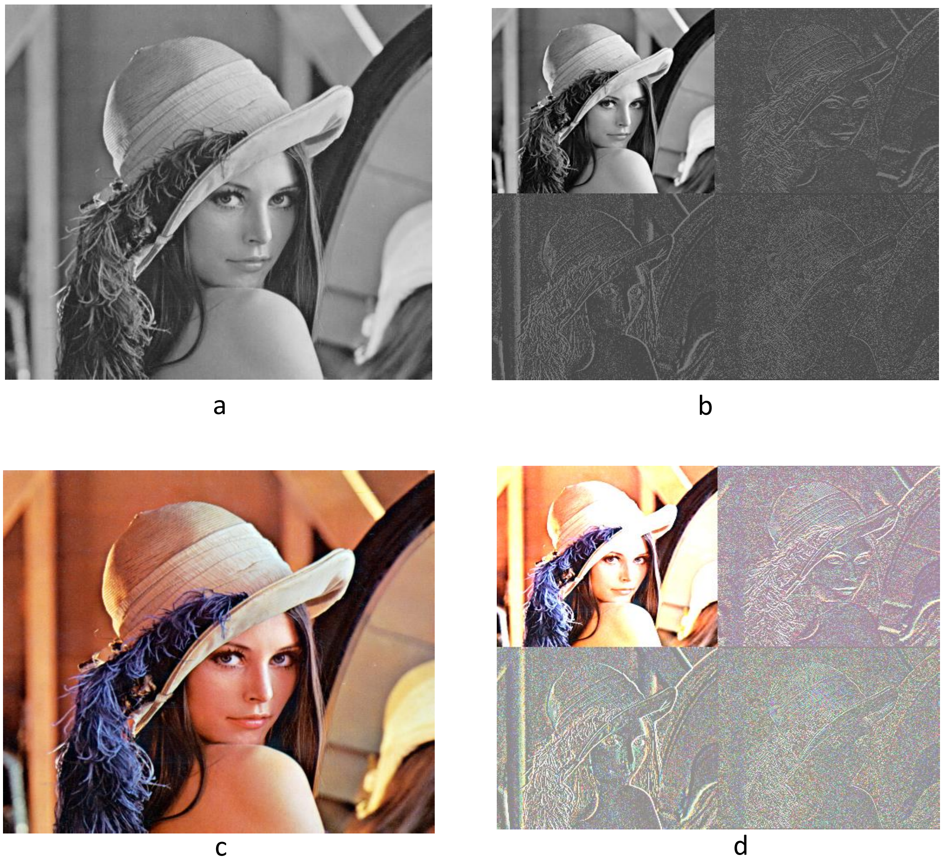


Figure 4.2: a) Gray-scale Lena image, b) decompose gray-scale Lena image one level DWT, c) color Lena image, d) decompose color Lena image one level DWT

4.3 Discrete Cosine Transformation (DCT)

The discrete cosine transform is closely related to the discrete Fourier transform. Where the one-dimensional DCT is useful in processing one-dimensional signal such as speech waveforms, but in the digital image processing (two-dimensional), we need to two -dimensional DCT [3][13]. The 2-D DCT definition for an input image A and output image B is defined as following:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\left(\frac{\pi(2m+1)p}{2M}\right) \cos\left(\frac{\pi(2n+1)q}{2N}\right), \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix} \quad (4.1)$$

where,

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases} \quad (4.2)$$

and,

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases} \quad (4.3)$$

M and *N* are size of *A*, and the corresponding DCT coefficient B_{00} is often called the DC coefficient. Figure 4.3 show (8×8) DCT blocks, where the horizontal frequencies increase from the left to the right and the vertical frequencies increase from the top to the bottom.

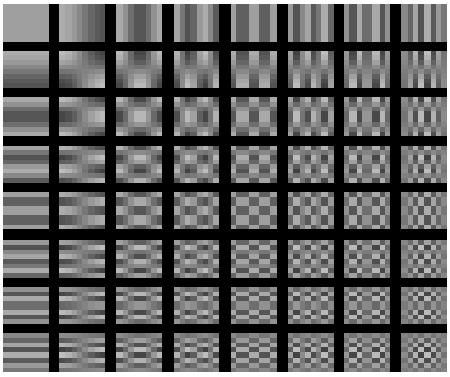


Figure 4.3: (8×8) DCT blocks [3]

4.4 Singular Value Decomposition (SVD)

The SVD is one of linear algebra tools. And, it is an approximation and factorization technique that effectively reduces any matrix into a smaller invertible matrix, where SVD of a rectangular matrix A is a decomposition of the form [14][15]:

$$\mathrm{A}_{(\mathrm{M}*\mathrm{N})} = \mathrm{U}_{(\mathrm{M}*\mathrm{M})}\mathrm{S}_{(\mathrm{M}*\mathrm{N})}\mathrm{V}_{(\mathrm{N}*\mathrm{N})} \tag{4.4}$$

Where *U* and *V* are orthogonal matrices and *S (sigma)* is a diagonal matrix. The columns of *U* are called the left singular vectors and the columns of *V* are called the right singular vectors and the diagonal elements of *S* are called the singular values (non-negative diagonal elements in decreasing order).

4.5 Arnold Transformation

Arnold Transform is commonly known as cat face transform and is a simple chaotic method. It changes the position of pixels and if done several times, scrambled image is obtained and is only suitable for square images. The decryption of image depends on transformation periods. Period changes in accordance with size of image like Figure 3.4. In addition, Iteration number is used as the encryption key. In other words, when Arnold transform is applied, the image can do iteration, the iteration number is used as a secret key for extracting the secret image [16][17]. Arnold transform is defined as follows:

$$\begin{pmatrix} \mathrm{x}' \\ \mathrm{y}' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} \mathrm{x} \\ \mathrm{y} \end{pmatrix} \bmod \mathrm{N} \tag{4.5}$$

Where (x, y) is the position of the pixels in the original image, (x', y') is the position of the pixels after the Arnold transform and N is the size of an image. The watermark image is scrambled using Arnold transform to ensure its security. Usually scrambling transform (or Arnold transform) is used to encrypt the watermark. After a scrambling transform, the watermark image becomes chaotic. The attacker can not extract the watermark, if the key and the scrambling algorithm are not known. Therefore, the Arnold transform gives a security for the digital content and robustness of the algorithm because the spatial relationships of the pixels of an image have been destroyed completely [17][18][19].

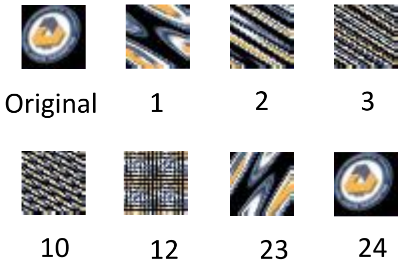


Figure 4.4: Arnold transform applied to color EMU logo with different iteration number

In Figure 4.4, Arnold transform has been applied to color EMU logo (32×32). As shown, in 24Th iteration, the EMU logo reappears.

Chapter 5

PROPOSED DWT, DCT AND SVD BASED WATERMARKING TECHNIQUES

5.1 Introduction

This chapter shows seven methods, these methods are based on DWT, DCT and SVD. In general, these methods encode the watermark image into the original image in frequency domain in low frequency band (LL) by the combined DWT and DCT. This gives more quality and robustness of the watermark technique against various attacks. In addition, we use SVD to increase the quality and robustness of the watermark technique.

Every method consists of two stages which is embedding procedure and extraction procedure. After that, it will calculate the quality and robustness of the watermark technique using the PSNR, SSIM and correlation coefficient (CC). The results of this algorithm are available in next chapter.

5.2 Proposed Method I: Gray Image Watermarking Technique

This method consists of two stages; the first stage is the embedding procedure, in this stage, the watermark image with size (32×32) will be embedded into the original image with size (512×512) based on DWT, DCT and SVD as shown in Figure 5.1. The second stage is the extraction procedure that is used to extract the watermark image. In this method, the original image and the watermark image are gray-scale images.

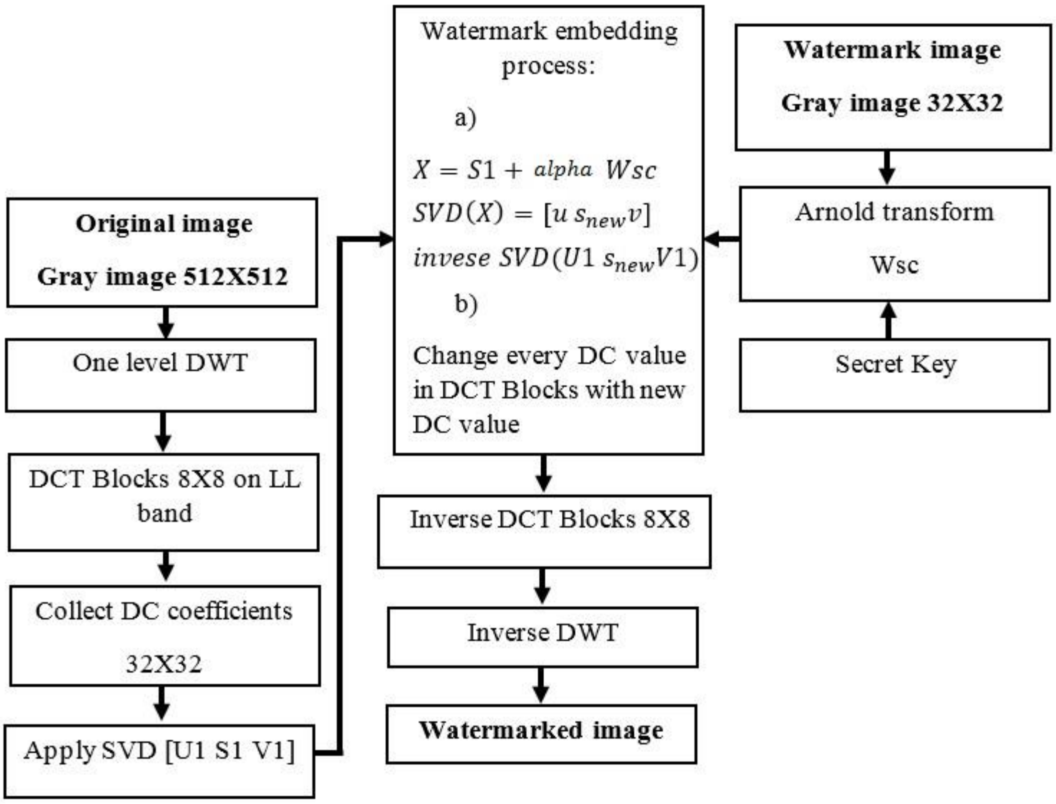


Figure 5.1: The embedding procedure of proposed method I

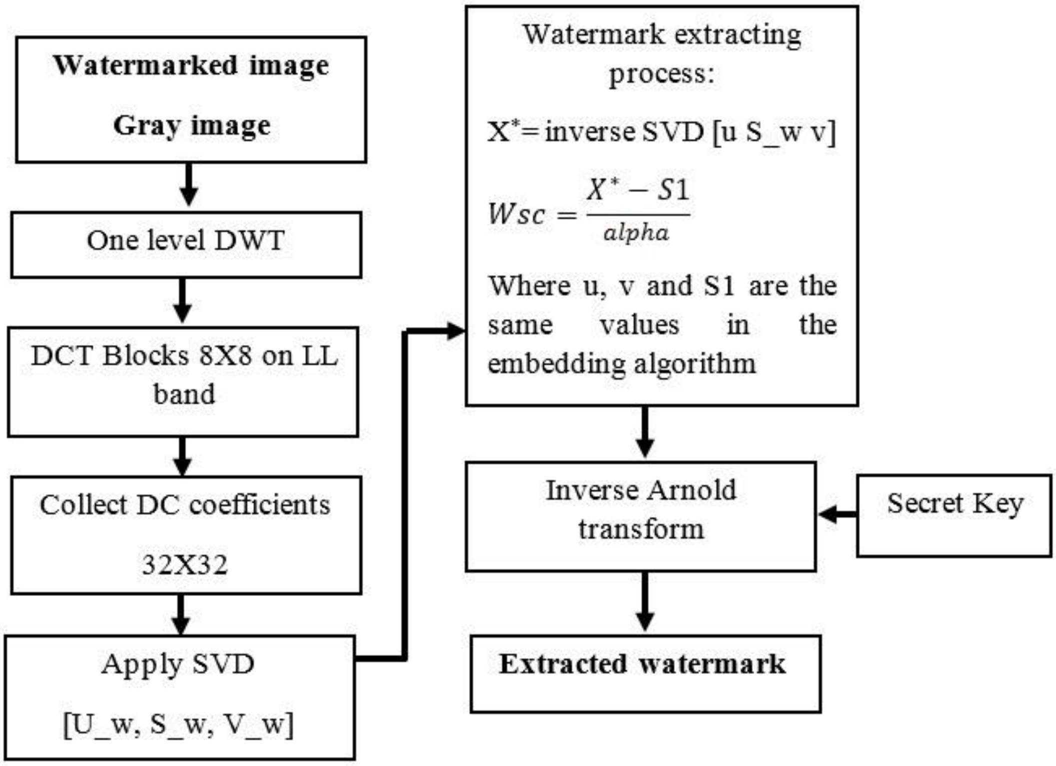

Watermark extracting process:
X*= inverse SVD [u S_w v]
$Wsc = \frac{X^* - S1}{alpha}$
Where u, v and S1 are the same values in the embedding algorithm
Watermarked image
Gray image
One level DWT
DCT Blocks 8X8 on LL band
Collect DC coefficients
32X32
Apply SVD
[U_w, S_w, V_w]
Inverse Arnold transform
Secret Key
Extracted watermark

Figure 5.2: The extraction procedure of proposed method I

5.3 Proposed Method II: Image Watermarking Technique in RGB Color Space using Gray watermark image

In this scheme, the original image is color image and the watermark image is gray-scale image. In addition, this method divides into two stages the embedding procedure and the extraction procedure as shown in Figures 5.3-5.4. In the embedding stage, the watermark image with size (32×32) will be embedded into the original image with size (512×512) in R "Red" component. In addition, the watermark image is extracted from the watermarked image in the extraction stage.

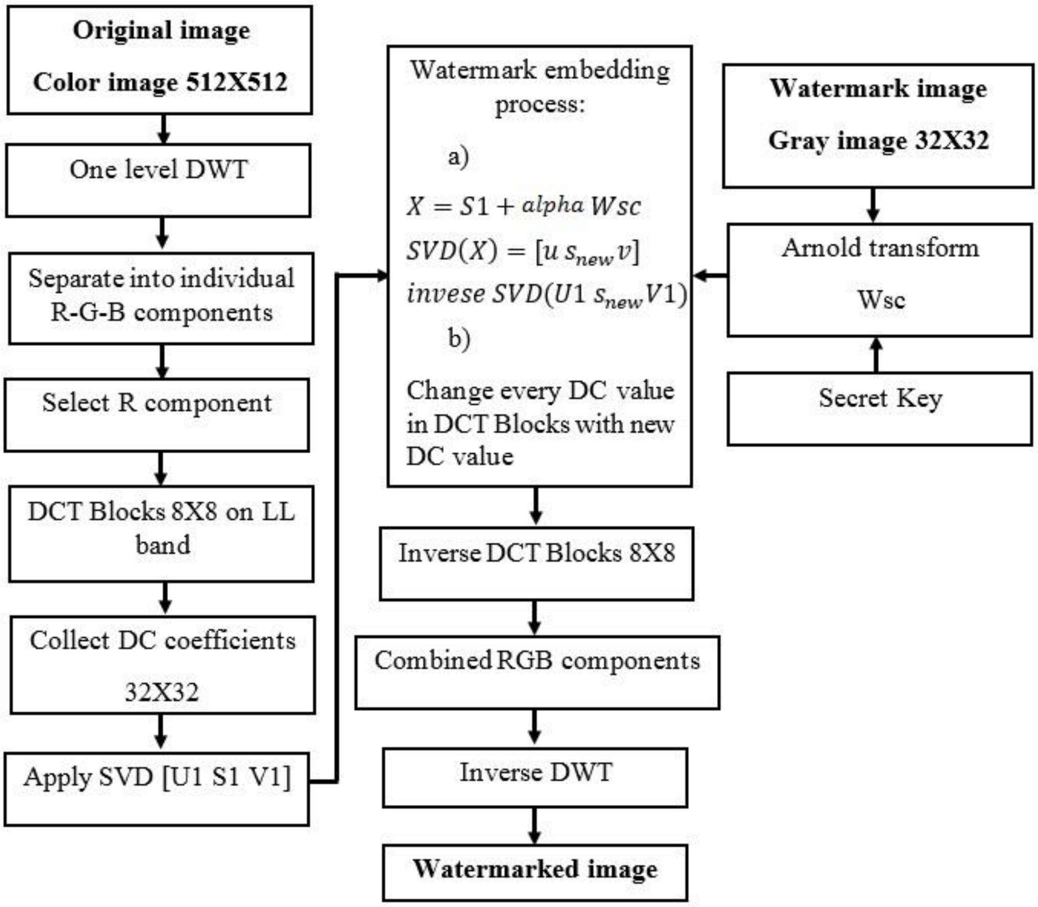


Figure 5.3: The embedding procedure of proposed method II

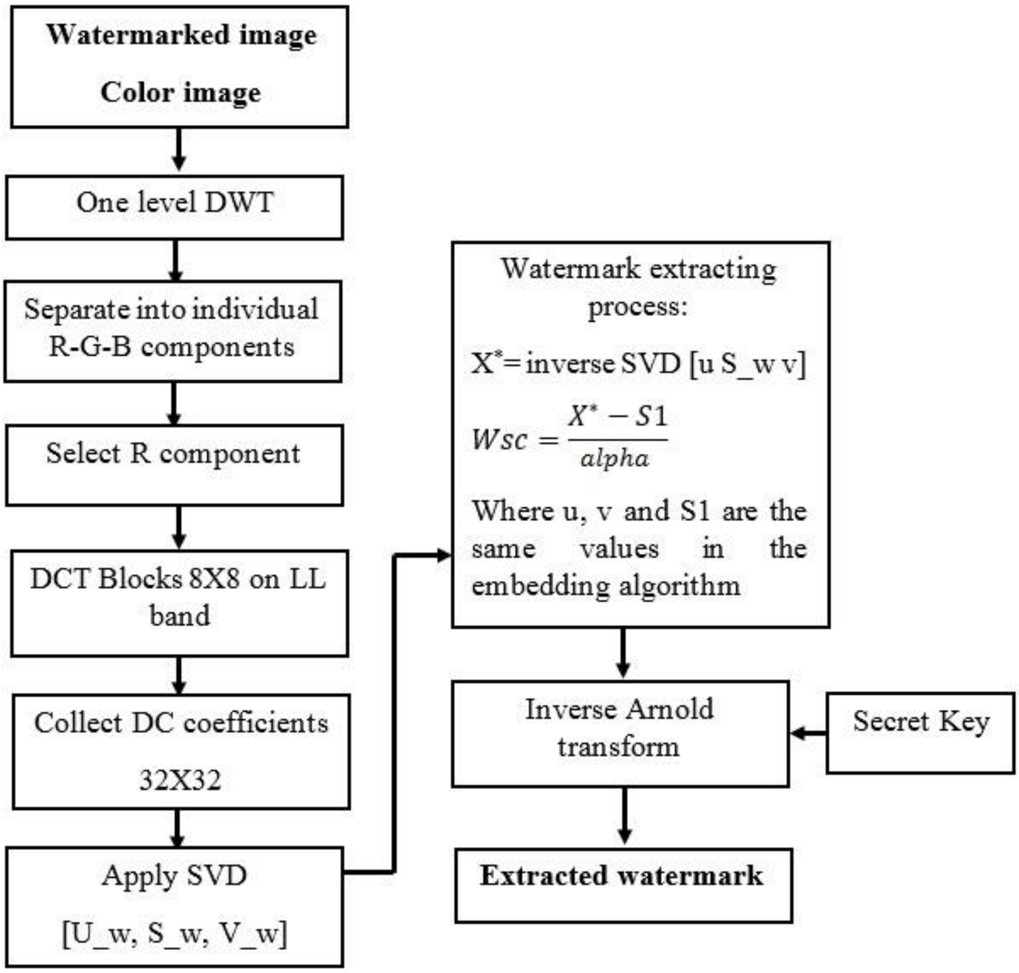

Watermarked image
Color image
One level DWT
Separate into individual R-G-B components
Select R component
DCT Blocks 8X8 on LL band
Collect DC coefficients
32X32
Apply SVD
[U_w, S_w, V_w]
Watermark extracting process:
X*= inverse SVD [u S_w v]
$Wsc = \frac{X^* - S1}{alpha}$
Where u, v and S1 are the same values in the embedding algorithm
Inverse Arnold transform
Secret Key
Extracted watermark

Figure 5.4: The extraction procedure of proposed method II

5.4 Proposed Method III: Image Watermarking Technique in RGB Color Space using Color watermark image

In this scheme, the original image and the watermark image are color images. In addition, this method consists of two stages [the embedding procedure and the extraction procedure]. In the embedding stage, the watermark image with size (32×32) will be embedded into the original image with size (512×512) in RGB components as shown in Figure 5.5. The second stage is the extraction procedure that is used to extract the watermark image.

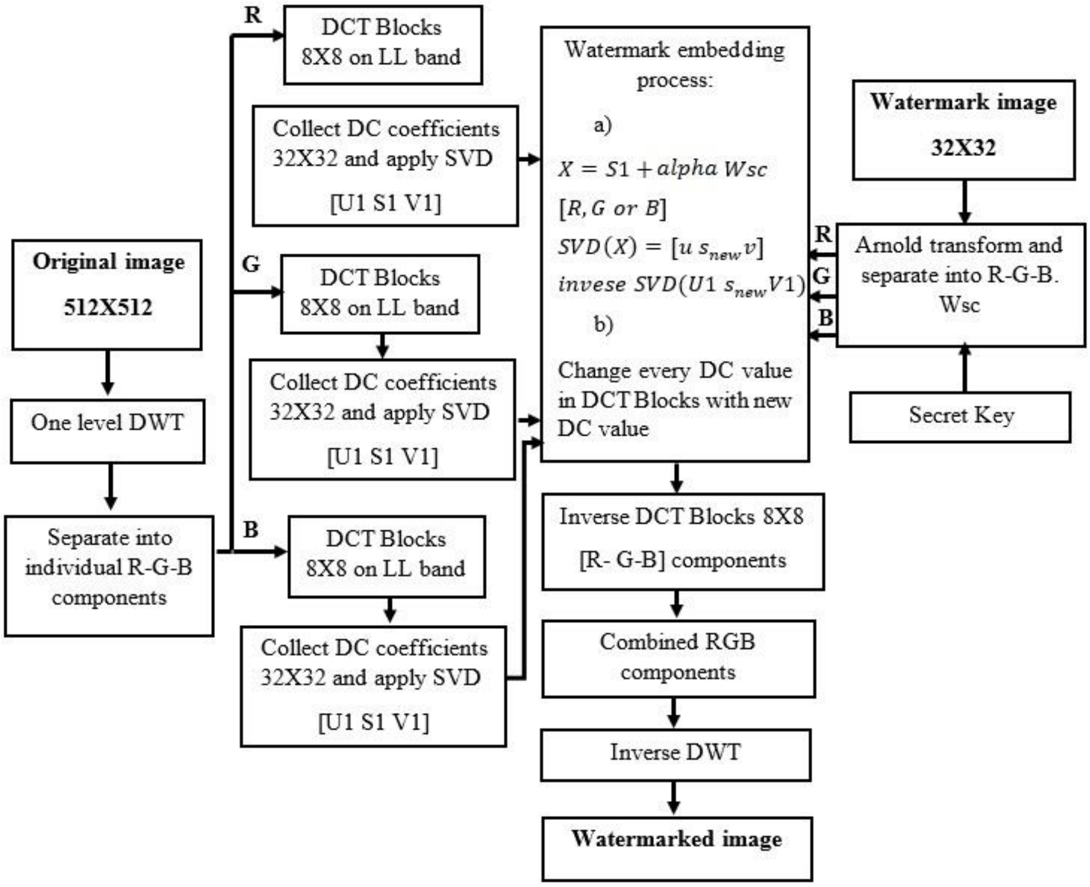

Original image
512X512
One level DWT
Separate into individual R-G-B components
R
G
B
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
Watermark embedding process:
a)
$X = S1 + alpha\ Wsc$
$[R, G\ or\ B]$
$SVD(X) = [u\ s_{new} v]$
$invese\ SVD(U1\ s_{new} V1)$
b)
Change every DC value in DCT Blocks with new DC value
Watermark image
32X32
Arnold transform and separate into R-G-B. Wsc
Secret Key
R
G
B
Inverse DCT Blocks 8X8
[R- G-B] components
Combined RGB components
Inverse DWT
Watermarked image

Figure 5.5: The embedding procedure of proposed method III

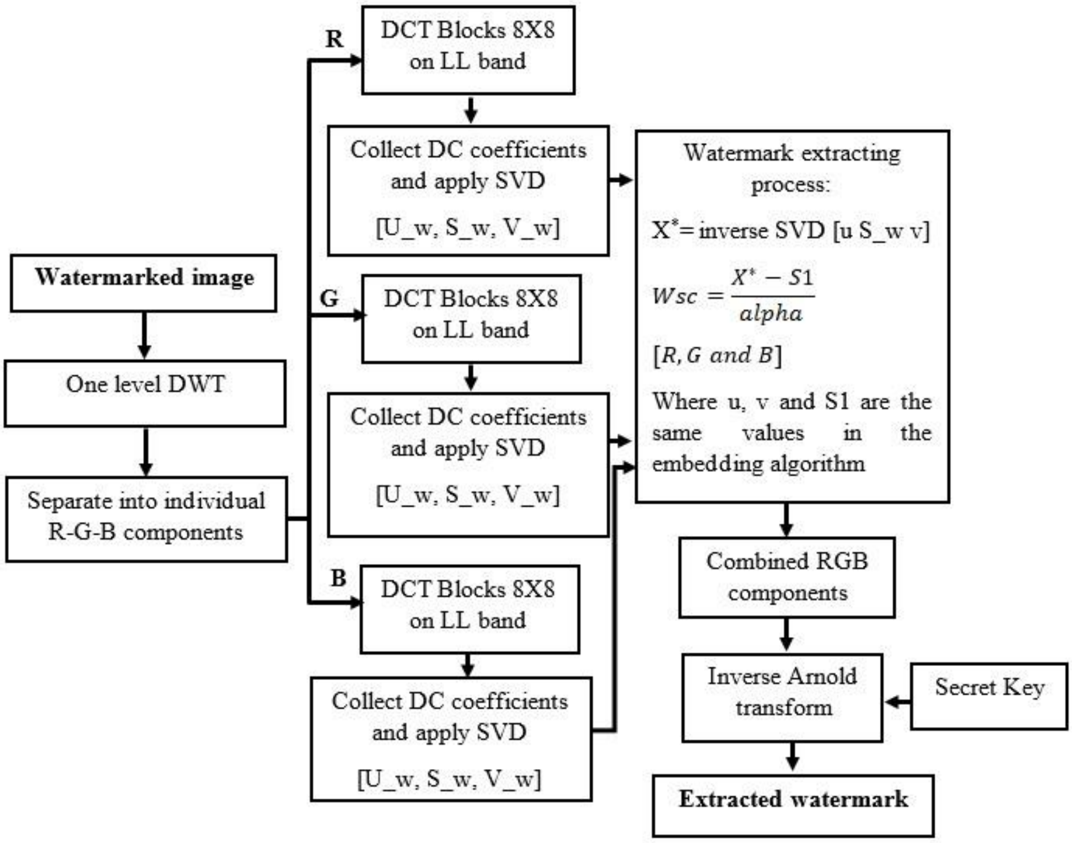

Watermarked image
One level DWT
Separate into individual R-G-B components
R
G
B
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD [U_w, S_w, V_w]
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD [U_w, S_w, V_w]
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD [U_w, S_w, V_w]
Watermark extracting process:
X*= inverse SVD [u S_w v]
Wsc = (X* − S1)/alpha
[R, G and B]
Where u, v and S1 are the same values in the embedding algorithm
Combined RGB components
Inverse Arnold transform
Secret Key
Extracted watermark

Figure 5.6: The extraction procedure of proposed method III

5.5 Proposed Method IV: Image Watermarking Technique in YIQ Color Space using Gray watermark image

In this scheme, the original image is color image and the watermark image is gray-scale image. In addition, this method divides into two stages [the embedding procedure and the extraction procedure] as shown in Figures 5.7-5-8. In the embedding stage, the original image with size (512×512) will be converted from RGB into YIQ color space, and then the watermark image with size (32×32) will be embedded into the original image in Y component. In addition, the watermark image is extracted from the watermarked image in the extraction stage.

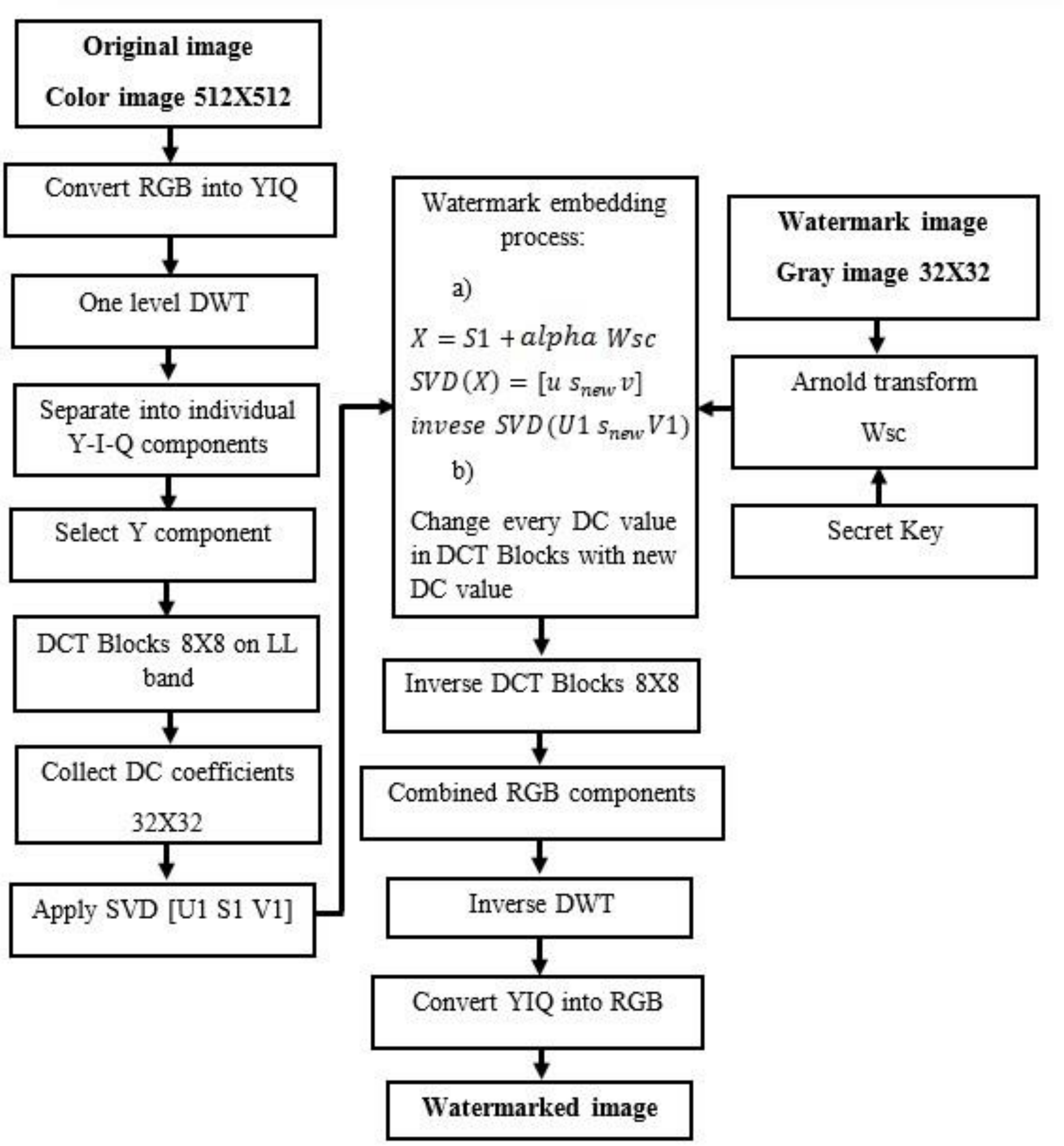


Figure 5.7: The embedding procedure of proposed method IV

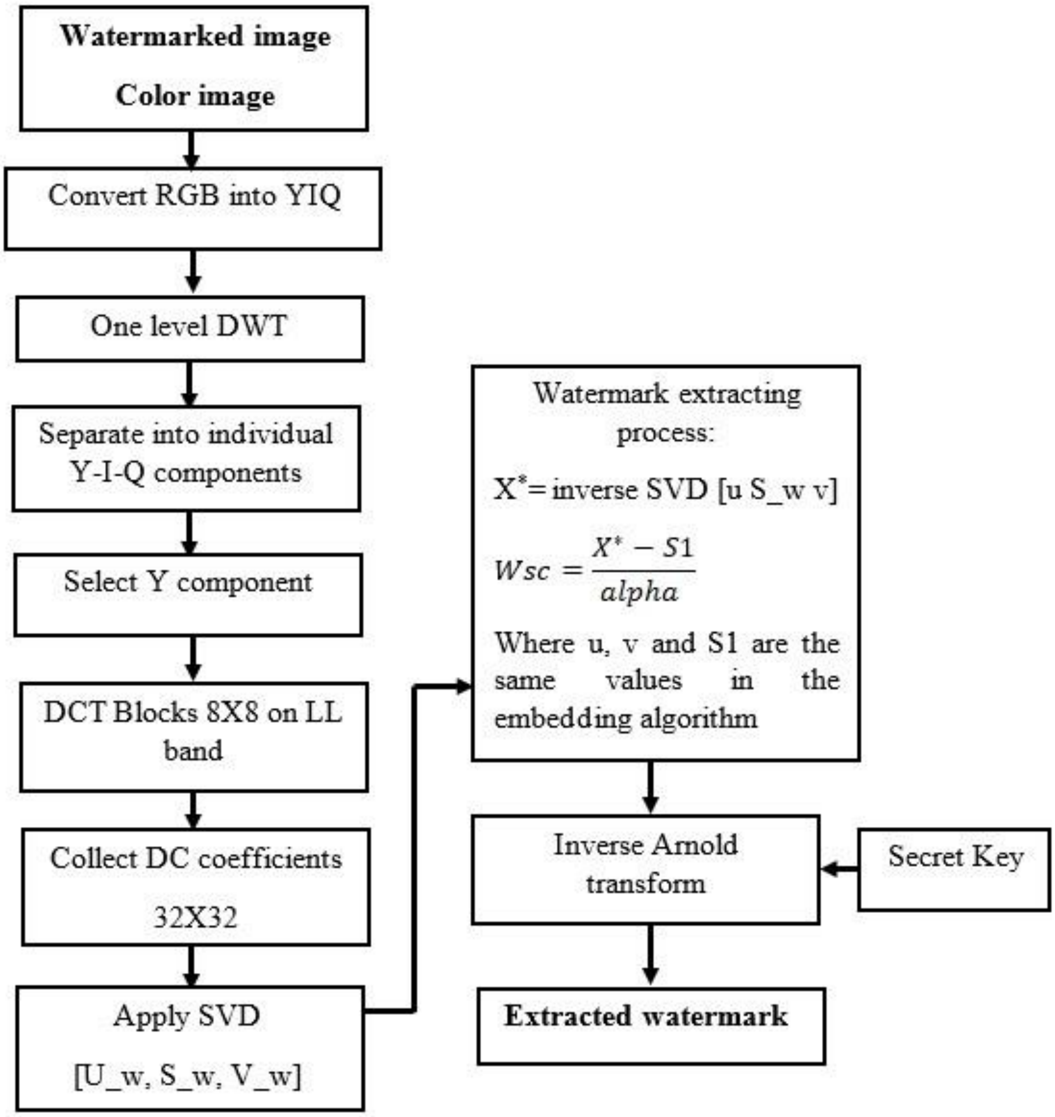
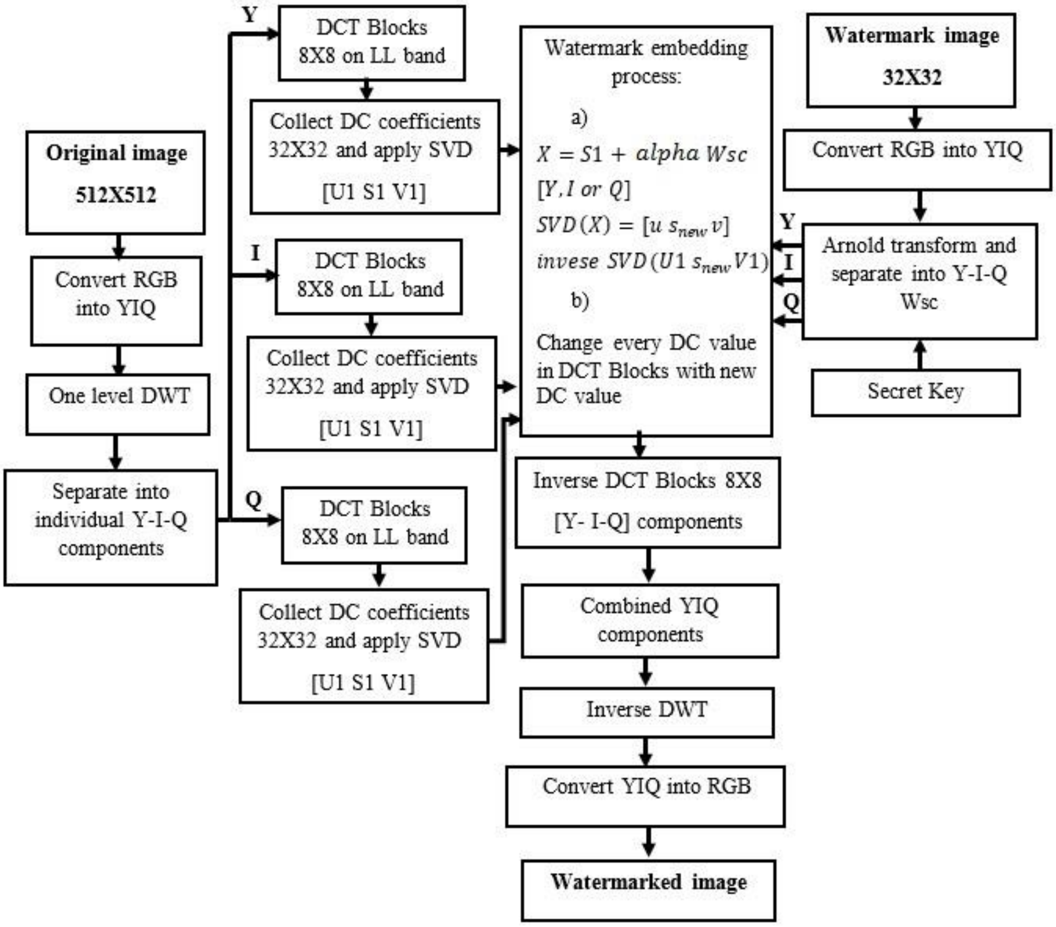

Watermarked image
Color image
Convert RGB into YIQ
One level DWT
Separate into individual Y-I-Q components
Select Y component
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32
Apply SVD [U_w, S_w, V_w]
Watermark extracting process:
X*= inverse SVD [u S_w v]
$Wsc = \frac{X^* - S1}{alpha}$
Where u, v and S1 are the same values in the embedding algorithm
Inverse Arnold transform
Secret Key
Extracted watermark

Figure 5.8: The extraction procedure of proposed method IV

5.6 Proposed Method V: Image Watermarking Technique in YIQ Color Space using Color watermark image

In this scheme, the original image and the watermark image are color images. In addition, this method divides into two stages [the embedding procedure and the extraction procedure] as shown in Figures 5.9-5.10. In the embedding stage, the original image with size (512×512) will be converted from RGB into YIQ color space, and then the watermark image with size (32×32) will be embedded into the original image in YIQ components. In addition, the watermark image is extracted from the watermarked image in the extraction stage.



Original image
512X512
Convert RGB into YIQ
One level DWT
Separate into individual Y-I-Q components
Y
I
Q
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
Watermark embedding process:
a)
$X = S1 + alpha\ Wsc$
$[Y, I\ or\ Q]$
$SVD(X) = [u\ s_{new}\ v]$
$invese\ SVD(U1\ s_{new}\ V1)$
b)
Change every DC value in DCT Blocks with new DC value
Watermark image
32X32
Convert RGB into YIQ
Arnold transform and separate into Y-I-Q Wsc
Secret Key
Y
I
Q
Inverse DCT Blocks 8X8
[Y- I-Q] components
Combined YIQ components
Inverse DWT
Convert YIQ into RGB
Watermarked image

Figure 5.9: The embedding procedure of proposed method V

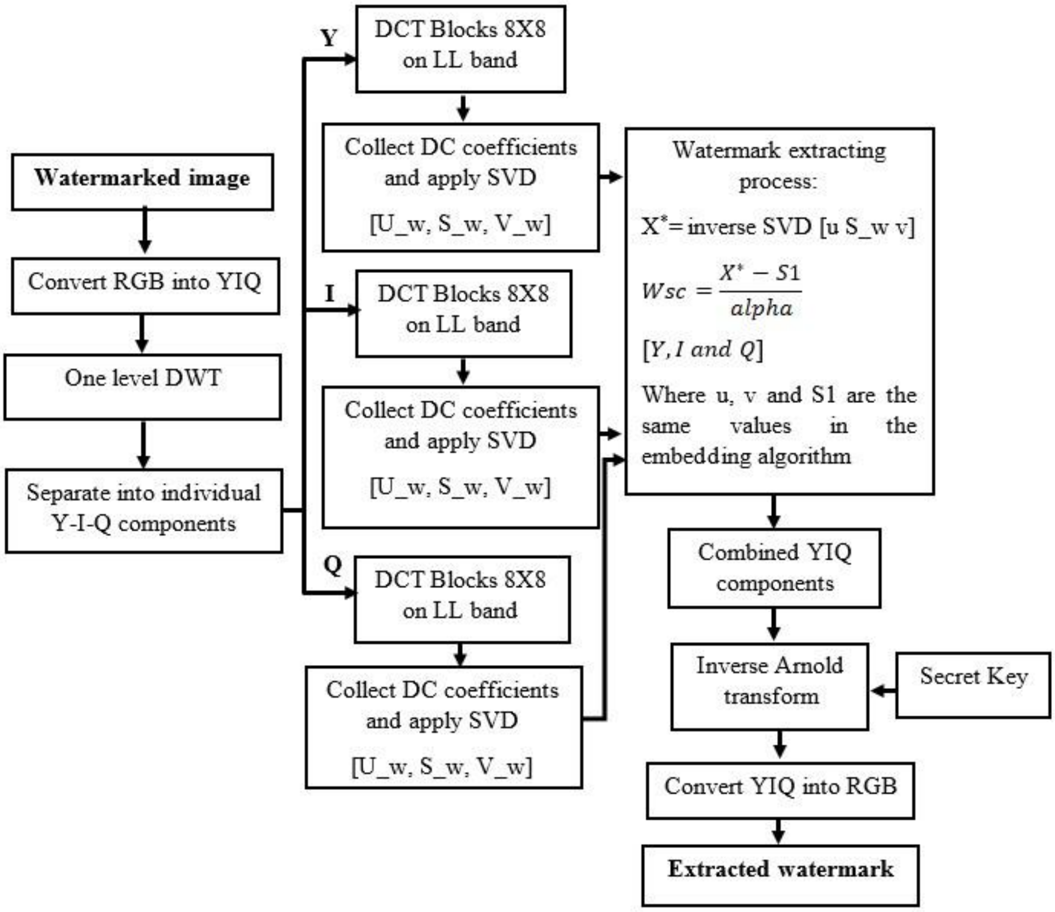

Watermarked image
Convert RGB into YIQ
One level DWT
Separate into individual Y-I-Q components
Y
I
Q
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD [U_w, S_w, V_w]
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD [U_w, S_w, V_w]
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD [U_w, S_w, V_w]
Watermark extracting process:
X*= inverse SVD [u S_w v]
Wsc = (X* − S1) / alpha
[Y, I and Q]
Where u, v and S1 are the same values in the embedding algorithm
Combined YIQ components
Inverse Arnold transform
Secret Key
Convert YIQ into RGB
Extracted watermark

Figure 5.10: The extraction procedure of proposed method V

5.7 Proposed Method VI: Image Watermarking Technique in YCbCr Color Space using Gray watermark image

In this scheme, the original image is color image and the watermark image is gray-scale image. In addition, this method divides into two stages [the embedding procedure and the extraction procedure] as shown in Figures 5.11-512. In the embedding stage, the original image with size (512×512) will be converted from RGB into YCbCr color space, and then the watermark image with size (32×32) will be embedded into the original image in Y component. In addition, the watermark image is extracted from the watermarked image in the extraction stage.

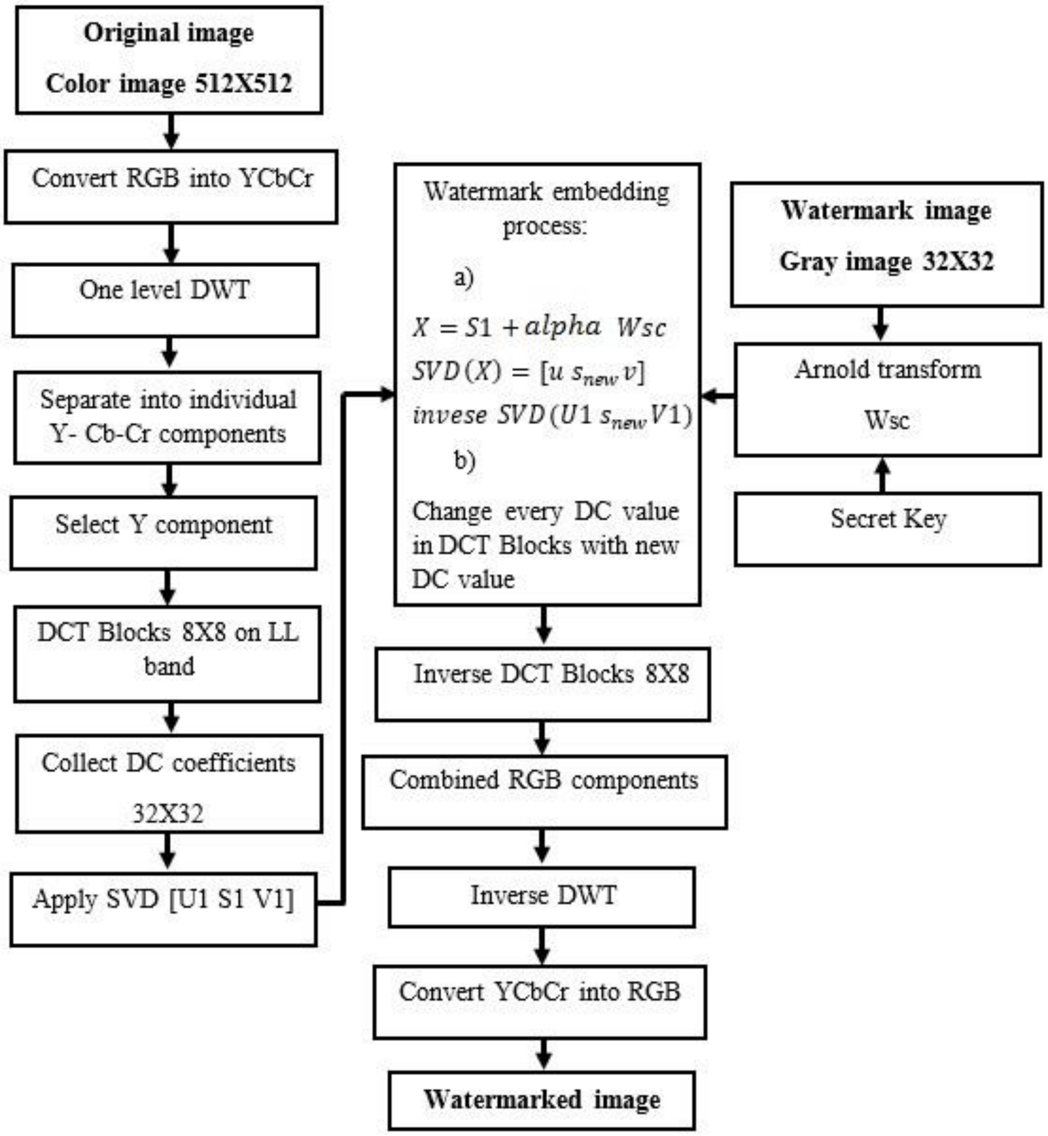


Figure 5.11: The embedding procedure of proposed method VI

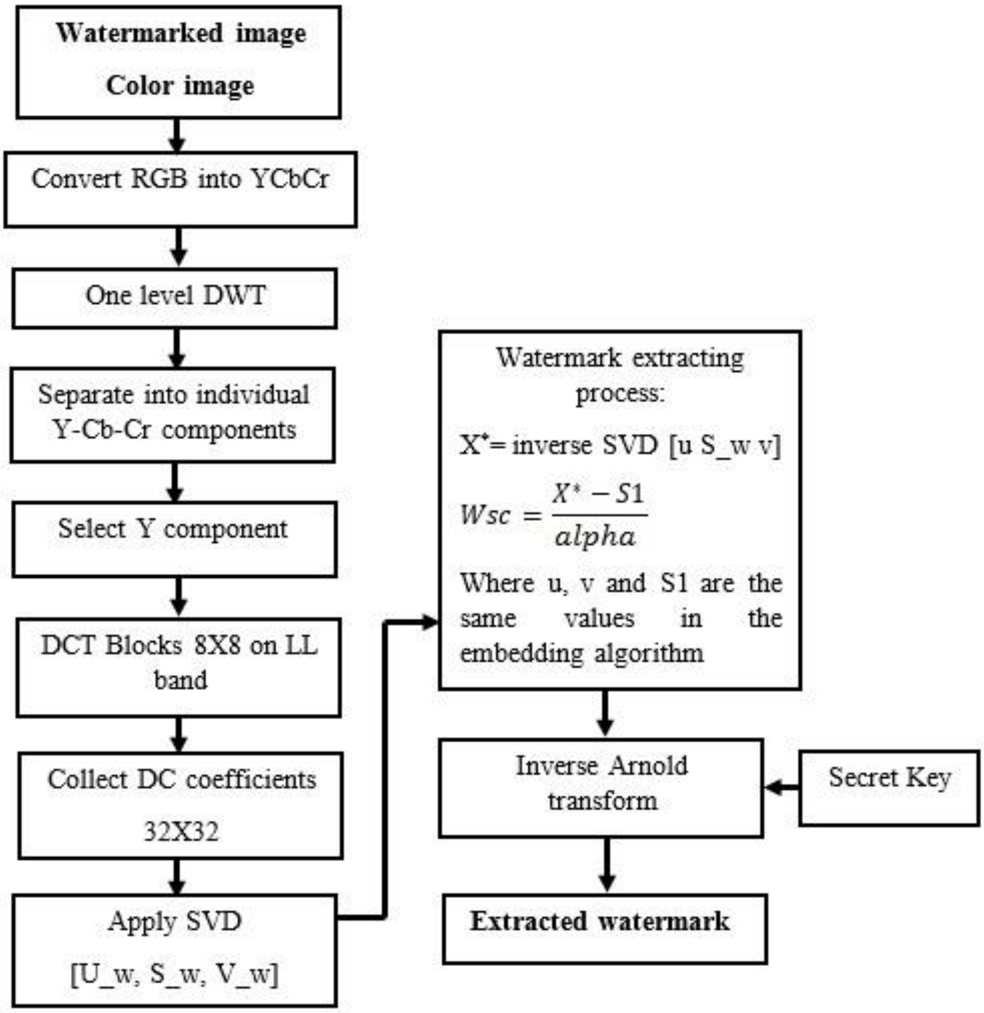

Watermarked image
Color image
Convert RGB into YCbCr
One level DWT
Separate into individual Y-Cb-Cr components
Select Y component
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32
Apply SVD [U_w, S_w, V_w]
Watermark extracting process:
X*= inverse SVD [u S_w v]
$Wsc = \frac{X^{*} - S1}{alpha}$
Where u, v and S1 are the same values in the embedding algorithm
Inverse Arnold transform
Secret Key
Extracted watermark

Figure 5.12: The extraction procedure of proposed method VI

5.8 Proposed Method VII: Image Watermarking Technique in YCbCr Color Space using Color watermark image

In this scheme, the original image and the watermark image are color images. In addition, this method consists of two stages [the embedding procedure and the extraction procedure]. In the embedding stage, the original image with size (512×512) will be converted from RGB into YCbCr color space, and then the watermark image with size (32×32) will be embedded into the original image in YCbCr components. The second stage is the extraction procedure The second stage is the extraction procedure that is used to extract the watermark image.

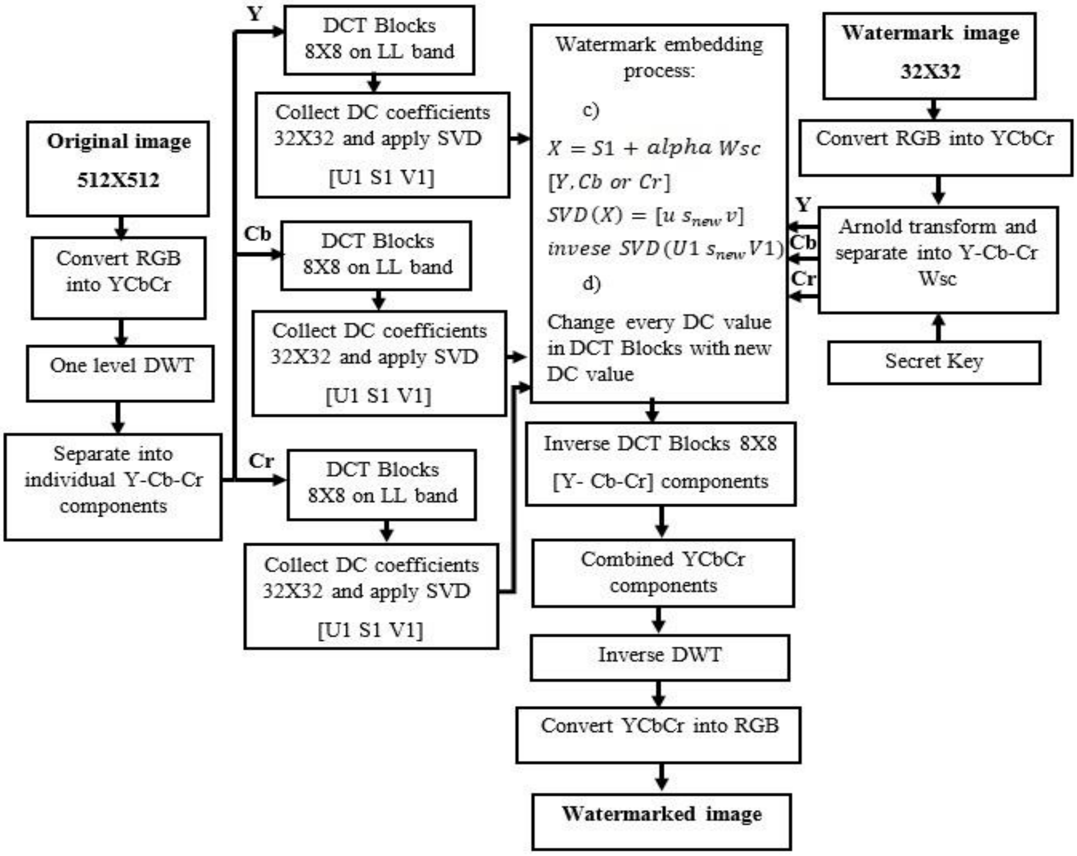

Original image
512X512
Convert RGB into YCbCr
One level DWT
Separate into individual Y-Cb-Cr components
Y
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
Cb
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
Cr
DCT Blocks 8X8 on LL band
Collect DC coefficients 32X32 and apply SVD
[U1 S1 V1]
Watermark embedding process:
c)
$X = S1 + alpha\ Wsc$
$[Y, Cb\ or\ Cr]$
$SVD(X) = [u\ s_{new}\ v]$
$invese\ SVD(U1\ s_{new}\ V1)$
d)
Change every DC value in DCT Blocks with new DC value
Watermark image
32X32
Convert RGB into YCbCr
Arnold transform and separate into Y-Cb-Cr Wsc
Y
Cb
Cr
Secret Key
Inverse DCT Blocks 8X8
[Y- Cb-Cr] components
Combined YCbCr components
Inverse DWT
Convert YCbCr into RGB
Watermarked image

Figure 5.9: The embedding procedure of proposed method VII

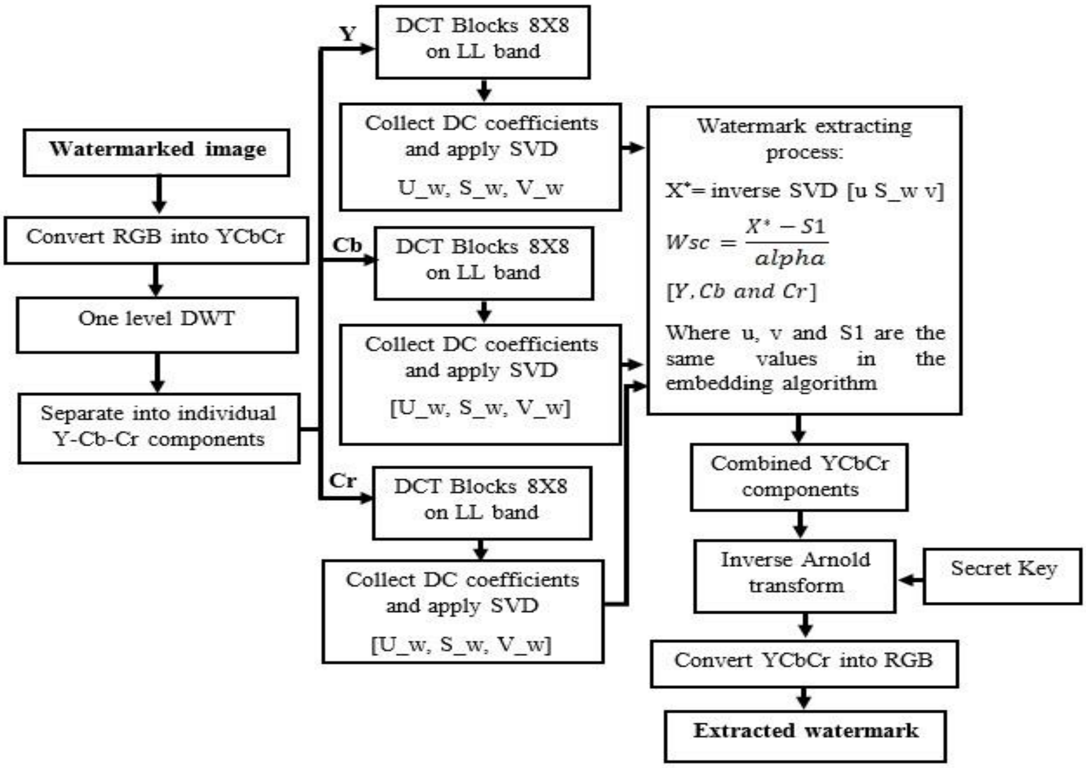

Watermarked image
Convert RGB into YCbCr
One level DWT
Separate into individual Y-Cb-Cr components
Y
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD
U_w, S_w, V_w
Cb
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD
[U_w, S_w, V_w]
Cr
DCT Blocks 8X8 on LL band
Collect DC coefficients and apply SVD
[U_w, S_w, V_w]
Watermark extracting process:
X*= inverse SVD [u S_w v]
$Wsc = \frac{X^* - S1}{alpha}$
$[Y, Cb\ and\ Cr]$
Where u, v and S1 are the same values in the embedding algorithm
Combined YCbCr components
Inverse Arnold transform
Secret Key
Convert YCbCr into RGB
Extracted watermark

Figure 5.10: The extraction procedure of proposed method VII

Chapter 6

EXPERIMENTAL RESULTS & ANALYSIS

6.1 Introduction

In this chapter, we will be to show the robustness of our algorithm against attacks such as compression, scaling, rotation and noise .and also, we calculated the quality of watermarked image using Peak Signal to Noise Ratio (PSNR), between the original image and the watermarked image.

To calculate the robustness of the image watermarking technique, we used SSIM to calculate the similarity between the original watermark image and the watermark image recovered after one of the attacks.

We applied the algorithm on Lena image (gray, color) with size (512×512) as the original image and emu-logo (gray, color) with size (32×32) as the watermark image. In addition, we applied the algorithm on the gray and color spaces (RGB, YIQ and YCbCr). In the last, the analysis will be based on these results.

6.2 Evaluating Robustness and Quality of the Image Watermarking Techniques

In order to find the quality and the robustness of the image watermarking technique, we use the peak signal-to-noise ratio (PSNR) and structural similarity index measurement (SSIM). Where, the PSNR is measured between the original image and watermarked image, and the SSIM is measured between the watermark image and the extracted watermark after the attacks such as the compression, the scaling, the rotation and the noise.

6.2.1 Peak Signal to Noise Ratio (PSNR)

The PSNR commonly used to measure the quality of images depending on difference of pixels between two images; the PSNR (dB) is defined as in:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \tag{6.1}$$

For color image, the PSNR (dB) is defined as in:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{[\mathrm{MSE(R)}+\mathrm{MSE(G)}+\mathrm{MSE(B)}]/3}\right) \tag{6.2}$$

Where MSE is computed by averaging the squared intensity of the original (input) image and the resultant (output) image pixels, the MSE is defined as in:

$$\mathrm{MSE} = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M\times N} \tag{6.3}$$

Where *M* and *N* are size of input images, respectively and I_1 (m, n) is the original image, I_2 (m, n) is the resultant image (here the watermarked image) [20].

Note:

The original image and the resultant image are the same size.

6.2.2 Structural Similarity Index Measurement (SSIM)

Structural similarity index measurement (SSIM) is a novel method to measure the quality of images and the similarity between two images. The SSIM will vary between two values 0 and +1, the SSIM is defined as in:

$$\mathrm{SSIM}(x,y) = [l(x,y)]^{\alpha}\cdot[c(x,y)]^{\beta}\cdot[s(x,y)]^{\gamma} \tag{6.4}$$

where,

$$l(x,y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2\mu_y^2 + c_1}, \tag{6.5}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2\sigma_y^2 + c_2}, \tag{6.6}$$

$$s(x,y) = \frac{\sigma_{xy}+c_3}{\sigma_x\ \sigma_y\ +c_3}, \qquad (6.7)$$

Where μ_x and μ_y are the local mean, μ_x and μ_y are the standard deviations and the cross-covariance for images *x*, *y*. If α = β = γ = 1 (the default for Exponents), and $C_3 = C_2/2$ (default selection of C_3) [21], the SSIM is defined as in:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\mu_x^2+\mu_y^2+c_2)} \qquad (6.8)$$

6.2.3 Correlation Coefficient (CC)

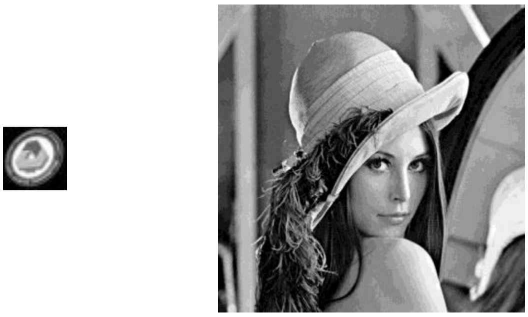
The correlation coefficient (or cross-correlation coefficient) also used to measure the quality of images and the similarity between two images. The correlation coefficient will vary between two values -1 and +1, where +1 value means a perfect positive correlation and -1 value means a perfect negative correlation, the CC is defined as in:

$$\mathrm{CC} = \frac{\sum_{M,N}[I_1(m,n).I_2(m,n)]}{\sqrt{\sum_{M,N}[I_1(m,n)]^2.\sum_{M,N}[I_2(m,n)]^2}} \qquad (6.9)$$

Where *M* and *N* are size of input images, respectively and I_1 (m, n) is the watermark image, I_2 (m, n) is the extracted image.

6.3 Proposed Method I Results: Gray Image Watermarking Technique

All of the proposed approaches are simulated by using MATLAB software. In this section, the original image is gray-scale Lena image (512×512) and gray scale watermark image is a gray-scale emu-logo (32×32).



a b

Figure 6.1: a) Gray-scale watermark image, b) Gray-scale Lena image

In this algorithm the watermark image is encrypted using Arnold transform with a secret key (the iteration number) equal one.

a b

Figure 6.2: a) Gray-scale watermark image, b) Arnold transform apply on watermark image "Iteration number=1"

In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.1. After the embedding stage, the result image that is called watermarked image is shown in following figure:

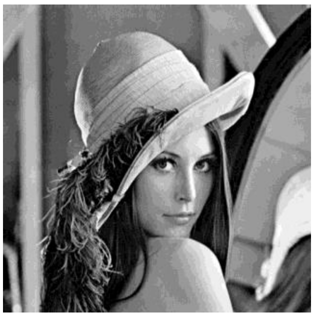


Figure 6.3: The watermarked image

To extract the watermark image from the watermarked image, we apply the extraction procedure.

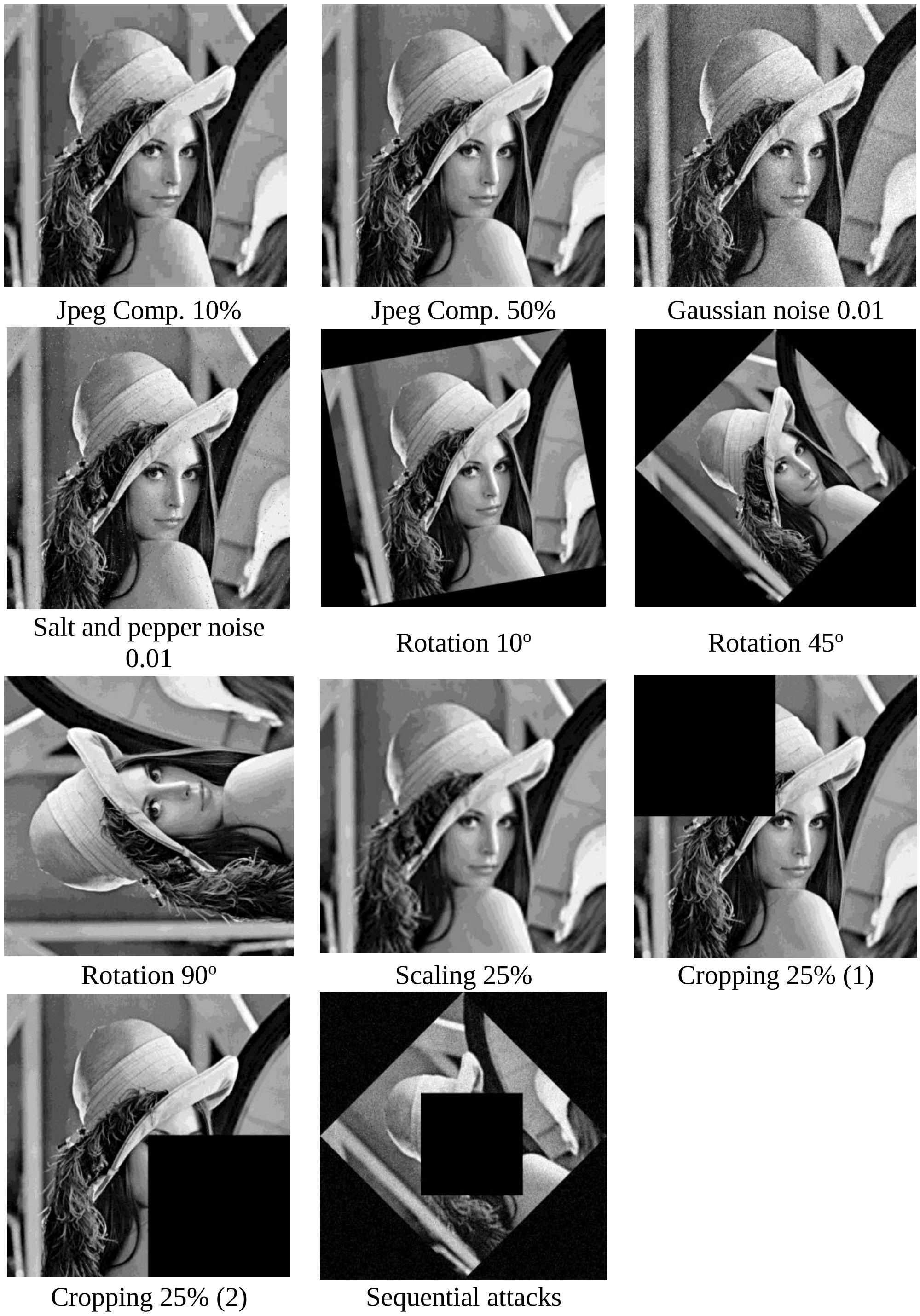
Figure 6.4: The extracted watermark

To test the performance of the proposed algorithm, we calculated the PSNR between the watermarked image and the original image which equal 81.81dB. In addition, the different of attacks are applied on the proposed scheme like the compression, the scaling, the rotation, the noise, the cropping and sequential attacks (jpeg comp. 10%, scaling 25%, rotation 45^0, Gaussian noise 0.01 and the cropping 25%), to calculate the robustness of the image watermarking technique. Also, we use the SSIM to measure the similarity between the watermark image and the extracted watermark after the attacks. Table 6.1 gives SSIM values of watermarking techniques for different attacks.

Table 6.1: Robustness test of proposed method I

Attacks	**SSIM**
Jpeg Comp. 10%	0.89
Jpeg Comp. 50%	0.97
Gaussian noise 0.01	0.94
Salt and pepper noise	0.95
Rotation 10^0	0.76
Rotation 45^0	0.79
Rotation 90^0	1
Scaling 25%	0.98
Cropping 25% (1)	0.81
Cropping 25% (2)	0.75
Sequential attacks	0.72
Without attack	1

In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10^o

Rotation 45^o

Rotation 90^o

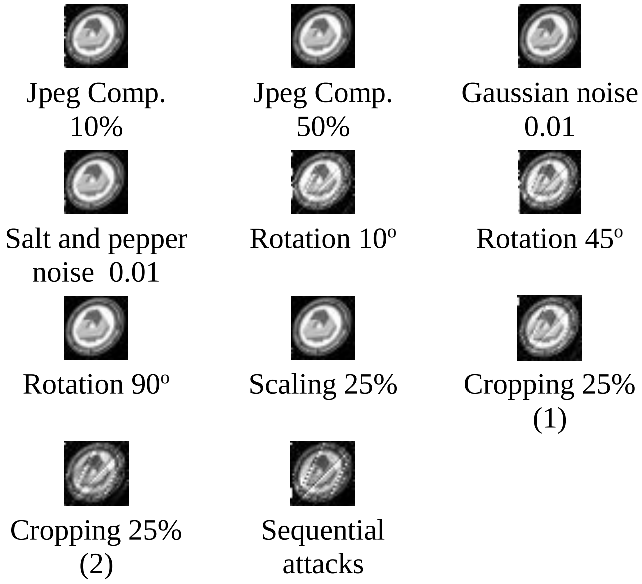
Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.5: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10º

Rotation 45º

Rotation 90º

Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.6: The extracted watermarks after the attacks

6.4 Proposed Method II: Image Watermarking Technique in RGB Color Space using Gray watermark image

In this method, the original image is a color Lena image (512×512) and the watermark image is a gray-scale emu-logo (32×32).

Figure 6.7:a) Color Lena image, b) a gray scale watermark image

In this method, the watermark images is encrypted using Arnold transform with a secret key (the iteration number) equal one as shown in Figure 6.2. In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.1. After the embedding stage, the extracted image and the watermarked image are shown in following figures:

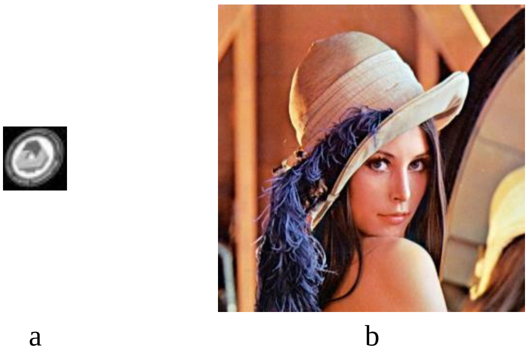


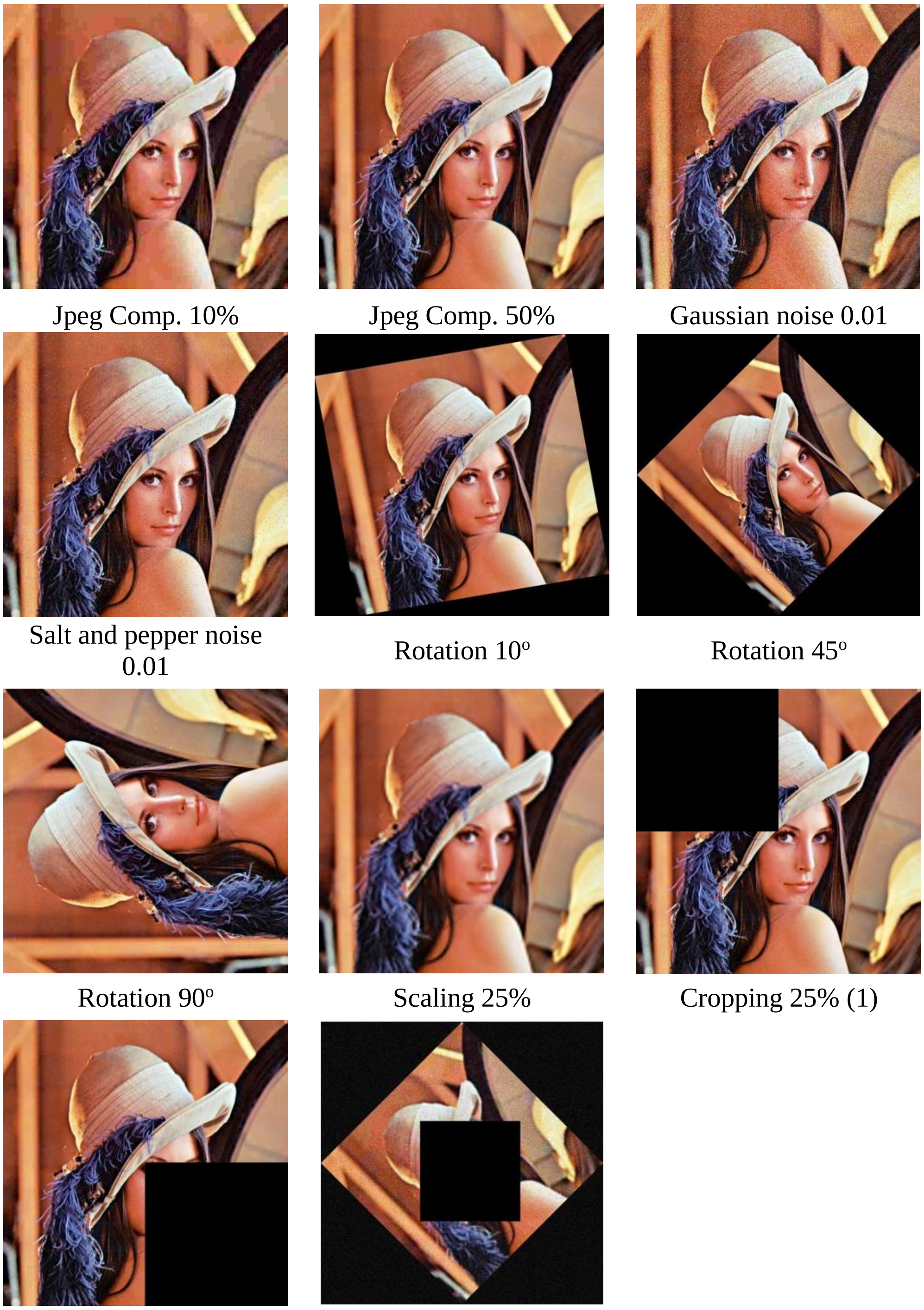
Figure 6.8: a) The extracted image, b) the watermarked image

The PSNR value of proposed method equal 86.80dB. Table 6.2 gives SSIM values of watermarking techniques for different attacks.

Table 6.2: Robustness test of proposed method II

Attacks	**SSIM**
Jpeg Comp. 10%	0.86
Jpeg Comp. 50%	0.94
Gaussian noise 0.01	0.93
Salt and pepper noise 0.01	0.94
Rotate 10^0	0.75
Rotate 45^0	0.77
Rotate 90^0	1
Scaling 25%	0.97
Cropping 25% (1)	0.79
Cropping 25% (2)	0.79
Sequential attacks	0.70
Without attack	1

In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10^o

Rotation 45^o

Rotation 90^o

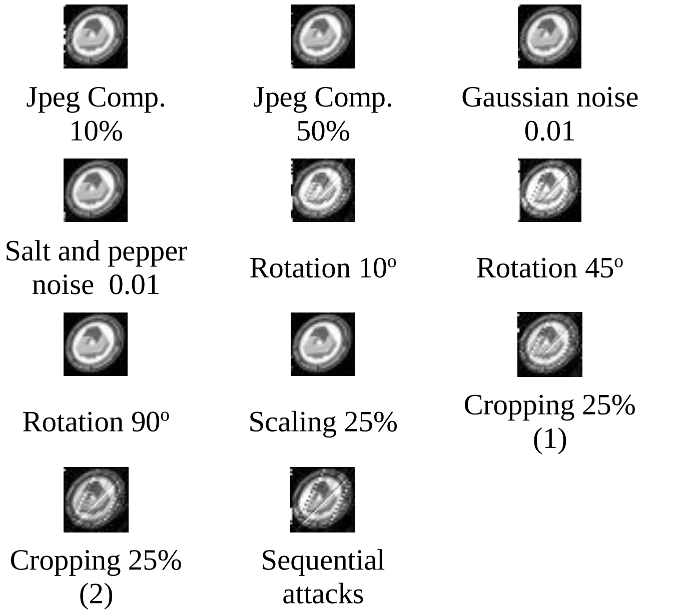
Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.9: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10°

Rotation 45°

Rotation 90°

Scaling 25%

Cropping 25% (1)

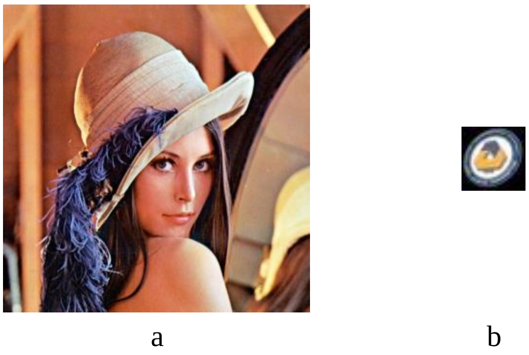
Cropping 25% (2)

Sequential attacks

Figure 6.10: The extracted watermarks after the attacks

6.5 Proposed Method III: Image Watermarking Technique in RGB Color Space using Color watermark image

In this method, the original image is a color Lena image (512×512) and the watermark image is a color emu-logo (32×32).



a

b

Figure 6.11: a) Color Lena image, b) color watermark image

In this method, the watermark image is encrypted using Arnold transform with a secret key (the iteration number) equal one.

Figure 6.12: a) RGB color watermark image, b) Arnold transform apply on the watermark image "Iteration number=1"

In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.1. After the embedding stage, the extracted image and the watermarked image are shown in following figures:

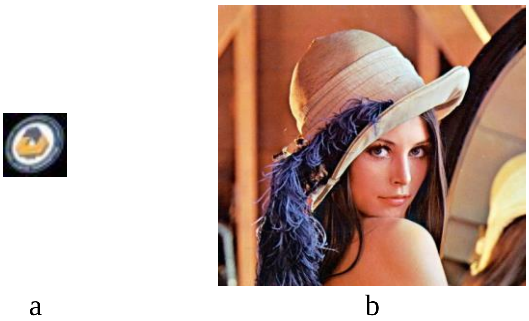


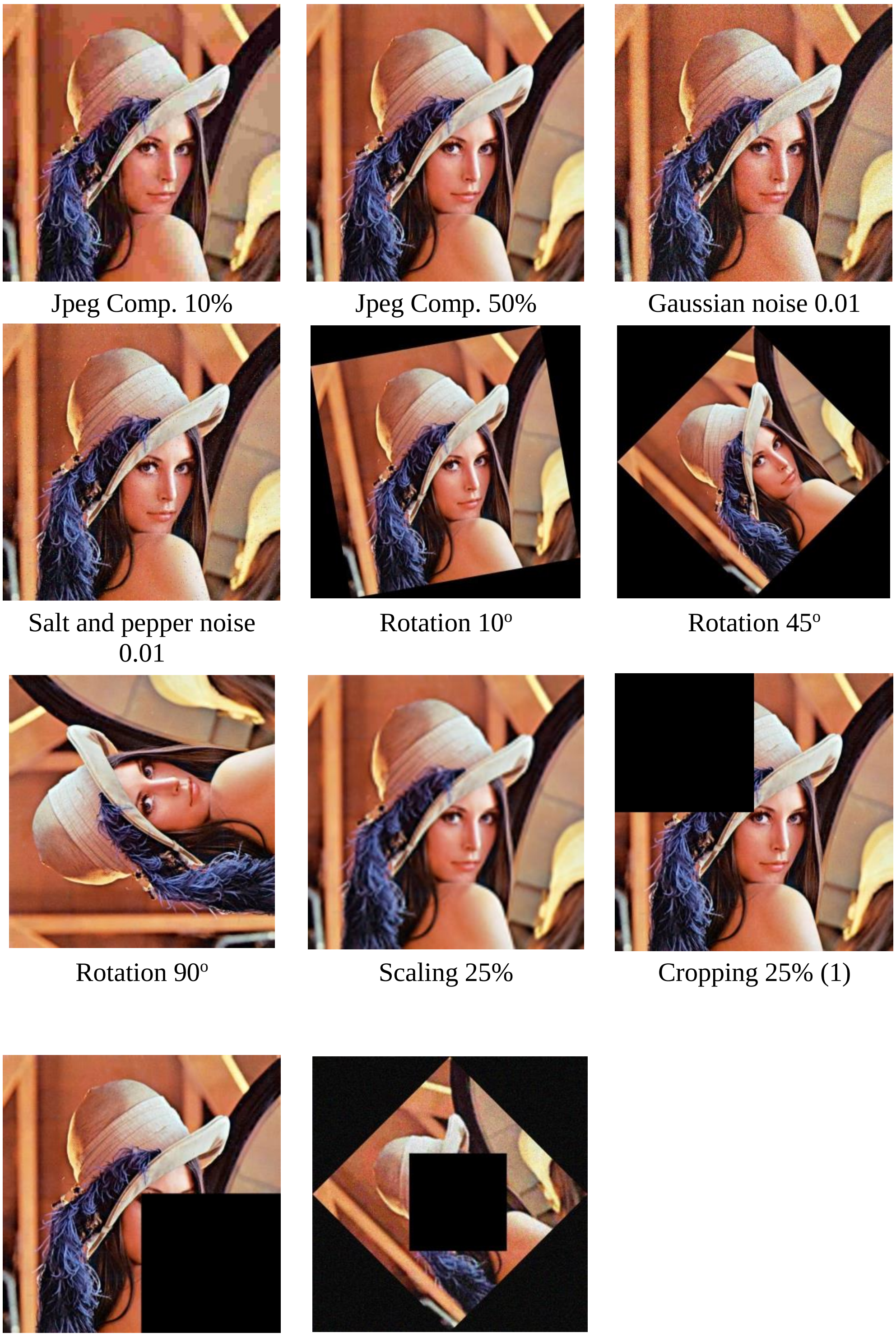
Figure 6.13: a) The extracted image, b) the watermarked image

The PSNR value of proposed method equal 81.62dB. Table 6.3 gives SSIM values of watermarking techniques for different attacks.

Table 6.3: Robustness test of proposed method III

Attacks	**SSIM**
Jpeg Comp. 10%	0.85
Jpeg Comp. 50%	0.93
Gaussian noise 0.01	0.93
Salt and pepper noise 0.01	0.94
Rotate 10^0	0.79
Rotate 45^0	0.80
Rotate 90^0	1
Scaling 25%	0.97
Cropping 25% (1)	0.82
Cropping 25% (2)	0.82
Sequential attacks	0.72
Without attack	1

In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10^{o}

Rotation 45^{o}

Rotation 90^{o}

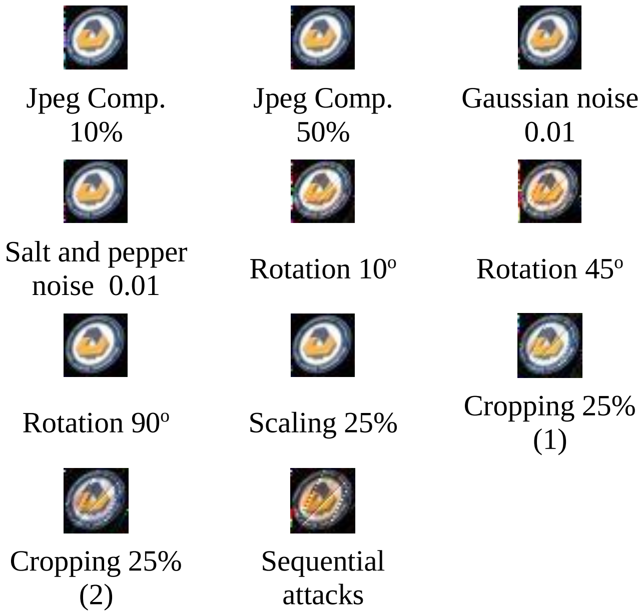
Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.14: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10°

Rotation 45°

Rotation 90°

Scaling 25%

Cropping 25% (1)

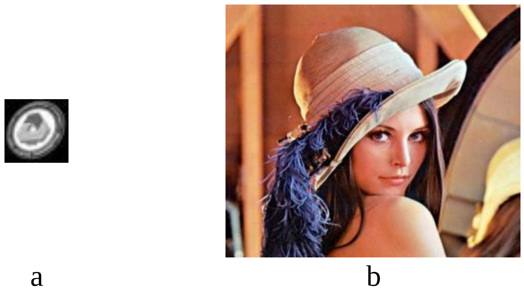
Cropping 25% (2)

Sequential attacks

Figure 6.15: The extracted watermarks

6.6 Proposed Method IV: Image Watermarking Technique in YIQ Color Space using Gray watermark image

In this method, the original image is a color Lena image (512×512) and the watermark image is a gray-scale emu-logo (32×32) as shown in Figure 6. 7. And, the watermark image is encrypted using Arnold transform with a secret key (the iteration number) equal one as shown in Figure 6.2. In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.002. After the embedding stage, the extracted image and the watermarked image are shown in following figures:



a

b

Figure 6.16: a) The extracted image, b) the watermarked image

The PSNR value of proposed method equal 107.14dB. Table 6.4 gives SSIM of watermarking techniques for different attacks.

Table 6.4: Robustness test of proposed IV

Attacks	**SSIM**
Jpeg Comp. 10%	0.96
Jpeg Comp. 50%	0.98
Gaussian noise 0.01	0.96
Salt and pepper noise 0.01	0.99
Rotate 10^0	0.76
Rotate 45^0	0.79
Rotate 90^0	0.99
Scaling 25%	0.99
Cropping 25% (1)	0.79
Cropping 25% (2)	0.71
Sequential attacks	0.70
Without attack	0.99

In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:

Jpeg Comp. 10%

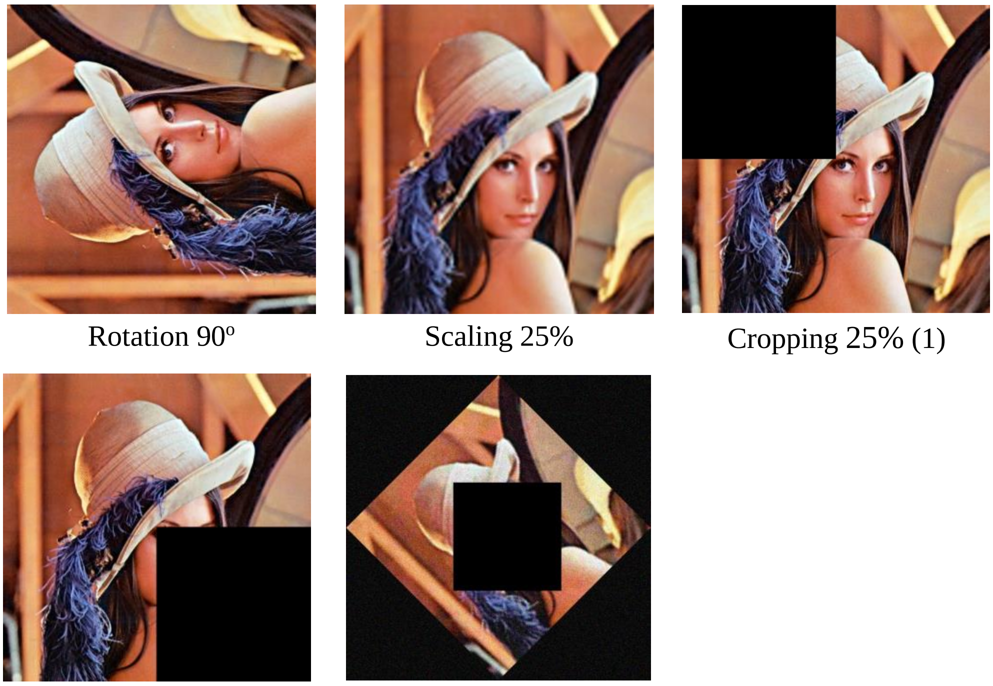
Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10^o

Rotation 45^o



Rotation 90°

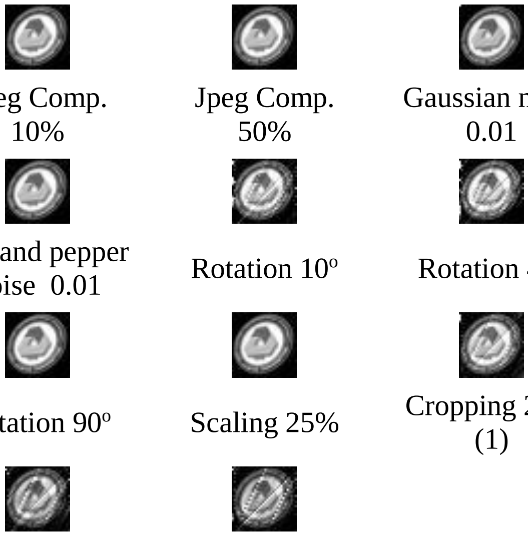
Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.17: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10°

Rotation 45°

Rotation 90°

Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.18: The extracted watermarks after the attacks

6.7 Proposed Method V: Image Watermarking Technique in YIQ Color Space using Color watermark image

In this method, the original image is a color Lena image (512×512) and the watermark image is a color emu-logo (32×32) as shown in Figure 6.11. Also, the watermark image is encrypted using Arnold transform with a secret key (the iteration number) equal one.

Figure 6.19: a) YIQ color watermark image, b) Arnold transform apply on the watermark image "iteration number=1"

In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.002. After the embedding stage, the extracted image and the watermarked image are shown in following figures:

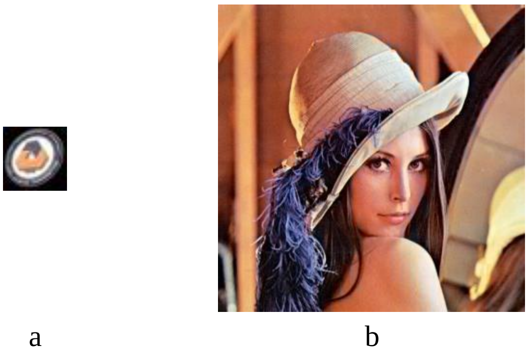


Figure 6.20: a) The extracted image, b) the watermarked image

The PSNR value of proposed method equal 78.43dB. Table 6.5 gives SSIM values of watermarking techniques for different attacks.

Table 6.5: Robustness test of proposed method V

Attacks	**SSIM**
Jpeg Comp. 10%	0.87
Jpeg Comp. 50%	0.96
Gaussian noise 0.01	0.93
Salt and pepper noise 0.01	0.97
Rotate 10^0	0.79
Rotate 45^0	0.82
Rotate 90^0	0.98
Scaling 25%	0.97
Cropping 25% (1)	0.82
Cropping 25% (2)	0.75
Sequential attacks	0.73
Without attack	0.98

In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:

Jpeg Comp. 10%

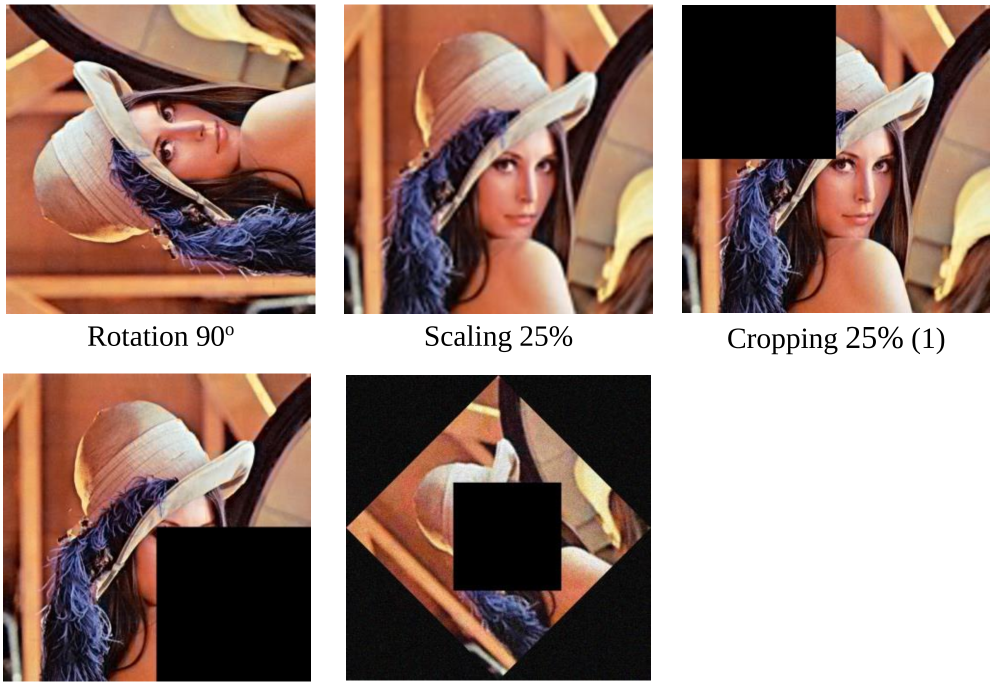
Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10^o

Rotation 45^o



Rotation 90°

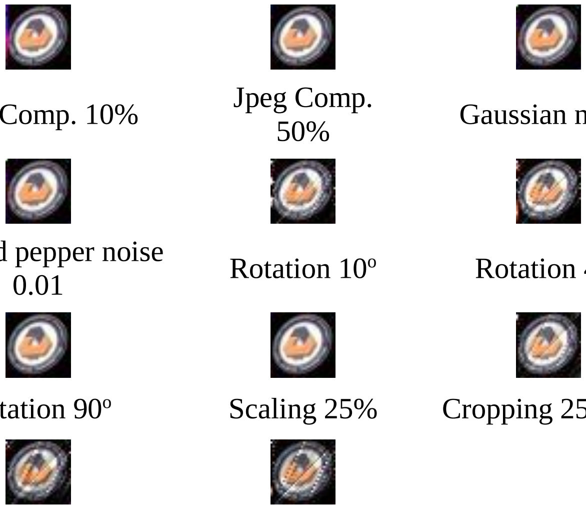
Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.21: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10°

Rotation 45°

Rotation 90°

Scaling 25%

Cropping 25% (1)

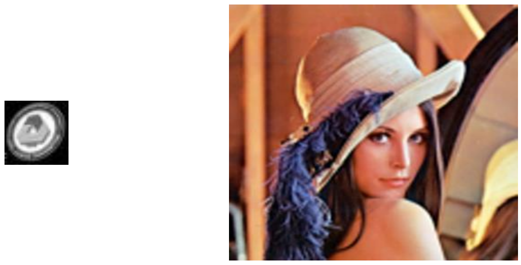
Cropping 25% (2)

Sequential attacks

Figure 6.22: The extracted watermarks after the attacks

6.8 Proposed Method VI: Image Watermarking Technique in YCbCr Color Space using Gray watermark image

In this method, the original image is a color Lena image (512×512) and the watermark image is a gray-scale emu-logo (32×32) as shown in Figure 6.7. And, the watermark image is encrypted using Arnold transform with a secret key (the iteration number) equal one as shown in Figure 6.2. In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.1. After the embedding stage, the extracted image and the watermarked are shown in following figures:



a b

Figure 6.23: a) The extracted image, b) the watermarked image

The PSNR value of proposed method equal **Inf** dB.Table 6.6 gives SSIM values of watermarking techniques for different attacks.

Table 6.6: Robustness test of proposed VI

Attacks	**SSIM**
Jpeg Comp. 10%	0.91
Jpeg Comp. 50%	0.98
Gaussian noise 0.01	0.95
Salt and pepper noise 0.01	0.95
Rotate 10^0	60.7
Rotate 45^0	0.78
Rotate 90^0	0.99
Scaling 25%	0.97
Cropping 25% (1)	0.82

Cropping 25% (2)	0.75
Sequential attacks	0.72
Without attack	0.99

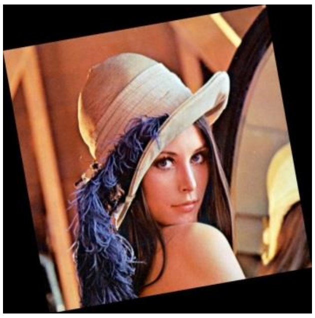
In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:

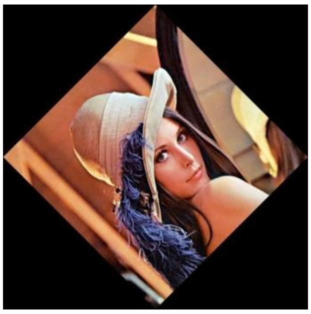
Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

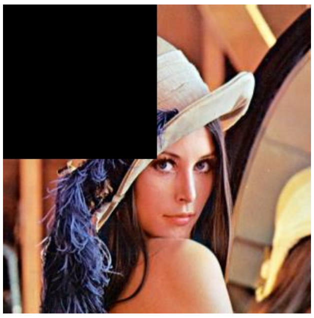
Salt and pepper noise 0.01

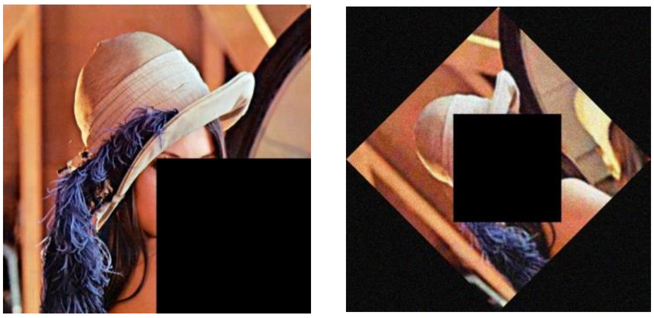

Rotation 10^{o}


Rotation 45^{o}

Rotation 90^{o}

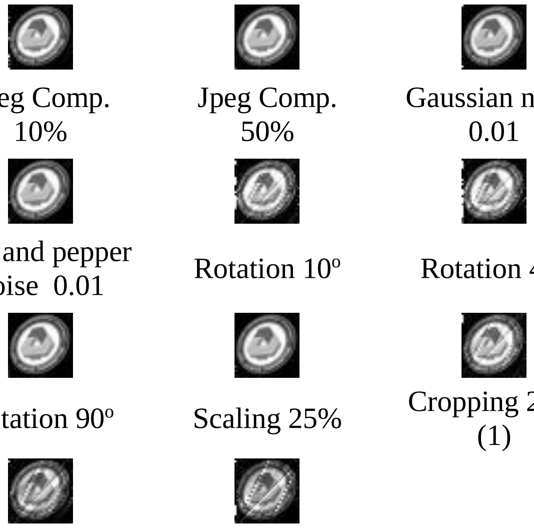
Scaling 25%


Cropping 25% (1)



Cropping 25% (2) Sequential attacks

Figure 6.24: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10°

Rotation 45°

Rotation 90°

Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.25: The extracted watermarks after the attacks

6.9 Proposed Method VII: Image Watermarking Technique in YCbCr Color Space using Color watermark image

In this method, the color Lena image of size (512×512) is taken as the original image and color emu-logo of size (32×32) is taken as a color watermark image as shown in Figure 6.11. Also, the watermark image is encrypted using Arnold transform with a secret key (the iteration number) equal one.

Figure 6.25: a) YCbCr color watermark image, b) Arnold transform apply on the watermark image "Iteration number=1"

In addition, the encrypted image is embedding into original image with strength watermark value (or the embedding coefficient) *alpha*=0.1. After the embedding stage, the extracted image and the watermarked image are shown in following figures:

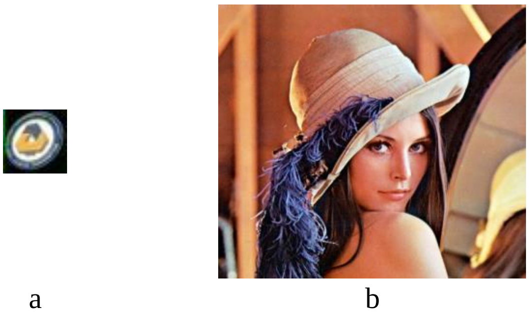


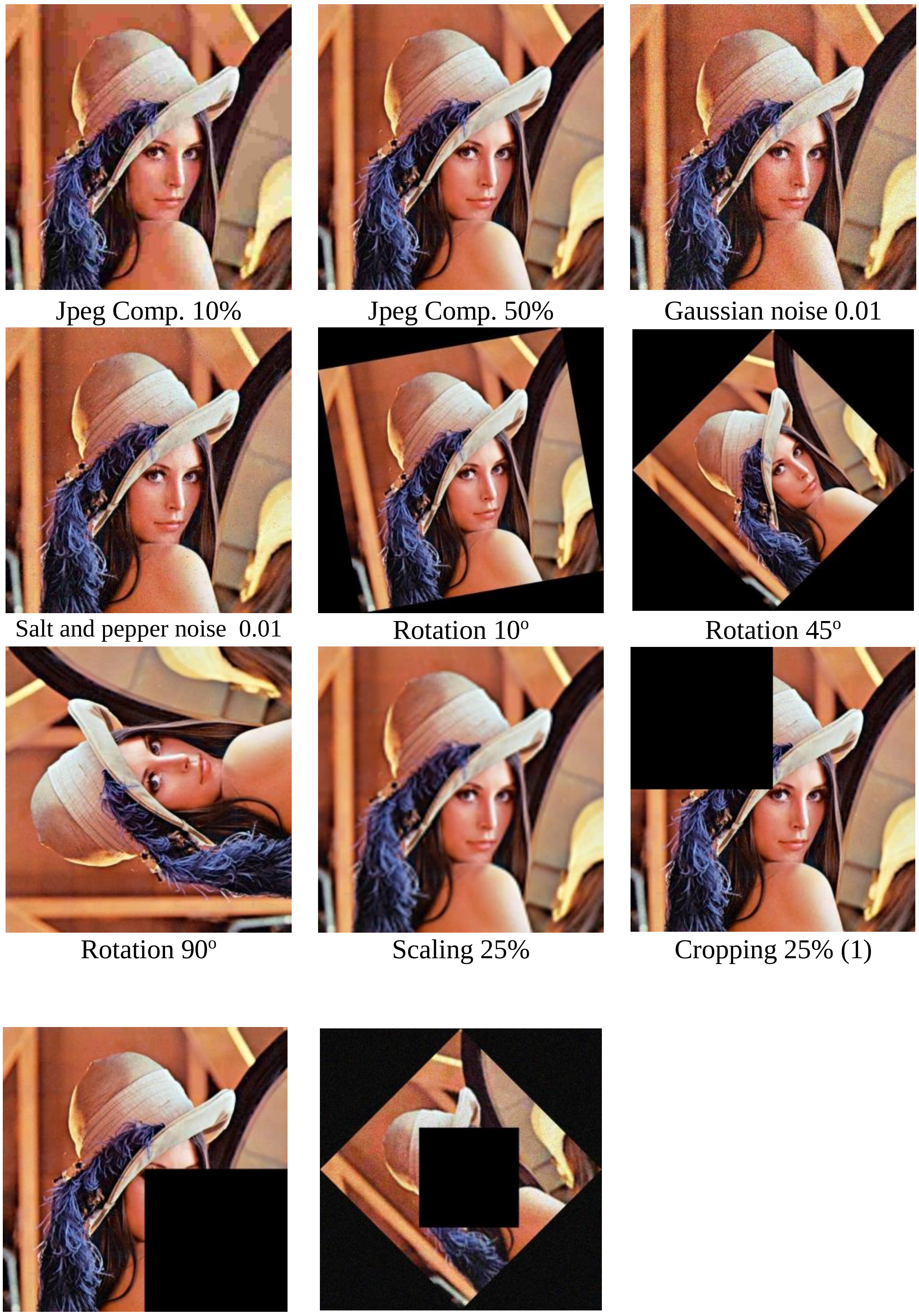
Figure 6.26: a) The extracted image, b) the watermarked image

The PSNR value of proposed method equal 63.53dB. Table 6.7 gives SSIM values of watermarking techniques for different attacks.

Table 6.7: Robustness test of proposed method VII

Attacks	**SSIM**
Jpeg Comp. 10%	0.73
Jpeg Comp. 50%	0.86
Gaussian noise 0.01	0.82
Salt and pepper noise 0.01	0.87
Rotate 10^0	0.55
Rotate 45^0	0.59
Rotate 90^0	0.92
Scaling 25%	0.90
Cropping 25% (1)	0.67
Cropping 25% (2)	0.59
Sequential attacks	0.50
Without attack	0.92

In addition, the watermarked images and extracted watermark images after these attacks are shown in following figures:



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10^{o}

Rotation 45^{o}

Rotation 90^{o}

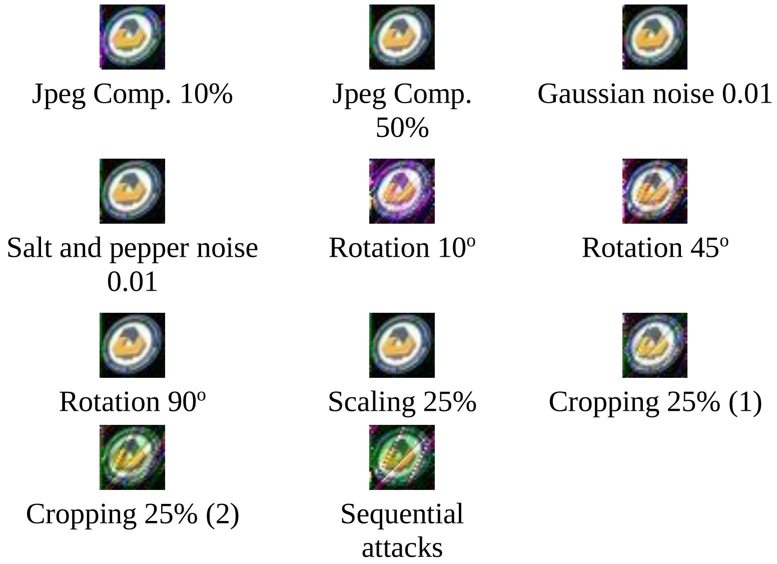
Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.27: The watermarked images after the attacks



Jpeg Comp. 10%

Jpeg Comp. 50%

Gaussian noise 0.01

Salt and pepper noise 0.01

Rotation 10º

Rotation 45º

Rotation 90º

Scaling 25%

Cropping 25% (1)

Cropping 25% (2)

Sequential attacks

Figure 6.28: a-h) The extracted watermarks after the attacks

6.10 The relation between the PSNR and the embedding coefficient

The following chart shows the relationship between the PSNR value and the embedding coefficient (*alpha*). The PSNR value between the watermarked image and the original image for gray and color image watermarking techniques.

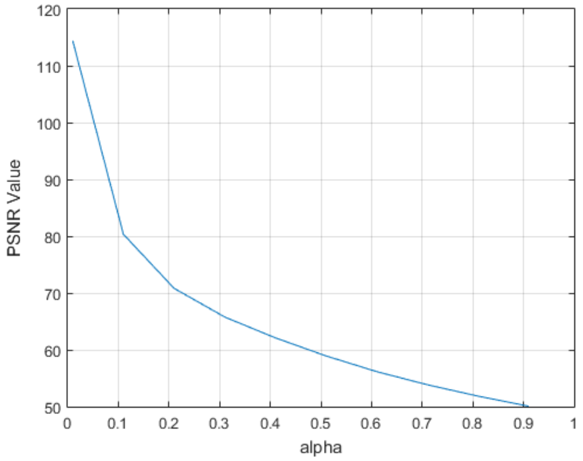
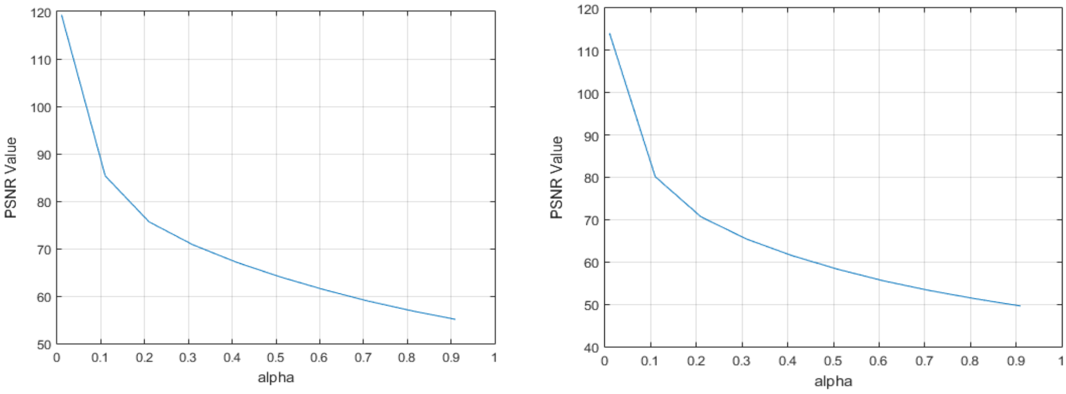
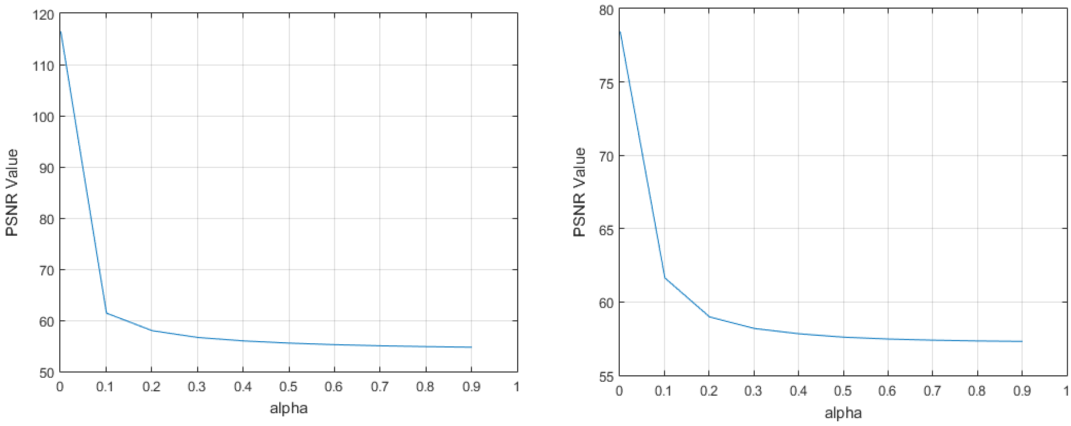


Figure 6.29: The relationship between the PSNR value and the embedding coefficient (*alpha*) (method I)



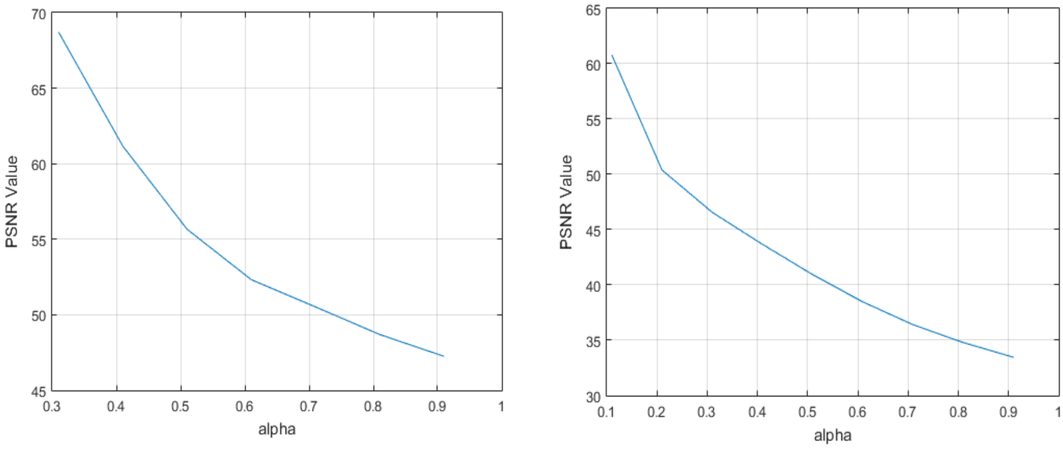
a b

Figure 6.30: a, b) The relationship between the PSNR value and the embedding coefficient (*alpha*) (method II and method III)



a b

Figure 6.31: a, b) The relationship between the PSNR value and the embedding coefficient (*alpha*) (method IV and method V)



a b

Figure 6.32: a, b) The relationship between the PSNR value and the embedding coefficient (*alpha*) (method VI and method VII)

6.11 The relation between the SSIM and the embedding coefficient

The following chart shows the relationship between the SSIM value and the embedding coefficient (*alpha*). The SSIM value is between the original watermark image and the extracted image that is extracted after one of different attacks like the compression, the noise, the scaling and the noise.

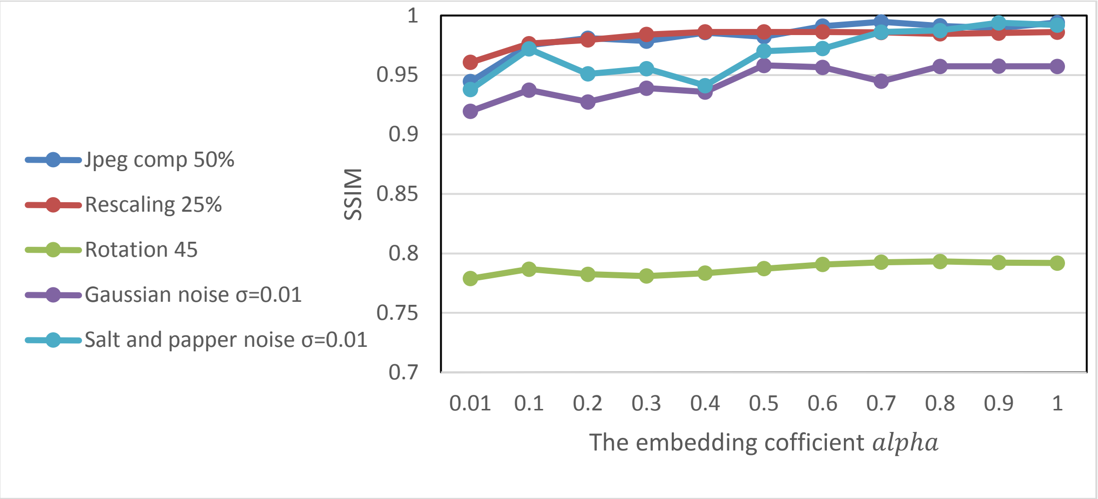
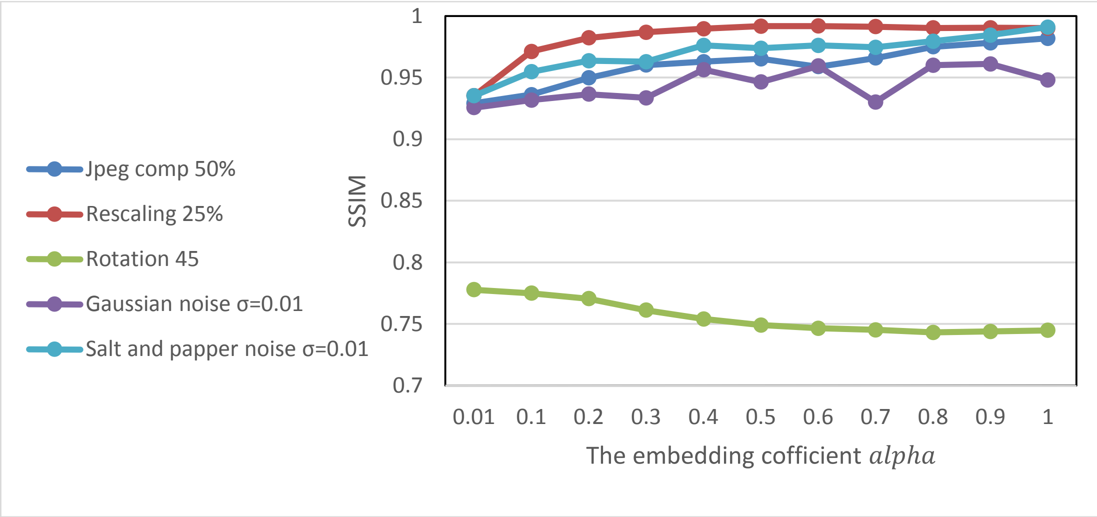
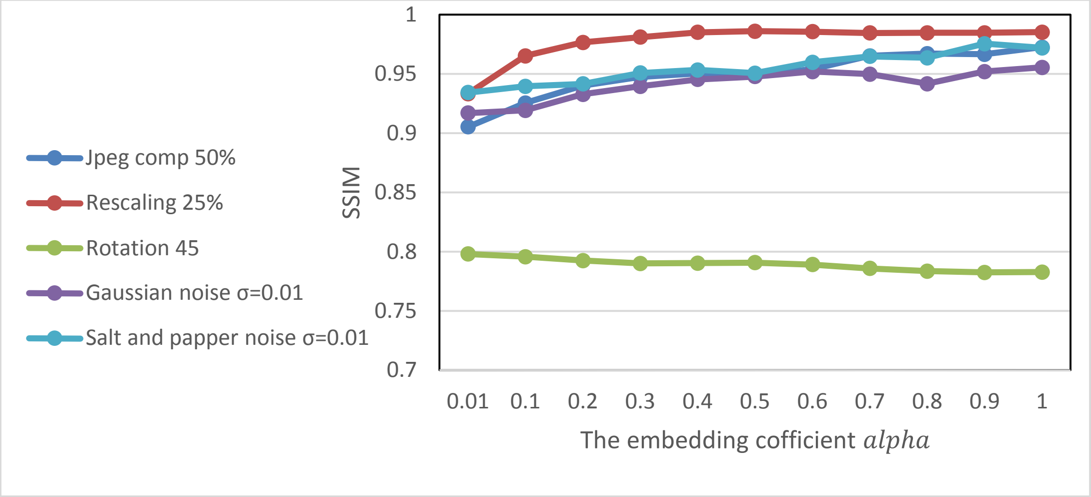


Figure 6.33: The relationship between the SSIM value and the embedding coefficient (*alpha*) (Method I)

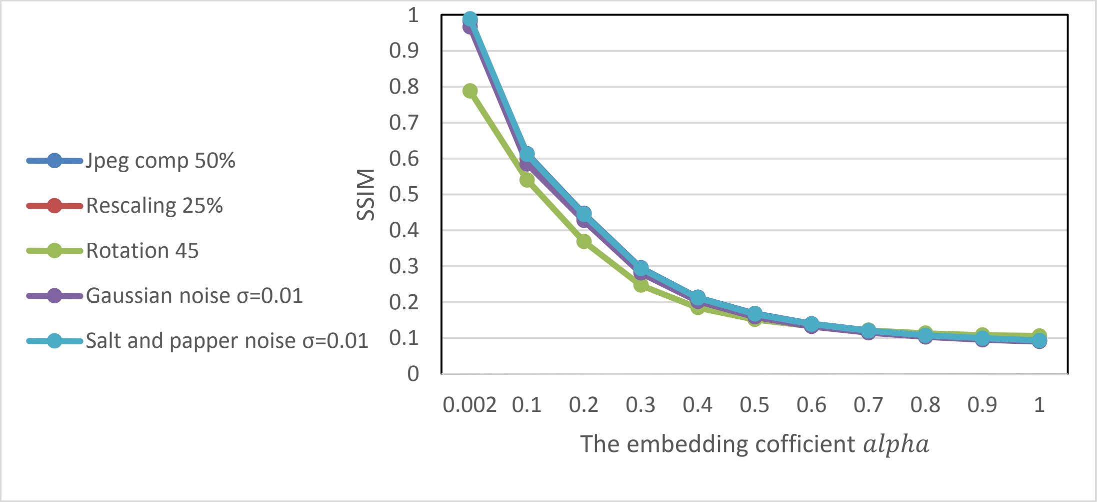


a

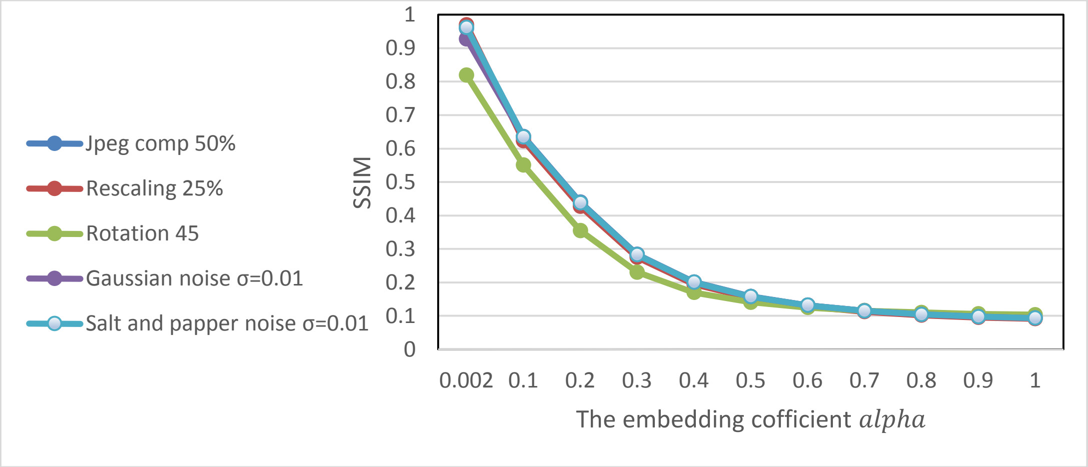


b

Figure 6.34: a, b): The relationship between the SSIM value and the embedding coefficient (*alpha*) (method II and method III)

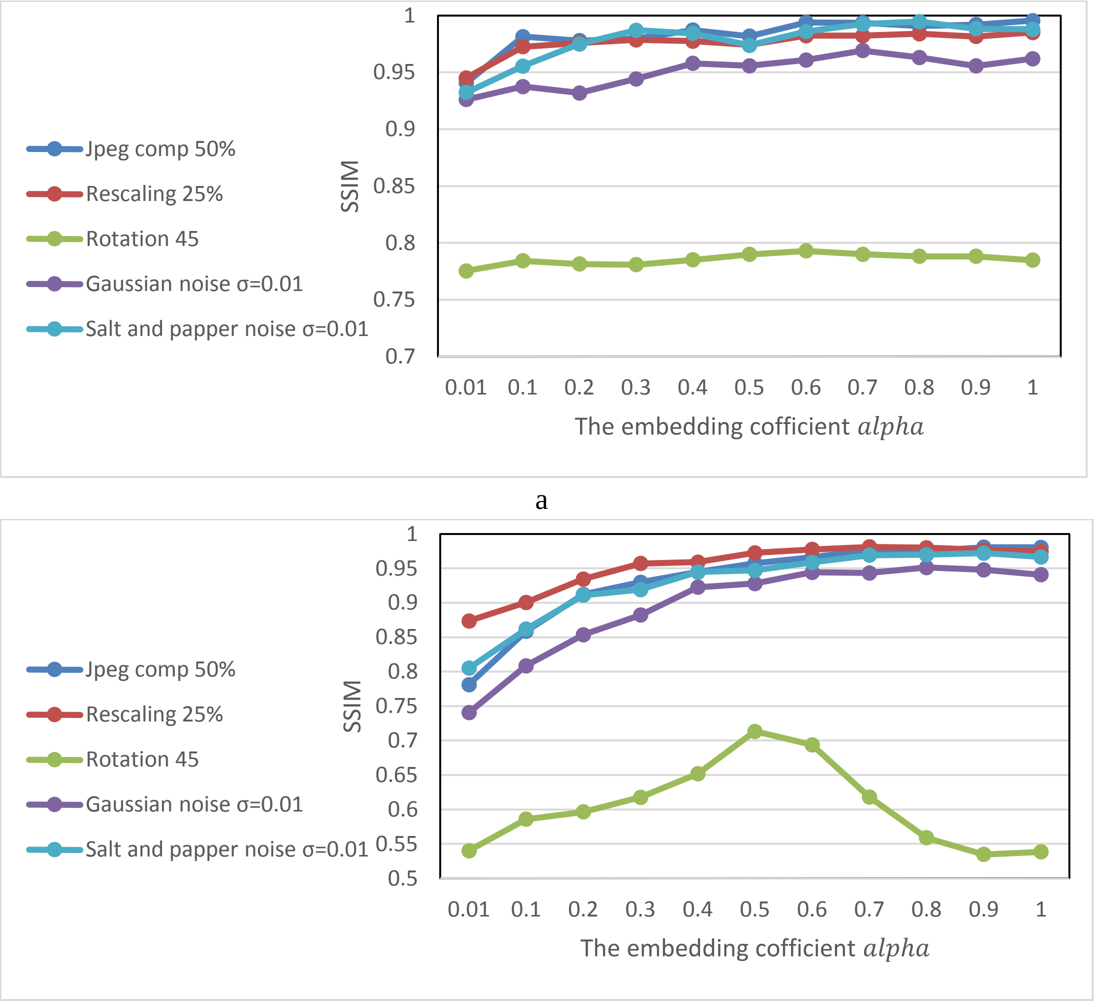


a



b

Figure 6.35: a, b): The relationship between the SSIM value and the embedding coefficient (*alpha*) (method IV and method V)



a

b

Figure 6.36 a, b): The relationship between the SSIM value and the embedding coefficient (*alpha*) (method VI and method VII)

6.12 Comparative analysis of the watermark techniques

This section analyses the robustness and imperceptibility of the watermark techniques. Where, the SSIM is calculated during different attacks to know the robustness of the watermark against the attacks. In addition, the PSNR is calculated to know imperceptibility of the watermark. In other words, the watermark must be invisible to get high PSNR value. However, when the imperceptibility is increased, the robustness will be reduced, and vice versa as the previous Figures 6.29-36. The following chart shows comparing the PSNR results between the different watermark techniques:

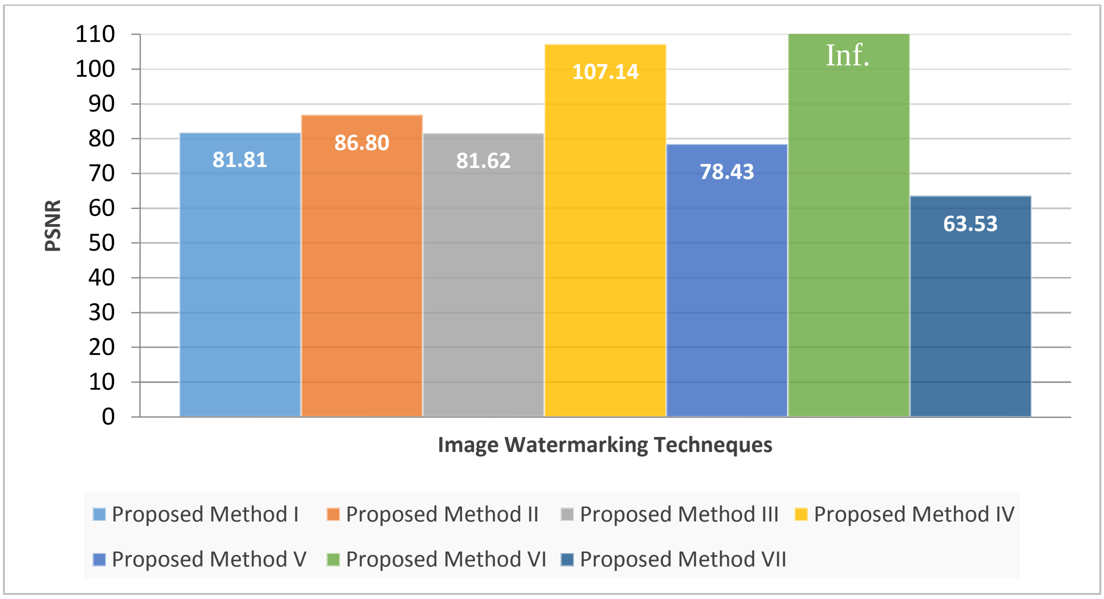


Figure 6.37 a, b): Comparing the PSNR results between the different watermark techniques

From this chart, we can see YCbCr color image watermarking technique (color watermark image) gives a least imperceptibility, but this value gives a good imperceptibility thereby gives a good watermarked image quality and this technique is less robustness against attacks as Figure 6.38. In addition, YCbCr color image watermarking technique (gray watermark image) gives best imperceptibility and good robustness ageist the attacks. The following chart shows comparing the SSIM results between the different watermark techniques:

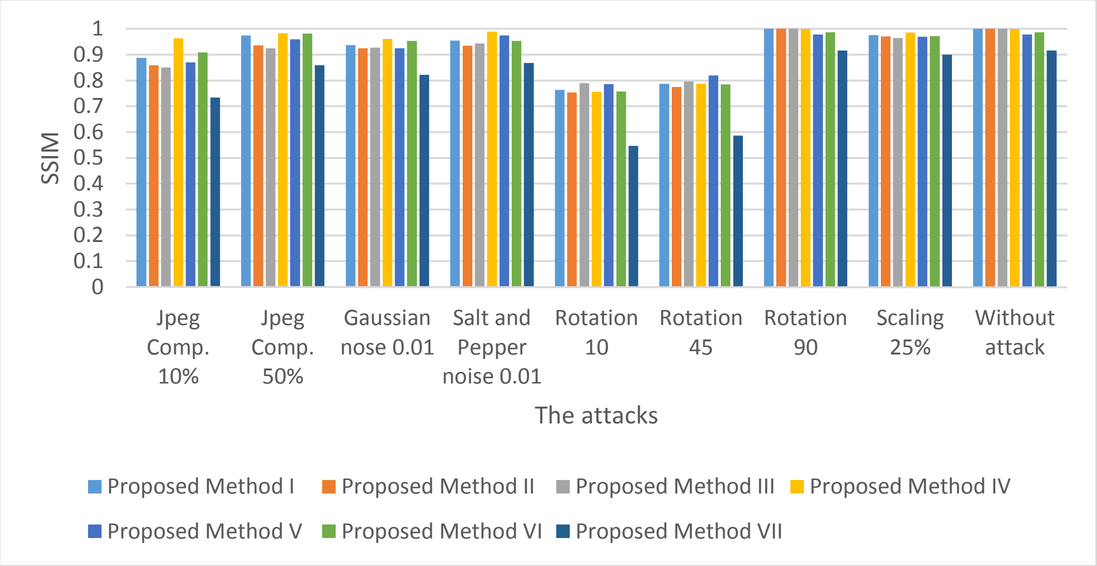


Figure 6.38 a, b): Comparing the SSIM results between the different watermark techniques

In addition, all the techniques give a good robustness against different attacks like jpeg compression, Gaussian noise, salt and pepper noise and scaling, but against the rotation attack gives less robustness. Also, the extracted watermark without attacks in gray-scale and RGB color space techniques is the same original watermark, but the extracted watermark in YIQ and YCbCr techniques is not same the original watermark because there is small error value when the image is converted from RGB color space into YIQ or YCbCr color and back again into RGB color space.

In general, these techniques give high robustness against the different attacks, high imperceptibility thereby high watermarked image quality and a security of the watermark image using encryption technique (Arnold transformation). Thus, the watermark image can be obtained only by a legitimate user.

6.13 Comparative Between Our Proposed Methods and Other Techniques

In this section, we did comparative between our proposed methods and other techniques as following:

6.13.1 The Comparative I

In this comparison, the proposed technique [method I] has been applied on gray Lena image with size (512×512) as original image and color logo image with size (64×64) as watermark image to compare with [22]. The difference between the proposed method I and [22]. In [22] can be summarized as follows: the first level DWT has been used followed by DCT blocks on horizontal sub-band (HL). In addition, it has been used sequence generation to generate 0 or 1 sequence which is embedded into image. However, in the approaches: the first level DWT has been used then DCT (8×8) blocks have been applied on diagonal sub-band (LL) followed by application of SVD on DC components.

Figure 6.39: a) Original image, b) The watermark image

Table 6.8 gives PSNR values of our proposed techniques and the other technique in [22].

Table 6.8: Comparative PSNR values of different methods

Proposed method I	**Paper[22]**
61.24	35.63

Table 6.9 gives CC values of our proposed techniques and other technique in [22] during different attacks.

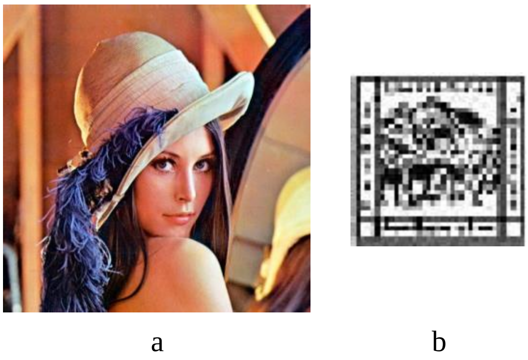
Table 6.9: Comparative CC values of different methods during attacks

Attacks	**CC**	
	Proposed method I	**Paper (22)**
Jpeg Comp 90%	**0.99**	1
Gaussian noise 0.002	**0.99**	0.99
Salt and Pepper noise 0. 1	**0.99**	0.95
Cropping (128×128)	**0.99**	0.92
Without attack	**1**	1

Through the results, the existing method has high degree of robustness against varıous attacks and low degree of imperceptibility (PSNR=35.63dB). In contrast, our proposed schemes have high degree of robustness and imperceptibility in the same time. Among the proposed approaches method I is superior.

6.13.2 The Comparative II

In this comparison, the proposed techniques [method II, method IV and method VI] have been applied on color Lena image with size (1024×1024) as original image and Gray Logo image with size (64×64) as watermark image to compare with [23]. The difference between the proposed methods (method II, method IV and method VI) and [23]. In [23] can be summarized as follows: the forth level DWT has been used followed by application of SVD horizontal sub-band (HL4). In addition, the existing method has been applied on color image in YUV color space. However, in the approaches: the first level DWT has been used then DCT (8×8) blocks have been applied on diagonal sub-band (LL) followed by application of SVD on DC components.



a b

Figure 6.40: a) Original image, b) The watermark image

Table 6.10 gives PSNR values of our proposed techniques and the other technique in [23].

Table 6.10: Comparative PSNR values of different methods

Proposed method II	**Proposed method IV**	**Proposed method VI**	**Paper[23]**
69.66	**96.23**	68.17	51.95

Table 6.11 gives CC values of our proposed techniques and other technique in [23] during different attacks.

Table 6.11: Comparative CC values of different methods during attacks

Attacks	CC			
	Proposed method II	**Proposed method IV**	**Proposed method VI**	**Paper[23]**
Jpeg Comp 30%	0.99	**0.99**	0.99	0.99
Jpeg Comp 50%	0.99	**0.99**	0.99	0.94
Jpeg Comp 60%	0.99	**0.99**	0.99	0.97
Jpeg Comp 90%	0.99	**0.99**	0.99	0.99
Rotate 20^0	0.98	**0.99**	0.98	0.92
Gaussian noise 20%	0.99	**0.99**	0.99	0.99
Gaussian noise 50%	0.96	**0.97**	0.97	0.99
Salt and Paper noise 20%	0.99	**0.99**	0.99	0.99
Without attack	1	**1**	0.99	1

Through the results, the existing method has high degree of robustness against various attacks and medium degree of imperceptibility (PSNR=51.95dB). In contrast, our proposed schemes have high degree of robustness and imperceptibility in the same time. Among the proposed approaches method IV is superior.

6.13.3 The Comparative III

In this comparison, the proposed techniques [method III, method V and method VII] have been applied on color Lena image with size (512×512) as original image and color Cat image with size (64×64) as watermark image to compare with [17]. The difference between the proposed methods (method III, method V and method VII) and [17]. In [17] can be summarized as follows: the third level DWT has been used followed by application of SVD on diagonal sub-band (LL3). In addition, the existing method [17] has been applied on color image in RGB color space. However, in the approaches: the first level DWT has been used then DCT (8×8) blocks have been applied on diagonal sub-band (LL) followed by application of SVD on DC components.

a

b

Figure 6.41: a) Original image, b) The watermark image

Table 6.11 gives PSNR values of our proposed techniques and the other technique in [17].

Table 6.11: Comparative PSNR values of different methods

Proposed method III	**Proposed method V**	**Proposed method VII**	**Paper[17]**
65.14	**80.82**	51.67	33.20

Table 6.12 gives CC values of our proposed techniques and other technique [17] during different attacks.

Table 6.112: Comparative CC values of different methods during attacks

Attacks	**CC**			
	Proposed method III	**Proposed method V**	**Proposed method VII**	**Paper [17]**
Jpeg Comp 70%	0.99	**0.99**	0.99	0.89
Gaussian noise 0.1	0.97	**0.96**	0.82	0.85
Salt and Pepper noise 0.01	0.99	**0.99**	0.91	0.91

Attacks	**CC**			
	Proposed method III	**Proposed method V**	**Proposed method VII**	**Paper [17]**
Gaussian filter 3×3	0.99	**0.99**	0.95	0.91
Gaussian filter 5×5	0.99	**0.99**	0.95	0.91
Median filter 3×3	0.99	**0.99**	0.93	0.91
Median filter 5×5	0.99	**0.99**	0.89	0.89
Mean filter 3×3	0.98	**0.98**	0.93	0.91
Mean filter 5×5	0.95	**0.96**	0.88	0.91

Through the results, the existing method has high degree of robustness against varıous attacks and low degree of imperceptibility (PSNR=33.20dB). In contrast, our proposed schemes have high degree of robustness and imperceptibility in the same time. Among the proposed approaches method V is superior.

Chapter 7

CONCLUSION

7.1 Conclusion

In this thesis, we suggest novel technique of image watermarking based on DWT, DCT and SVD in different color spaces (RGB, YIQ and YCbCr) and gray-scale image. This technique applied the DWT, DCT and SVD to make the watermarking scheme more robustness against various attacks and more imperceptibility. Therefore, we have seven proposed algorithms used this scheme. Our proposed algorithms have been applied on Lena image with size (512×512) and EMU logo with size (32×32). To test the performance of the proposed algorithms, we calculated the PSNR and SSIM. The SSIM is calculated during different attacks to know the robustness of the watermark against the various attacks. The PSNR is calculated to know the imperceptibility of the watermark. In addition, we applied the Arnold transform to ensure the watermark image. Thus, only a legitimate user can obtain the watermark image.

Through the results, the best proposed approach which gives high robustness and imperceptibility is an image watermarking technique in YIQ color space using gray watermark image. And, the worst proposed approach which gives low robustness and imperceptibility is an image watermarking technique in YCbCr color space using color watermark image.

7.2 Future Work

According to the results which were discussed in the previous chapter, we propose to improve our proposed algorithms to give high robustness against the rotation attack and apply other encryption methods like hashing, symmetric methods and asymmetric methods to give security. In addition, we propose to embed other digital signal like audio into the image using the same scheme.

REFERENCES

[1] Santhi, V., Rekha, N., & Tharini, S. (2008, December). A hybrid block based watermarking algorithm using DWT-DCT-SVD techniques for color images. In *Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on* (pp. 1-7). IEEE.

[2] Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography*. Morgan Kaufmann.

[3] Jain, A. K. (1989). *Fundamentals of digital image processing*. Prentice-Hall, Inc.

[4] Seitz, J. (2005). *Digital watermarking for digital media*. IGI Global.

[5] Abdullatif, M., Zeki, A. M., Chebil, J., & Gunawan, T. S. (2013, March). Properties of digital image watermarking. In *Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on* (pp. 235-240). IEEE.

[6] *RGB_color_model*, retrived on December, 2015, from:
https://en.wikipedia.org/wiki/RGB_color_model

[7] *Color_Models:_RGB,_HSV,_HSL*, retrived on December, 2015, from:
https://en.wikibooks.org/wiki/Color_Models:_RGB,_HSV,_HSL

[8] *YIQ*, retrived on December, 2015, from:

https://en.wikipedia.org/wiki/YIQ

[9] *YCbCr*, retrived on December, 2015, from:
https://en.wikipedia.org/wiki/YCbCr

[10] Santhi, V., & Thangavelu, A. (2011). DC Coefficients Based Watermarking Techniquefor color Images Using Singular ValueDecomposition. *International Journal of Computer and Electrical Engineering*, *3*(1), 8.

[11] Gunjal, B. L., & Mali, S. N. (2011). Comparative performance analysis of DWT-SVD based color image watermarking technique in YUV, RGB and YIQ color spaces. *International Journal of Computer Theory and Engineering*, *3*(6), 714.

[12] Gunjal, B. L., & Mali, S. N. (2011). Secured color image watermarking technique in DWT-DCT domain. *arXiv preprint arXiv:*1109.2325.

[13] Pennebake, W. Still Image Data Compression Standard.

[14] Jadav, R. A., & Patel, S. S. (2010). Application of singular value decomposition in image processing. *Indian Journal of Science and Technology*, *3*(2), 148-150.

[15] Choras, R. S. *Image Processing & Communications Challenges 2*, springer berlin heidelberg, 2010.

[16] Hui-qin, W., Ji-chao, H., & Fu-ming, C. (2010, April). Colour Image Watermarking Algorithm Based on the Arnold Transform. In *Communications and Mobile Computing (CMC), 2010 International Conference on* (Vol. 1, pp. 66-69). IEEE.

[17] George, J., Varma, S., & Chatterjee, M. (2014, December). Color image watermarking using DWT-SVD and Arnold transform. In *India Conference (INDICON), 2014 Annual IEEE* (pp. 1-6). IEEE.

[18] Zhang, Y., Wang, J., & Chen, X. (2012, May). Watermarking technique based on wavelet transform for color images. In *Control and Decision Conference (CCDC), 2012 24th Chinese* (pp. 1909-1913). IEEE.

[19] Boora, M., & Gambhir, M. Arnold Transform Based Steganography.

[20] Zhang, Y., Wang, J., & Chen, X. (2012, May). Watermarking technique based on wavelet transform for color images. In *Control and Decision Conference (CCDC), 2012 24th Chinese* (pp. 1909-1913). IEEE.

[21] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *Image Processing, IEEE Transactions on*, *13*(4), 600-612.

[22] Deb, K., Al-Seraj, M. S., Hoque, M. M., & Sarkar, M. I. H. (2012, December). Combined DWT-DCT based digital image watermarking technique for

copyright protection. In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on* (pp. 458-461). IEEE.

[23] Roy, A., Maiti, A. K., & Ghosh, K. (2015, February). A perception based color image adaptive watermarking scheme in YCbCr space. In *Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on* (pp. 537-543). IEEE.