Robust Watermarking Schemes for Digital Images

Abdallah Muneer Elayan

A Thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of Master of Applied Science at

Concordia University

Montreal, Quebec, Canada

December 2013

CONCORDIA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: Abdallah Muneer Elayan

Entitled: Robust Watermarking Schemes for Digital Images

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science

Complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair

Dr. Kabir M. Zahangir

_____ Examiner, External-to-Program

Dr. Terry Fancott

_____ Examiner

Dr. M.N.S. Swamy

_____ Supervisor

Dr. M. Omair Ahmad

Approved by: _____

Dr. W. E. Lynch, Chair

Department of Electrical and Computer Engineering

_____20____ _____

Dr. Christopher W. Trueman

Dean, Faculty of Engineering and Computer Science

Abstract

Robust Watermarking Schemes for Digital Images

Abdallah M. Elayan

Concordia University, 2013

With the rapid development of multimedia and the widespread distribution of digital data over the internet networks, it has become easy to obtain the intellectual properties. Consequently, the multimedia owners need more than ever before to protect their data and to prevent their unauthorized use. Digital watermarking has been proposed as an effective method for copyright protection and an unauthorized manipulation of the multimedia. Watermarking refers to the process of embedding an identification code or some other information called watermark into digital multimedia without affecting the visual quality of the host multimedia. Such a watermark can be used for several purposes including copyright protection and fingerprinting of the multimedia for tracing and data authentication.

The goal in a watermarking scheme is to embed a watermark that is robust against various types of attacks while preserving the perceptual quality of the cover image. A variety of schemes have been proposed in the literature to achieve these goals for watermarking of images. These schemes either provide good imperceptibility of the watermark without sufficient resilience to certain types of attacks or provide good robustness against attacks at the expense of degraded perceptual quality of the cover images. The objective of this

work is to develop image watermarking schemes with performance that is superior to those of existing schemes in terms of their robustness against various types of attacks while preserving the perceptual of the cover image. In this thesis, two new digital image watermarking schemes are proposed.

In the first scheme, an Arnold transform integrated DCT-SVD based image watermarking scheme is developed. The main idea in this scheme is to improve the robustness of the watermarking further by scrambling the watermark data using the Arnold transform while still preserving the good perceptibility of the watermarked image furnished by a DCT-SVD based embedding. Also, it is shown that considerable savings in the computation time to recover the original watermark image can be provided by using the anti-Arnold transform in the watermark extraction process.

In the second scheme, a DWT-SVD digital image watermarking scheme that makes use of visual cryptography to embed and extract a binary watermark image is developed. The use of visual cryptography in the proposed watermarking scheme is intended to provide improved robustness against attacks along with furnishing security to the content of the embedded data.

Extensive experiments are conducted throughout this investigation in order to examine the performance of the proposed watermarking schemes. It is shown that the two proposed watermarking schemes developed in this thesis provide a performance superior to that of the existing schemes in terms of robustness against various types of attacks while preserving the perceptual quality of the cover image.

Acknowledgments

I would like to take this opportunity to express my deep gratitude to my supervisor, Professor M. Omair Ahmed, for his constant support, encouragement, patience, and invaluable guidance during this research. I am grateful to him for spending many hours with me in correcting and improving the writing of this thesis. The useful suggestions provided by the committee members are also deeply appreciated.

My sincere and heartfelt thanks go to my mother, my aunt, my brothers, Ahmed, Mohammad and Elayan, and to my sisters, Duaa, Muna, Sumaia, Nansy and Sereen for their support and encouragement during the course of this research. Special thanks are also due to my friends.

To my Mother and Late Father

Table of Contents

List of Figures ……ix

List of Tables……xiii

List of Abbreviations……xiv

List of Acronyms……xv

1. Introduction……1

1.1 Importance of Digital Watermarking……1

1.2 Literature Review and Motivation ……3

1.3 Scope of the Thesis……8

1.4 Organization of the Thesis ……9

2. Background Material……11

2.1 General Watermarking Scheme ……11

2.2 Classification of Watermarking Schemes ……13

2.3 Desired Features of Watermarking ……16

2.4 A Review of Transforms Commonly used in Watermarking ……18

2.4.1 Singular value decomposition (SVD) ……18

2.4.2 Discrete cosine transform (DCT)……21

2.4.3 Discrete wavelet transform (DWT) ……23

2.5 Summary……25

3. An Arnold Transform integrated DCT-SVD Based Digital Watermarking Scheme……26

3.1 Introduction……26

3.2 Image Scrambling ……27

3.3 Proposed Watermarking Algorithm ……31

3.3.1 Watermark embedding ……33

3.3.2 Watermark extraction ……36

3.4 Experimental Results and Discussion ……38
3.5 Summary……52
4. Visual Cryptography Based Digital Watermarking Scheme……54
4.1 Introduction……54
4.2 Visual Cryptography ……56
4.3 Proposed Watermarking Algorithm ……58
4.3.1 Watermark embedding ……58
4.3.2 Watermark extraction ……60
4.4 Experimental Results and Discussion ……63
4.5 Summary……77
5. Conclusion……78
5.1 Concluding Remarks ……78
5.2 Scope for Further Research ……80
6. References……81

List of Figures

Figure 2.1: A general block diagram for image watermarking…… 12

Figure 2.2: Lena image and its singular value matrix…… 19

Figure 2.3: Lena image with salt & peppers noise attack and the singular value matrix…… 20

Figure 2.4: Wavelet sub-bands with 1-level decomposition of a 1-dimensional signal…… 24

Figure 2.5: Illustration of 2-dimensional DWT for an image…… 24

Figure 2.6: Wavelet sub-bands with 2-level decomposition of a 2-dimensional signal…… 25

Figure 3.1: (a) Peppers image of size128×128. (b) Scrambled image after $n = 5$ iterations of the operation of the Arnold transform. (c) The reconstructed image after $n = T_{128} = 96$ iterations of the Arnold transform…… 29

Figure 3.2: (a) Boat image. (b) Scrambled image after $n = 15$ iterations of the operation of the Arnold transform. (c) The recovered image after $n = 15$ iterations of the operation of the anti- Arnold transform on the scrambled image of Figure 3.2(b)…… 31

Figure 3.3: Time needed to recover the original image from a scrambled image by using the Arnold and anti-Arnold transforms. The scrambled images have been obtained by applying 20 iterations of the Arnold transform on the original images…… 32

Figure 3.4: Block diagram of the proposed watermark embedding scheme…… 34

Figure 3.5: (a) Zig-zag scanning of the 2D- discrete cosine transform coefficients.(b) Mapping of the scanned DCT coefficients into four subbands…… 35

Figure 3.6: Block diagram of the proposed watermark extraction scheme..... 37

Figure 3.7: Cover images: (a) *Lena*, (b) *Pirate*, and (c) *Couple*. Watermark images: (d) *Boat,* (e) *Peppers*, and (f) *Cameraman*..... 39

Figure 3.8: (a) Cover image, *Lena*. (b) Watermark image, *Boat*. (c) Watermarked image. (d) Watermark images extracted from the each of the four subbands of the watermarked image..... 40

Figure 3.9: (a) Original cover image, *Lena*. (b) Original watermark image, *Boat*..... 43

Figure 3.10: (a) Watermarked *Lena* image attacked by JPEG compression. (b) Extracted watermark image..... 43

Figure 3.11: (a) Watermarked *Lena* image attacked by Gaussian noise. (b) Extracted watermark image..... 43

Figure 3.12: (a) Watermarked *Lena* image attacked by cropping. (b) Extracted watermark image..... 44

Figure 3.13: (a) Watermarked *Lena* image attacked by re-scaling. (b) Extracted watermark image..... 44

Figure 3.14: (a) Watermarked *Lena* image attacked by translation. (b) Extracted watermark image..... 44

Figure 3.15: (a) Watermarked *Lena* image attacked by rotation. (b) Extracted watermark image..... 45

Figure 3.16: (a) Watermarked *Lena* image attacked by darkening. (b) Extracted watermark image..... 45

Figure 3.17: (a) Watermarked *Lena* image attacked by brightening. (b) Extracted watermark image..... 45

Figure 3.18: (a) Watermarked *Lena* image attacked by sharpening. (b) Extracted watermark image..... 46

Figure 3.19: (a) Watermarked *Lena* image attacked by blurring. (b) Extracted watermark image..... 46

Figure 3.20: (a) Watermarked *Lena* image attacked by contrast adjustment. (b) Extracted watermark image..... 46

Figure 3.21: (a) Watermarked *Lena* image attacked by gamma correction. (b) Extracted watermark image..... 47

Figure 3.22: (a) Watermarked *Lena* image attacked by median filtering. (b) Extracted watermark image..... 47

Figure 3.23: (a) Watermarked *Lena* image attacked by histogram equalization. (b) Extracted watermark image..... 47

Figure 4.1: The basic scheme of Naor and Shamir [53] for visual cryptography. (a) Encryption and decryption. (b) Codebook..... 57

Figure 4.2: Block diagram of the proposed watermark embedding scheme..... 59

Figure 4.3: Block diagram of the proposed watermark extraction scheme..... 61

Figure 4.4: Cover images: (a) *Pirate*, (b) *Boat*, and (c) *Elaine*. (d) Watermark image..... 63

Figure 4.5: (a) Cover image, *Pirate*. (b) Watermark image. (c) Watermarked image. (d) Watermark images extracted from the LH and HL subbands of the watermarked image..... 64

Figure 4.6: (a) Original cover image, Pirate. (b) Original watermark image..... 66

Figure 4.7: (a) Watermarked Pirate image attacked by JPEG compression (Q=10). (b) Extracted watermark image..... 67

Figure 4.8: (a) Watermarked Pirate image attacked by JPEG compression (Q = 5). (b) Extracted watermark image..... 67

Figure 4.9: (a) Watermarked Pirate image attacked by cropping (left and right sides by 25 columns each). (b) Extracted watermark image..... 67

Figure 4.10: (a) Watermarked Pirate image attacked by translation (horizontally and vertically by 40 lines each). (b) Extracted watermark image……... 68

Figure 4.11: (a) Watermarked Pirate image attacked by darkening (70%). (b) Extracted watermark image……... 68

Figure 4.12: (a) Watermarked Pirate image attacked by Brightening (70%). (b) Extracted watermark image……... 68

Figure 4.13: (a) Watermarked *Pirate* image attacked by Gaussian noise contamination (σ^2 = 0.3). (b) Extracted watermark image…… 69

Figure 4.14: (a) Watermarked *Pirate* image attacked by gamma correction (γ = 0.6). (b) Extracted watermark image…… 69

Figure 4.15: (a) Watermarked *Pirate* image attacked by re-scaling (512-256-512). (b) Extracted watermark image……... 69

Figure 4.16: (a) Watermarked *Pirate* image attacked by rotation (25°). (b) Extracted watermark image……... 70

Figure 4.17: (a) Watermarked *Pirate* image attacked by rotation (rotated by 5° and restored to the original size). (b) Extracted watermark image…… 70

Figure 4.18: (a) Watermarked *Pirate* image attacked by blurring using 3×3 Gaussian filter with σ = 1. (b) Extracted watermark image…… 70

Figure 4.19: (a) Watermarked *Pirate* image attacked by median filtering (3×3). (b) Extracted watermark image……... 71

Figure 4.20: (a) Watermarked *Pirate* image attacked by histogram equalization. (b) Extracted watermark image……... 71

Figure 4.21: (a) Watermarked *Pirate* image attacked by contrast adjustment (decreased by 60%). (b) Extracted watermark image……... 71

Figure 4.22: Watermarked and attacked watermarked *Pirate* images using (a) Scheme 1 and (b) Scheme 2…… 76

List of Tables

Table 2.1: Classifications of the watermarking techniques..... 15

Table 3.1: The periods of Arnold transformation for different values of N 29

Table 3.2: The PSNR values (in dB) of various watermarked images obtained by using the proposed watermarking scheme..... 41

Table 3.3: Values of the correlation coefficient between the extracted and original watermark images..... 49

Table 3.4: Values of the correlation coefficient between the extracted and original watermark images..... 50

Table 3.5: Performance, in terms of PSNR and normalized correlation coefficient, of the proposed and two other watermarking schemes against various types of attacks..... 51

Table 3.6: Execution times of running the proposed and two other watermarking schemes..... 52

Table 4.1: The PSNR values (in dB) of various watermarked images obtained by using the proposed watermarking scheme..... 65

Table 4.2: Values of the correlation coefficient between the extracted and original watermark images..... 72

Table 4.3: Performance, in terms of normalized correlation coefficient, of the proposed and three other watermarking schemes against various types of attacks..... 74

Table 4.4: Performance comparison of the two proposed watermarking schemes, in terms of normalized correlation coefficient, against various types of attacks..... 75

List of Abbreviations

1D	One dimensional
2D	Two dimensional
DCT	Discrete cosine transform
IDCT	Inverse discrete cosine transform
DWT	Discrete wavelet transform
IDWT	Inverse discrete wavelet transform
DFT	Discrete fourier transform
SVD	Singular value decomposition
VC	Visual cryptography
PSNR	Peak signal-to-noise ratio
NC	Normalized correlation
MSE	Mean squared error
LL	Low-low
LH	Low-high
HL	High-low
HH	High-high
HVS	Human visual system
SDM	Sampling distribution of means

List of Acronyms

S	Singular value matrix
U	Left singular matrix
V	Right singular matrix
$\lambda_{i,j}$	Elements of singular value matrix
W	Original watermark image
W^*	Extracted watermark image
α	Scaling factor
T_N	Period of the Arnold transform
r	Number of iterations
C	Cover image
C_w	Watermarked image
$C_{i,j}$	Pixel value in original cover image
$C'_{i,j}$	Pixel value in watermarked image
M×M	Size of the cover image
N×N	Size of watermark image
μ	Mean value
$\oplus$	Exclusive-OR operation

Chapter 1

Introduction

The explosion of the digital multimedia is one of the greatest technology events of the last two decades. Unlike the analog media, digital media can be stored efficiently and transmitted in a fast and inexpensive way through communication networks. Furthermore, digital data can be manipulated easily using computers. With the rapid development of multimedia and the widespread distribution of digital data over the internet networks, it has become easy to obtain the intellectual properties. Consequently, the multimedia owners need more than ever before to protect their data and to prevent the unauthorized use of their data. The design of new techniques for protecting the ownership of digital information is key to future development of data services.

1.1 Importance of Digital Watermarking

There are a number of techniques that exist for protecting ownership of multimedia. Traditionally encryption and access control techniques have been used for ownership protection; but these techniques do not protect the ownership of the data after the

multimedia have been received and decrypted successfully [1]. A subsequent technique to protect the ownership rights is watermarking. Watermarking is a technique for hiding the owner's information in the multimedia to provide a proof of ownership. Watermarking provides a solution for copyright protection and an unauthorized manipulation of the multimedia. In general, embedding of the watermark and its detection process can be described as follows. The owner of the original data embeds a secret watermark into the original data to produce a watermarked data. The owner keeps the original data and the original watermark hidden and publishes the watermarked data. A hacker (an unauthorized party) takes a copy of the watermarked data and modifies it and starts publishing the hacked data as his/ her own data. The actual owner of the original data takes a copy of the hacked data and extracts the embedded watermark, then he checks the similarity between the extracted and the original watermarks. If the similarity is found to be high, this will give a clear proof that the attacked data were taken from the originally watermarked data.

Watermarking can be found in a wide variety of applications [1], and may be classified as follows:

(a) Unauthorized copying of multimedia*:* In multimedia distribution systems banning the unauthorized copying of the data is one of the most important features. The embedded watermark in the multimedia protects unauthorized copying of the multimedia. In this case the watermark detector in the copying device verifies if the copying of the multimedia is legal or not.

(b) Fingerprinting of the multimedia for tracing*:* To trace the illegal copying of the original data, the fingerprinting is used. The owner of the original data embeds a unique watermark that identifies the customer receiving the data. Any copy made of the watermarked data by the customer will be also watermarked; this enables the owner of the original data to identify customer who has broken his/her license agreement by illegal copying of the data. The watermark used in fingerprinting applications should be robust against general processing attacks.

(c) Copyright protection*:* Copyright protection has become extremely important because of the increase in the volumes of distribution and circulation of multimedia products over the internet. Copyright protection of these products is one of the most important applications of the watermarking schemes.

(d) Image authentication*:* In authentication application, any changes in the content should be detected in order to validate the content and ensure its integrity. Fragile watermarks having low robustness are used in these applications, since the purpose of the watermark is not to protect the content, but to authenticate it.

(e) Content description*:* The embedded watermark can be used to provide more information about the host image.

1.2 Literature Review and Motivation

Since digital data can easily be transported and distributed over internet, development of multimedia products has surged tremendously. At the same time, use of digital technology has allowed the alteration and manipulation of these products to become much easier. Thus, copyright protection of multimedia products has now become more of an important

issue than ever before. The objective of watermarking is to provide such a protection. The goal in a watermarking scheme is to embed a watermark that is robust against attacks and difficult to notice while maintaining the original quality of the multimedia.

A variety of schemes have been proposed to achieve these goals for watermarking of images. Based on the embedding domain, these schemes can be categorized into two groups [1, 2], spatial domain schemes and transform domain schemes. The simplest and earliest watermarking techniques are the spatial domain methods, where the watermarks can be embedded by modifying the pixel values. As an example of a watermarking scheme in this class, the authors in [3] have proposed a watermarking algorithm, in which the watermark is embedded by modifying the pixel values of a blue channel in a colored image, and the watermark detection was done by comparing the neighboring pixels. The limitation of this scheme is that it is not robust against blurring attack and as the compression ratio increases the robustness tends to decrease. In [4], a watermarking scheme for digital images has been proposed, where the cover image is divided into blocks having the same size as that of the watermark. The watermark was added into each of the blocks. However, this scheme is not robust enough for general processing, such as noisy transmission, filtering and cropping. In general, the spatial domain schemes lack the robustness against lossy compression attack and have low-information hiding capacity.

On the other hand, a more robust watermarking can be achieved by embedding the watermark into the transform coefficients of the host multimedia. Typical transform methods used are discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD) [5-11].

In recent years, most of the watermarking schemes have used the transform domain technique to embed watermarks. In [12], the authors have proposed a DCT based watermarking algorithm, in which the watermark is embedded in the n largest magnitude coefficients of the DCT-transformed cover image. The watermark consists of normally-distributed coefficients with zero mean and unit variance. However, the modification of these coefficients of the DCT transformed image can lead to perceptual degradation. In [13], authors have proposed a watermarking scheme based DCT. The watermark is embedded in the low-frequency coefficients, then, the watermarked image is adjusted by a mechanism called weighted correction, to improve the imperceptibility. This technique performs well under JPEG compression. However, when the watermarked images are compressed with a high compression ratio, the embedded watermarks may be affected seriously. Another DCT-based watermarking scheme was proposed by Deng and Wang in [14], where the cover image is divided into 8×8 blocks and a binary watermark is scrambled using a linear feedback shift register and embedded by modifying the DC components. This algorithm provides good robustness against general processing attacks. A DCT-based multipurpose watermarking using subsampling has been proposed in [15]. The subsampling is first applied over the cover image to obtain four sub images, then DCT is applied over the subimages. Two different watermarks are embedded in the subimages of the cover image. The proposed algorithm has a good resistant against general processing attacks such as noise adding and filtering. The limitation of the schemes described in [14] and [15], is that as the JPEG compression ratio is increased, the robustness tends to decrease.

A number of watermarking schemes have also been proposed using DWT [8, 9, 16-18]. In [16] a multi resolution watermarking method for digital images based on the discrete wavelet transform has been proposed, where the cover image is decomposed into four sub-bands and the numbers from a pseudo random sequence are added to the large coefficients of the middle and high sub-bands of the DWT transformed image. Watermark extraction is carried out by comparing the original cover image with the possible attacked watermarked image. A scheme of embedding multiple watermarks in the discrete wavelet transform coefficients has been proposed by Raval and Rege in [17]. The watermarks embedded in the low-frequency coefficients are resistant to group of attacks, such as, lossy compression and low-pass filtering, whereas embedded in the high-frequency coefficients are resistant to other group attacks, such as gamma correction, lightening, and contrast adjustment. The drawback of this scheme is that embedding of the watermarks, especially that in the low-frequency area, causes a perceptual degradation in the cover image. In 2004, Tao and Eskicioglu [18] presented a wavelet based watermarking scheme, wherein a binary watermark is embedded in all the four sub-bands of the DWT transformed cover image. The watermarks embedded in different bands with a variable scaling factor; the scaling factor for the LL sub-band is large, whereas it is lower for the other sub-bands.

The DCT-based watermarking schemes are based on two facts. The first one is that most of the image energy is concentrated in the low-frequency band that holds the most important visual parts of the image, whereas the second one is that compression and noise attacks usually remove the high frequency components of the image [19]. Therefore in a DCT-based watermarking scheme, the modification is usually carried out in the middle-frequency band, so that the visual quality of the cover image is not affected and, at the same

time, the watermark is not removed by compression attack [12-15]. Similarly, in a DWT band watermarking scheme, depending on the decomposition level(s) chosen to embed a watermark, the LL and HH sub-bands of that level(s) should be avoided in order to provide a good trade-off between the robustness and transparency of the watermark.

In order to provide more robustness against attacks by embedding the watermark in the low-frequency band coefficients, but without affecting the visual quality of the watermarked images, in recent years a number of watermarking schemes have been developed using singular value decomposition on the DCT or DWT coefficients [6-10]. The main property of singular value decomposition is that the singular values of an image are less sensitive to general signal processing operation performed on an image. In [7] and [8], two image watermarking algorithms, one based on DCT-SVD and the other on DWT-SVD, have, respectively, been proposed. In these methods, a gray scale watermark is embedded by modifying the singular values of each sub-band by making use of the singular values of the watermark. The two schemes provide a good robustness against different attacks. The limitation of these algorithms is that the correlation between the singular values of the watermark and that of extracted watermark is not high enough after a rotation attack for the first method and after contrast adjustment and sharpening attacks for the second method. Feng and Yangguang have also proposed a watermarking scheme [6] based on DCT and SVD. This algorithm provides a good robustness against general processing attacks while having a good imperceptibility of the watermark, but the scheme lacks robustness against contrast adjustment, rotation and cropping attacks. In [9], another watermarking algorithm using DWT and SVD has been proposed. The watermark image is divided into two parts and embedded by modifying the singular values of the middle sub-

bands of the one-level decomposed cover image. The proposed scheme has a good robustness against general processing attacks, but not so against other types of attacks such as, noise corruption or rotation of the watermarked image.

From the foregoing discussion, it is clear that the existing schemes employing singular-value decomposition in a transform domain, lack the robustness against attacks. It is, therefore, necessary to investigate new watermarking schemes that are capable of providing improved robustness against attacks while preserving the perceptual quality of the cover image.

1.3 Scope of the Thesis

In the current literature on watermarking schemes, there exist a number of algorithms that provide good imperceptibility of the watermark data but lack robustness against certain attacks, or provide good robustness against attacks at the expense of degraded perceptual quality of the cover data. The objective of this work is to develop image watermarking schemes with performance that is superior to that of the existing ones in terms of their robustness as well as to provide imperceptibility to the embedded watermark data. To this end, in this thesis two new digital image watermarking schemes are proposed.

The first scheme is a DCT-SVD based embedding technique that makes use of the Arnold transform. The main idea here is to improve the robustness of the watermarking further by scrambling the watermark data using this transform while still providing a good perceptibility of the watermarked image furnished by the DCT-SVD based embedding.

In visual cryptography, a secret binary image is decomposed into shares. If this approach is used to embed the watermark data, a watermarking scheme can be expected to be more resilient to attacks as well as to provide more security to the content of the embedded data. In view of these considerations, a second watermarking scheme, based on DWT and SVD and in which the watermark data is embedded using visual cryptography, is developed.

1.4 Organization of the Thesis

The thesis is organized as follows.

In Chapter 2, an introduction to the watermarking technology is presented, with a summary of the desired features of watermarking and its types along with a description of the commonly used attacks against watermark data. This chapter also includes preliminaries on some of the transforms used for digital watermarking.

In Chapter 3, a new robust scheme for digital image watermarking based on DCT-SVD and the Arnold transform is introduced. Extensive simulations are performed to demonstrate the performance of the proposed method. The new scheme is shown to provide good imperceptibility of the embedded watermark and to make the embedded watermark to be more resistant to a wide variety of attacks on the watermarked image.

In Chapter 4, a DWT-SVD based watermarking scheme, in which the watermark data is embedded using the approach of visual cryptography, is developed. Extensive experiments are performed for examining the performance of the proposed scheme. It is shown that the

proposed method can efficiently resists different types of attacks while preserving the perceptual quality of the cover data.

Finally, Chapter 5 concludes the thesis by highlighting its contributions and, suggesting the investigation of the problem of blind watermarking based on the ideas explored in this thesis.

Chapter 2

Background Material

This chapter gives a brief introduction to digital image watermarking to provide a context to the work undertaken in this thesis. First, a description on the general watermarking scheme, classifications of watermarking schemes, and some desired features of a watermarking are presented. Then, a brief review some commonly used transforms in watermarking algorithms is given.

Section 2.1, introduces the general scheme of watermarking. Sections 2.2, describes the various ways in which watermarking schemes can be classified. The desired features of a watermarking are described in Section 2.3. Section 2.4, provides an overview of the singular value decomposition and discrete transforms. Section 2.5, gives a summary of the chapter.

2.1 General Watermarking Scheme

Digital watermarking is a process of embedding an identification code or some other information called watermark into digital multimedia without affecting the visual quality of

the host multimedia. A block diagram for the general scheme of watermarking is shown in Figure 2.1 [2]. It consists of the following modules.

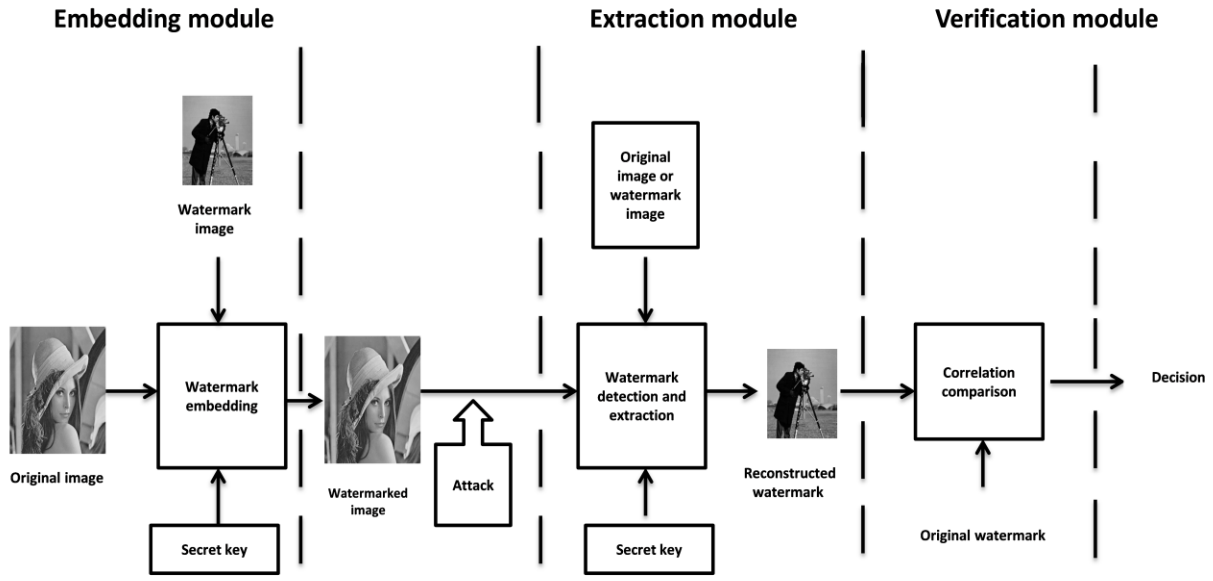


Figure 2.1: A general block diagram for image watermarking.

(a) Watermark embedding module

Inputs to a watermark embedding process are original data, watermark data, and a secret key. The output for the embedding module is watermarked data.

(b) Watermark detection and extraction module

Inputs to a watermark detection process are the watermarked data, the secret key, and depending on the watermarking algorithm, the original data, the original watermark or both. If the detection process needs a copy of the original cover image and a secret key, the

watermarking scheme is called *private watermarking* [5]. However, if a scheme requires only a secret key, it is called *public watermarking* [20]. On the other hand, if the detection process needs a copy of the watermark along with a secret key the scheme is called *semi-privet watermarking* [21].

(c) Verification module

In this module, the extracted watermark is checked whether or not it matches the original watermark. Usually this step is performed by comparing the original watermark with the extracted one using the correlation coefficient and the result gives a clear evidence whether or not the original watermark was embedded in the data.

2.2 Classification of Watermarking Schemes

Depending on the visibility, embedding domain, and embedding media of the watermark, watermarking techniques can be categorized into different classes.

Depending on the visibility of the watermark data embedded, a watermarking scheme can be classified as visible or invisible watermarking scheme.

(a) Visible watermarking*:* In these techniques, the watermark is embedded in the original cover image in a way that the watermark can be seen by the human visual system [32]. Logos are examples of visible watermarks, which indicate the owner of the data. A disadvantage of visible watermarks is that it can be easily removed from the cover image.

(b) Invisible watermarking*:* In these techniques, the watermark is embedded in the original cover image in a way that the watermark is not noticeable [5, 6, 8]. Unlike visible watermarks, these watermarks cannot be removed easily, but the watermark can be extracted by performing an appropriate detection and extraction operation.

Watermark data could be embedded in the original data or in a transformed-domain data, such as cosine transformed frequency domain.

(a) Watermarking in spatial domain*:* In this type of watermarking schemes, the watermark data is embedded by modifying the pixels [33]. The spatial domain watermarking techniques are considered to be the simplest watermarking techniques.

(b) Watermarking in a transform domain*:* In this type of watermarking techniques, the transformed coefficients of the cover image are modified by embedding the watermark. Transform domain watermarking techniques have more robustness against attacks. Typical transform methods used are discrete fourier transform (DFT) [10], discrete cosine transform (DCT) [6, 7], discrete wavelet transform (DWT) [8, 9], and singular value decomposition (SVD) [5, 23]. Each of these transforms has its own characteristics and transforms an image in different ways.

A watermarking scheme could also be classified as robust [20], semi-fragile [24], or fragile [22], depending on its robustness. Finally, based on the medium of embedding a watermarking scheme could be classified as audio, image, or video watermarking scheme.

Table 1 gives a summary of the various types of classifications of watermarking schemes along with a brief description of each.

Table 1: Classifications of the watermarking techniques

Criterion	Class	Brief description
Embedding domain	Spatial domain	Pixel values of the cover image are modified to embed the watermark data.
	Transform domain	Transform coefficients of the cover data are modified to embed the watermark.
Robustness	Robust	Survives after different types of attacks to destroy the watermark. This type of watermarking is used for copyright protection and ownership verification.
	Semi-fragile	Resistant to compression but responsive to other malicious attacks that attempt to modify the multimedia. Used for selective authentication.
	Fragile	Has the lowest robustness and not detectable after the multimedia is modified in anyway. Used for authentication purposes.
visibility	Visible	The watermark can be seen by the human visual system
	Invisible	The watermark cannot be seen by the human visual system
Information needed to extract watermark data	Private (Non-blind)	Original data and secret key are needed to extract the watermark data
	Public (Blind)	Only the secret key is needed to extract the watermark data
	Semi-private (Semi-blind)	The watermark and the secret key are needed to extract the watermark data

2.3 Desired Features of Watermarking

There are some desired features that one aims at while designing a watermarking scheme. Significance of these features varies depending the purpose and application of the watermarking technique [25].

(a) Robustness

The watermarking scheme is said to be robust if the embedded watermark can be detected and extracted after different types of attacks. Examples of common attacks on images include filtering, compression, and geometric distortions. When discussing the attacks, the context of the application is an important concern. For a particular application, not all of the attacks are necessarily to be significant. The application may expect certain types of attacks and requires an embedded watermark that provides robustness against such attacks. For instance, in the case of broadcast attack often includes lossy compression, analog-to-digital (A/D) and digital-to-analog (D/A) conversion, and additive noise. Robustness against other types of attacks may not be of much concern, since these attacks are not expected to happen in the given application.

According to the watermarking terminology, an *attack* is any process that affects the detection process of the watermark or the information provided by the watermark. There are different types of attacks [29, 30].

- lossy compression : JPEG and MPEG
- Geometric distortion: rotation, scaling, translation and cropping
- Signal enhancement: sharpening, contrast enhancement, and gamma correction

- Common signal processing operation: linear filtering, non-linear filtering, noise addition and D/A and A/D conversion

(b) Imperceptibility

The watermarked data should look like the original data to the viewers. In other words, the embedded watermark should not affect the perceptual quality of the original data. Imperceptibility is the main concern for invisible watermarks. Embedding a more powerful watermark to increase the robustness may cause degradation in the visual quality of the cover image. Therefore, a tradeoff between robustness and imperceptibility should be taken into consideration. Some watermarking algorithms embed the watermark to imperceptible spots in the cover image, where the human visual system (HVS) is less sensitive to these regions. For visible watermarks, imperceptibility is not an issue.

(c) Security

Unauthorized party should not be able to detect, retrieve or modify the embedded watermark. Many watermarking schemes designed to use a secret key. In such schemes, the way by which watermarks are embedded depends on a secret key and the same key must be used to detect and extract those watermarks. Therefore, even if the watermarking algorithm is known, it should not be possible for unauthorized parties to detect the presence of a watermark in the cover data without the knowledge of the secret key.

2.4 A Review of Transforms Commonly used in Watermarking

Mapping an image into another transform domain may make the coefficients of the transformed image uncorrelated to each other and the energy of the original data may get concentrated into just a few coefficients. Many of the watermarking schemes have exploited these features of the transformed data. In this section, we briefly review some of the transforms commonly used in watermarking.

2.4.1 Singular value decomposition (SVD)

Singular value decomposition is a fundamental mathematical analysis tool used to analyze matrices, and it has been successfully applied to different applications, such as signal processing, pattern analysis, and data compression. The singular value decomposition of an $m \times n$ matrix $\boldsymbol{C}$ of rank r is given by [26-28, 31].

$$\boldsymbol{C = USV^T}$$

where $\boldsymbol{U} = [\boldsymbol{u_1}, \boldsymbol{u_2}, \dots, \boldsymbol{u_r}]$ and $\boldsymbol{V} = [\boldsymbol{v_1}, \boldsymbol{v_2}, \dots, \boldsymbol{v_r}]$ are, respectively, $m \times r$ and $n \times r$ orthogonal matrices, and $\boldsymbol{S}$ is a diagonal matrix whose elements, $\boldsymbol{\lambda_i}$are non-zero singular values of $\boldsymbol{C}$, arranged in decreasing order as

$$\boldsymbol{S} = \begin{bmatrix} \boldsymbol{\lambda_1} & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{\lambda_2} & \boldsymbol{0} & \vdots \\ \vdots & & & \boldsymbol{0} \\ \boldsymbol{0} & \dots & \boldsymbol{0} & \boldsymbol{\lambda_r} \end{bmatrix} = \boldsymbol{diag}(\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \dots, \boldsymbol{\lambda_r}),$$

$$\boldsymbol{\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 0}$$

The columns of $\boldsymbol{U}, \boldsymbol{u_i}, i = 1, \dots, r,$ are the left singular vectors of the matrix $\boldsymbol{C}$, and the columns of $\boldsymbol{V}, \boldsymbol{v_i}, i = 1, \dots, r,$are the right singular vectors of the matrix $\boldsymbol{C}$. The matrix $\boldsymbol{C}$ can

then be expressed in terms of the left and right singular vectors and non-zero singular values as

$$= \boldsymbol{\lambda_1 u_1 v_1^T} + \boldsymbol{\lambda_2 u_2 v_2^T} + \ \ldots + \boldsymbol{\lambda_r u_r v_r^T} = \sum_{i=0}^{r} \boldsymbol{\lambda_i u_i v_i^T}$$

The main property of singular value decomposition pertinent to digital watermarking is that the singular values of an image do not change significantly when common image processing attacks are performed on an image. To illustrate this, we consider the Lena image without attack and its singular value matrix shown in Figure 2.2. Figure 2.3, shows Lena image with salt and pepper noise attack and the corresponding singular value matrix. It is seen that the singular values given in $\boldsymbol{S_1}$ and $\boldsymbol{S_2}$ are not significantly different.

$$S_1 = \begin{bmatrix} 126.89 & & & & \\ & 20.75 & & & 0 \\ & & 16.0 & & \\ & & & 12.71 & \\ & 0 & & & 11.54 \\ & & & & \ddots \end{bmatrix}$$

Figure 2.2: Lena image and its singular value matrix.

$$S_2 = \begin{bmatrix} 126.64 & & & & \\ & 19.162 & & & \\ & & 15.055 & & 0 \\ & & & 12.091 & \\ & & 0 & & 10.925 \end{bmatrix}$$

Figure 2.3: Lena image with salt & peppers noise attack and the singular value matrix.

A number of watermarking schemes have been proposed using SVD [5-9]. In these methods, the watermark image is embedded by modifying the singular values of the cover image. Tan and Liu [5] have proposed a watermarking scheme based on SVD. The watermark embedding and extraction schemes can be described as follows. In the watermark embedding process, the singular value decomposition is performed on the cover image $\boldsymbol{C}$ giving the singular value matrix $\boldsymbol{S}$ and the two orthogonal matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ as

$$\boldsymbol{C = USV^T}$$

The watermark image $\boldsymbol{W}$ is added to the singular value matrix $\boldsymbol{S}$, and the resulting matrix is subjected to singular value decomposition as

$$\boldsymbol{S} + \alpha \boldsymbol{W} = \boldsymbol{U_w S_w V_w^T}$$

where α is a scaling factor (a constant). Thus, the watermarked image $\boldsymbol{C_w}$ is obtained by.

$$\boldsymbol{C_w} = \boldsymbol{U S_w V^T}$$

Being given $\boldsymbol{U_w}$, $\boldsymbol{S}$ and $\boldsymbol{V_w}$ matricesand a possibly distorted watermarked image $\boldsymbol{C_w^*}$, in the watermark extraction process, the possibly corrupted watermark $\boldsymbol{W^*}$can be extracted by essentially reversing the above steps as

$$\boldsymbol{C_w^* = U^* S_w^* V^{*T}}$$

$$\boldsymbol{A^* = U_w S_w^* V_w^T}$$

$$\boldsymbol{W^* = (A^* - S)/\alpha}$$

This algorithm provides a good robustness against compression, rescaling and cropping, but lacks robustness against contrast adjustment, noise corruption and histogram equalization.

2.4.2 Discrete cosine transform (DCT)

The discrete cosine transform is one of the processes of transforming data from the spatial domain to the frequency domain. The DCT has an excellent energy compaction. In DCT of a typical image, most of the energy is concentrated in the low-frequency band (upper left corner) that holds the most important visual parts of the image, and energy decreases rapidly as the frequency increases.

The two-dimensional DCT (2D-DCT) of an $N \times N$array x is defined as

$$X(k,l) = \frac{2}{N} C(k)C(l) \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} x(n,m) \cos \frac{(2m+1)\pi k}{2N} \cos \frac{(2n+1)\pi l}{2N}$$

where k, l = 0, 1, 2, …, N-1, C(0) =$\frac{1}{\sqrt{2}}$, and C(n)=1 for n≠0.

The DCT is an invertible transform, the two-dimensional inverse DCT (2D-IDCT) is given by

$$x(n,m) = \frac{2}{N} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} C(k)C(l)X(k,l) \cos \frac{(2m+1)\pi k}{2N} \cos \frac{(2n+1)\pi l}{2N}$$

where m, n = 0, 1, 2, …, N-1.

A variety of image watermarking schemes have been proposed using DCT. The authors in [12] have proposed a watermarking algorithm, in which the watermark is embedded into the spectral components of the image using DCT domain. The watermark consists of a sequence of real numbers $Z = \{z_1, z_2, z_3, \dots, z_n\}$, where each number is selected according to normal distribution with zero mean and unit variance. In order to provide robustness against JPEG compression and common signal processing attacks, the watermark is embedded in the n lowest frequency coefficients $\boldsymbol{X} = \{x_1, x_2, x_3, \dots, x_n\}$ of the DCT-transformed cover image. The watermark embedded into the cover image using.

$$y_i = x_i(1 + \alpha z_i)$$

where α is the scaling factor.

The watermark is extracted by essentially reversing the steps used to embed $\boldsymbol{W}$ into $\boldsymbol{X}$. The extracted watermark $\boldsymbol{W}^*$ is compared with the original watermark $\boldsymbol{W}$ using the following similarity measure.

$$sim(W, W^*) = \frac{W.W^*}{\sqrt{W^*.W^*}}$$

The watermark is present, if the similarity between the extracted watermark and the original watermark is greater than a specified threshold.

2.4.3 Discrete wavelet transform (DWT)

In this section, a brief introduction to DWT is provided. The DWT has received considerable attention in various signal processing applications, including digital image watermarking.

The basic idea of the DWT for a one-dimensional signal is the following. A signal is split into two sub-bands, as illustrated in Figure, 2.4. The output coefficients of the low-pass filter are called the approximation coefficients, whereas those of the high-pass filter are called the detail coefficients. A down-sampling by a factor of 2 is carried out at each level of decomposition, to keep the number of coefficients constant and equal to the length of the original signal being decomposed [34]. In case of two- dimensional signal, the signal is decomposed along the row and column directions by using a set of both low-pass and high-pass filters. At any decomposition level, the output consists of four sub-bands: an approximation sub-band (LL), and three detail sub-bands (LH, HL and HH) that are called the horizontal, vertical, and diagonal sub-bands, as shown in Figure 2.5. The approximation

sub-band (LL) is used to obtain the sub-bands at the next level of decomposition as depicted in Figure 2.6.

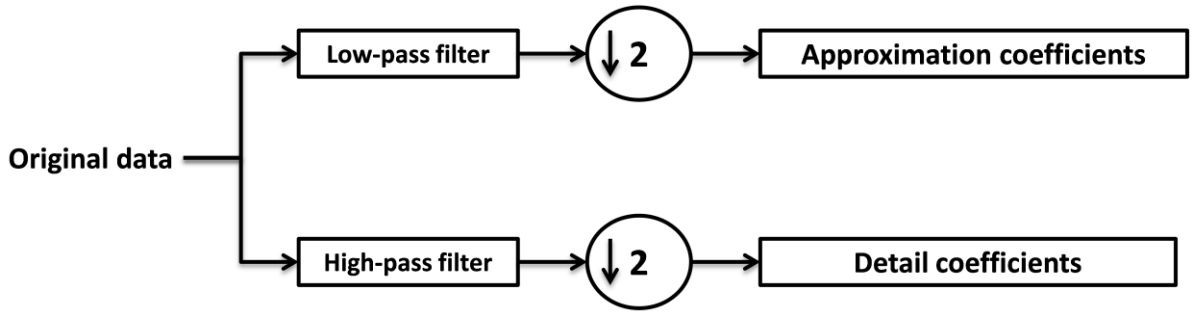


Figure 2.4: Wavelet sub-bands with 1-level decomposition of a 1-dimensional signal.

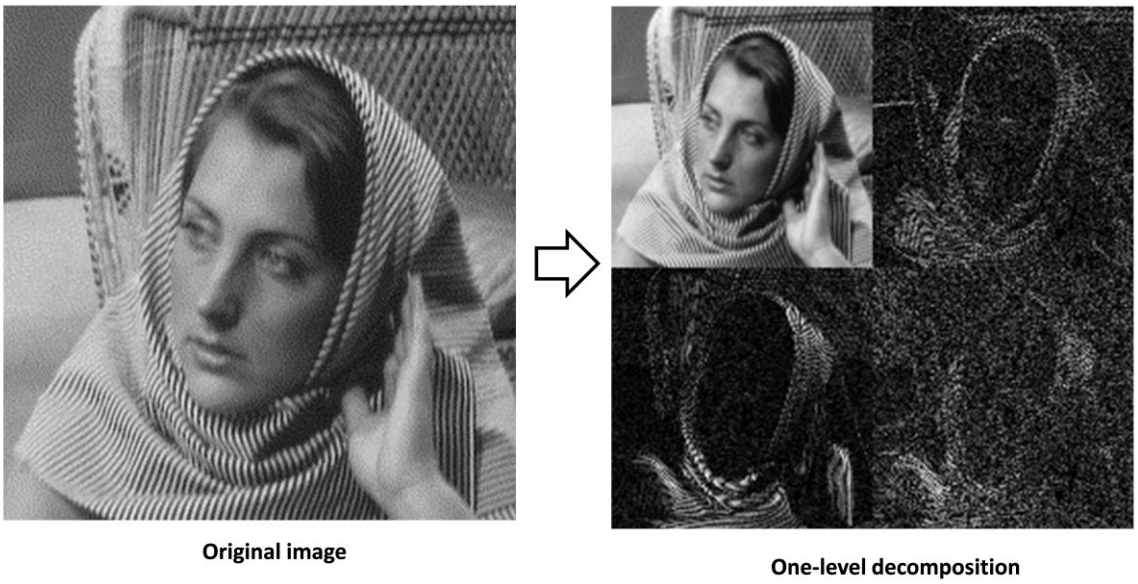


Figure 2.5: illustration of 2-dimensional DWT for an image.

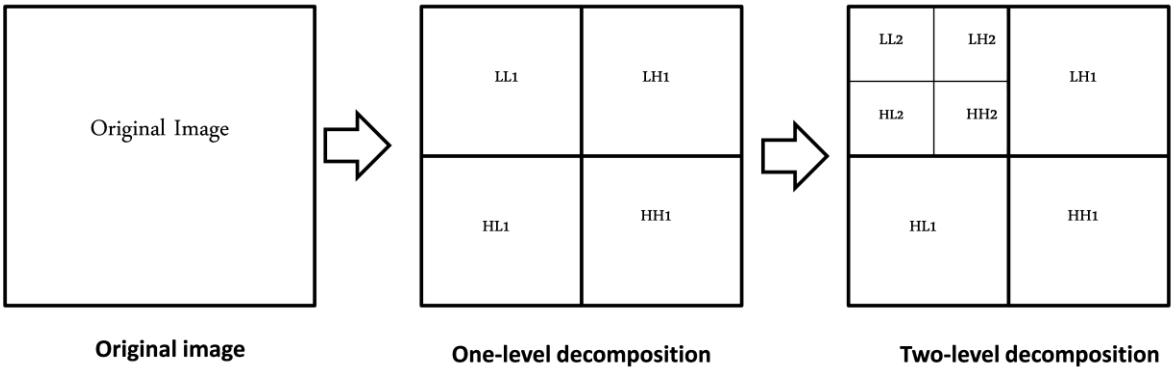


Figure 2.6: Wavelet sub-bands with 2-level decomposition of a 2-dimensional signal.

2.5 Summary

In this chapter, some background material pertinent to the development of the work undertaken in this thesis has been reviewed. First, a general scheme for watermarking comprising watermark embedding, watermark detection and extraction, and verification modules has been described. Next, the various categories of the watermarking schemes based on the embedding domain, robustness, visibility, and information required for extraction of the watermarks have been described. Finally, three transform methods, namely, singular value decomposition, discrete cosine transform, and discrete wavelet transform, commonly used for watermarking have been briefly reviewed.

Chapter3

An Arnold Transform integrated DCT-SVD Based Digital Watermarking Scheme

3.1 Introduction

As discussed in Chapter 1, spatial-domain watermarking schemes, in general, lack the robustness against lossy compression attacks, and have low-information hiding capacity. In order to preserve the perceptual quality of the cover image and make the watermark less prone to compression attacks, transform-domain watermarking schemes, in which the modification is usually carried out in the mid-frequency band, have been proposed. In an effort to further improve the robustness of these transform-domain watermarking schemes and preserve the visual quality of the cover image, the embedding of the watermark is carried out through a singular-value decomposition (SVD) in the transform domain. These schemes either provide good imperceptibility of the watermark without sufficient resilience to certain types of attacks or provide good robustness against attacks at the expense of a degraded perceptual quality of the cover image.

In this chapter, an Arnold transform integrated DCT-SVD based watermarking scheme is developed with a view to provide an improved robustness against a wide variety of attacks with little effect on the perceptual quality of the cover image.

In Section 3.2, image scrambling using Arnold transform is briefly discussed. In Section 3.3, a new DCT-SVD based digital image watermarking scheme that makes use of the Arnold transform for scrambling the watermark image prior to its embedding is proposed. In Section 3.4, experimental results demonstrating the performance of the proposed algorithm are presented. The performance of the proposed algorithm is also compared with those of other existing algorithms in this section. Finally, Section 3.5 gives a brief summary of the work carried out in this chapter.

3.2 Image Scrambling

Image scrambling process is an important image encryption technique that has been used in digital image watermarking for data hiding. The objective of digital image scrambling is to transform a meaningful image into unintelligible image that prevents unauthorized users from understanding its true content. An authorized user can descramble the image using the information on the technique utilized for scrambling and a secret key. Without the knowledge of the image scrambling algorithm and the secret key, an unauthorized user (attacker) would not be able to recover the original watermark, even if it has been extracted from the watermarked data. Thus, scrambling provides an additional security for

the digital data. Furthermore, since scrambling of an image, eliminates the spatial correlation of its pixels, the robustness of a watermarking scheme can be further improved.

There are several image scrambling techniques, most of which are based on the Arnold transform or on a combination of Arnold transform with other techniques [11, 35-37].

Arnold Transform

The Arnold transform, also commonly known as cat-face transformation, or cat-face mapping, was introduced by Arnold [38]. For an image $\boldsymbol{C}$ with $N \times N$ pixels, the Arnold transform operation on the position (x, y)pixel is given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \tag{3.1}$$

The Arnold transform, which changes the positions of the pixels, can be repeated many times in order to obtain a scrambled image. However, due to the periodicity of the Arnold transformation, the original image can be restored after a certain number of iterations. Dyson and Falk [39] have studied the properties of the Arnold transform and pointed out that the transform given by (3.1) has a period $T_N \leq N^2 / 2$, for $N > 2$. Table 3.1gives the values of T_N for various values of N. Figure 3.1 depicts an example of applying the Arnold transform on the Pepper image with $N = 128$. Figure 3.1 (a) is the original 128×128 Pepper image, whereas Figure 3.1 (b) and (c) show, respectively, the Arnold transformed image after $n = 5$ and $n = T_{128} = 96$ iterations. It is seen that the original image of Figure

3.1 (a) is recovered in Figure 3.1 (c) after applying on the former the operation of the Arnold transform a number of times that is equal to the period of the transform, i.e., $T_N = 96$.

Table 3.1: The periods of Arnold transformation for different values of N

N	**10**	**32**	**50**	**64**	**100**	**125**	**128**	**256**	**480**	**512**
Period (T_N)	30	24	150	48	150	250	96	192	120	384

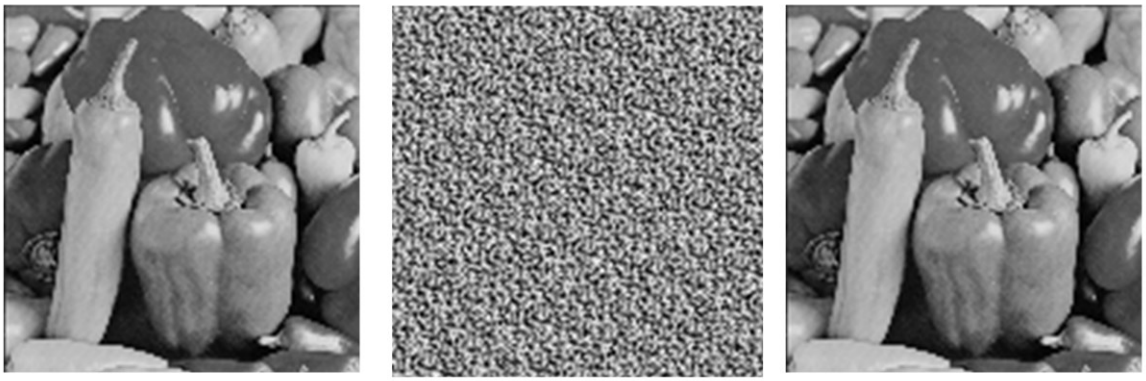


Figure 3.1: (a) Peppers image of size128×128. (b) Scrambled image after $n = 5$ iterations of the operation of the Arnold transform. (c) The reconstructed image after $n = T_{128} = 96$ iterations of the Arnold transform.

It is seen from Table 3.1 that there is no well-defined relationship between the image size and the transform period. For some images of certain sizes their period could be very long

and this could result in a computational complexity problem for images with these sizes in algorithms employing the Arnold transform for scrambling.

Anti-Arnold Transform

Use of the Arnold transform periodicity on a scrambled image to recover the original image could be achieved at the expense of possibly a large computational complexity depending on how many iterations have already been used to obtain the scrambled image. For this reason the authors in [40] have obtained the anti-Arnold transform. The anti-Arnold transform is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} mod\ N \tag{3.2}$$

If a scrambled image is obtained by using n iterations of the operation of the Arnold transform, it needs the same number of iterations to recover the original image using the anti-Arnold transform. Therefore, the use of anti-Arnold transform to recover the original image can provide significant savings in computation, if $n \ll T_N$. To illustrate this point, consider the 128×128 original Boat image shown in Figure 3.2(a). Figures 3.2 (b) and (c) show, respectively, the scrambled image using $n = 15$ iterations of the Arnold transform and the recovered image using $n = 15$ iterations of the anti-Arnold transform on the image of Figure 3.2 (b). Note that the use of $n = 15$ iterations is much less than the use of $T_N - n = 96 - 15 = 81$ iterations of the Arnold transform to recover the original image.

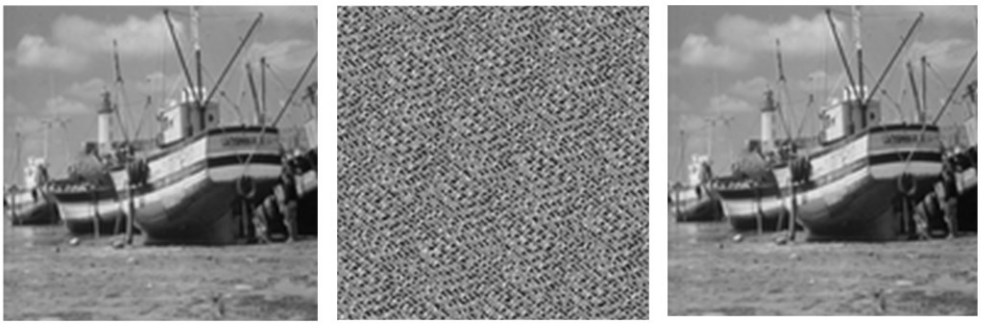


Figure 3.2: (a) Boat image. (b) Scrambled image after $n = 15$ iterations of the operation of the Arnold transform. (c) The recovered image after $n = 15$ iterations of the operation of the anti- Arnold transform on the scrambled image of Figure 3.2(b).

Figure 3.3 shows the times to recover the original images of various sizes using the Arnold and anti-Arnold transforms, when $n = 20$ iterations have been used to obtain the scrambled images. It is clear that in this case when only 20 iterations have been used to scramble an image, there is considerable savings in the computation time to recover the original image by using the anti-Arnold transform instead of using the Arnold transform.

3.3 Proposed Watermarking Algorithm

The proposed watermarking scheme consists of a watermark embedding process and a watermark extraction process.

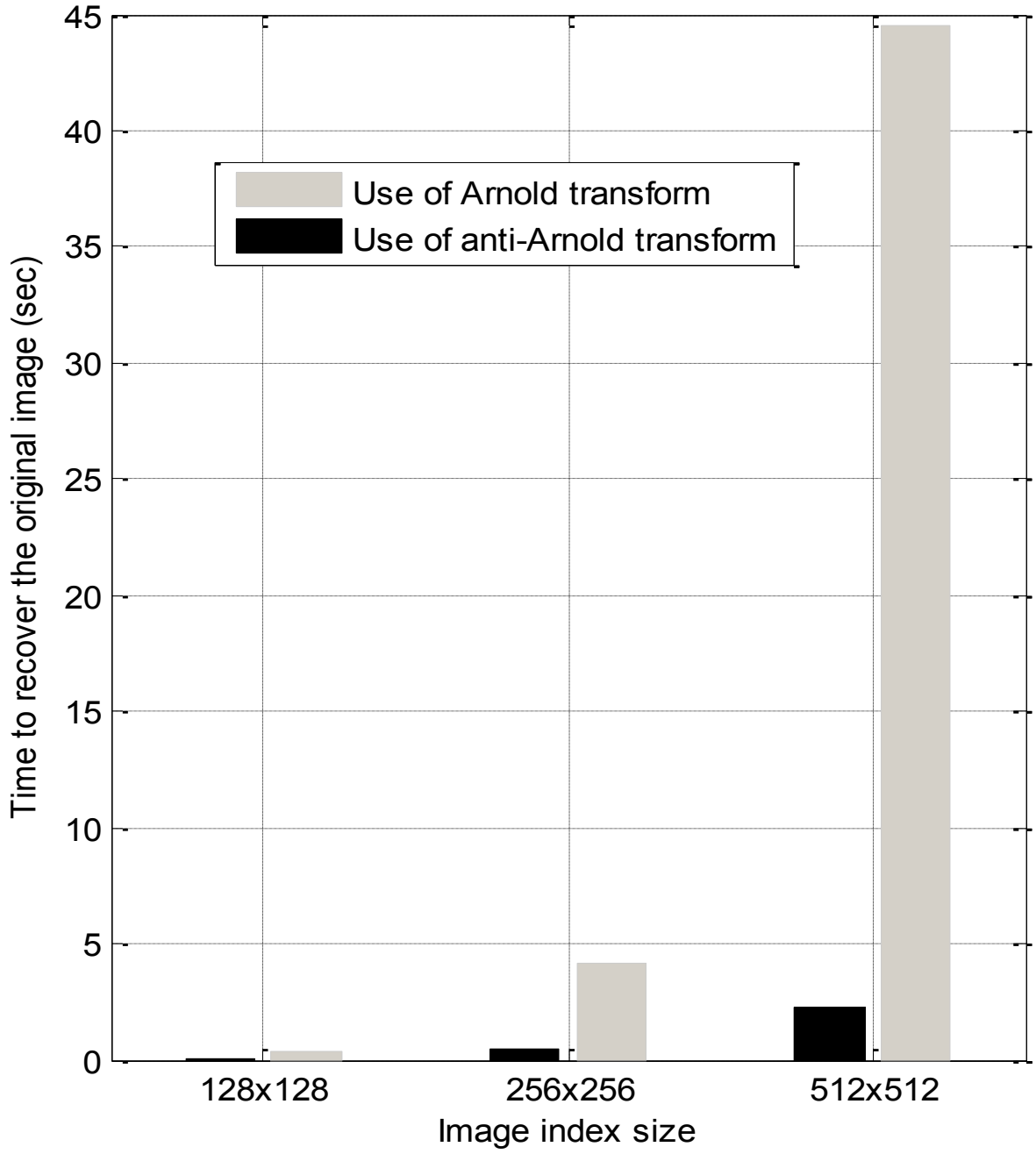


Figure 3.3: Time needed to recover the original image from a scrambled image by using the Arnold and anti-Arnold transforms. The scrambled images have been obtained by applying 20 iterations of the Arnold transform on the original images.

3.3.1 Watermark embedding

Figure 3.4 shows a block diagram of the proposed watermark embedding scheme. In this scheme, the discrete cosine transform is first applied to an $M \times M$ cover image $\boldsymbol{c}$. Then, the entire array of the DCT coefficients are zig-zag scanned as shown in Figure 3.5 (a), and the scanned coefficients are mapped into the subbands B_1, B_2, B_3 and B_4 of another array as shown in Figure 3.5 (b). The scanned coefficients are mapped in a zig-zag manner into the individual subbands starting from the subband B_1, and ending with the subband B_4 .Then, each subband is individually made to undergo an SVD operation. Next, an $N \times N (2N \leq M)$ watermark image is scrambled by applying r iterations of the Arnold transform. The number of iterations r is saved as a secret key, to be used during the extraction process to recover the original watermark image. The singular value matrix of each subband is then modified by adding to this matrix a scaled version of the scrambled watermark image. The resulting subband image $\mathrm{S}_k + \alpha \mathrm{W}'$ is singular value decomposed to obtain the singular value matrix S_{wk}^* of the watermarked subband. The subband watermarked DCT coefficients are obtained by augmenting S_{wk}^* with U_k and V_k^T as $B_k^* = U_k S_{wk}^* V_k^T$. Finally, the modified DCT coefficients are mapped back to their original positions, followed by an inverse discrete cosine transform operation to obtain the watermarked image. The proposed watermark embedding scheme is presented as Algorithm 3.1.

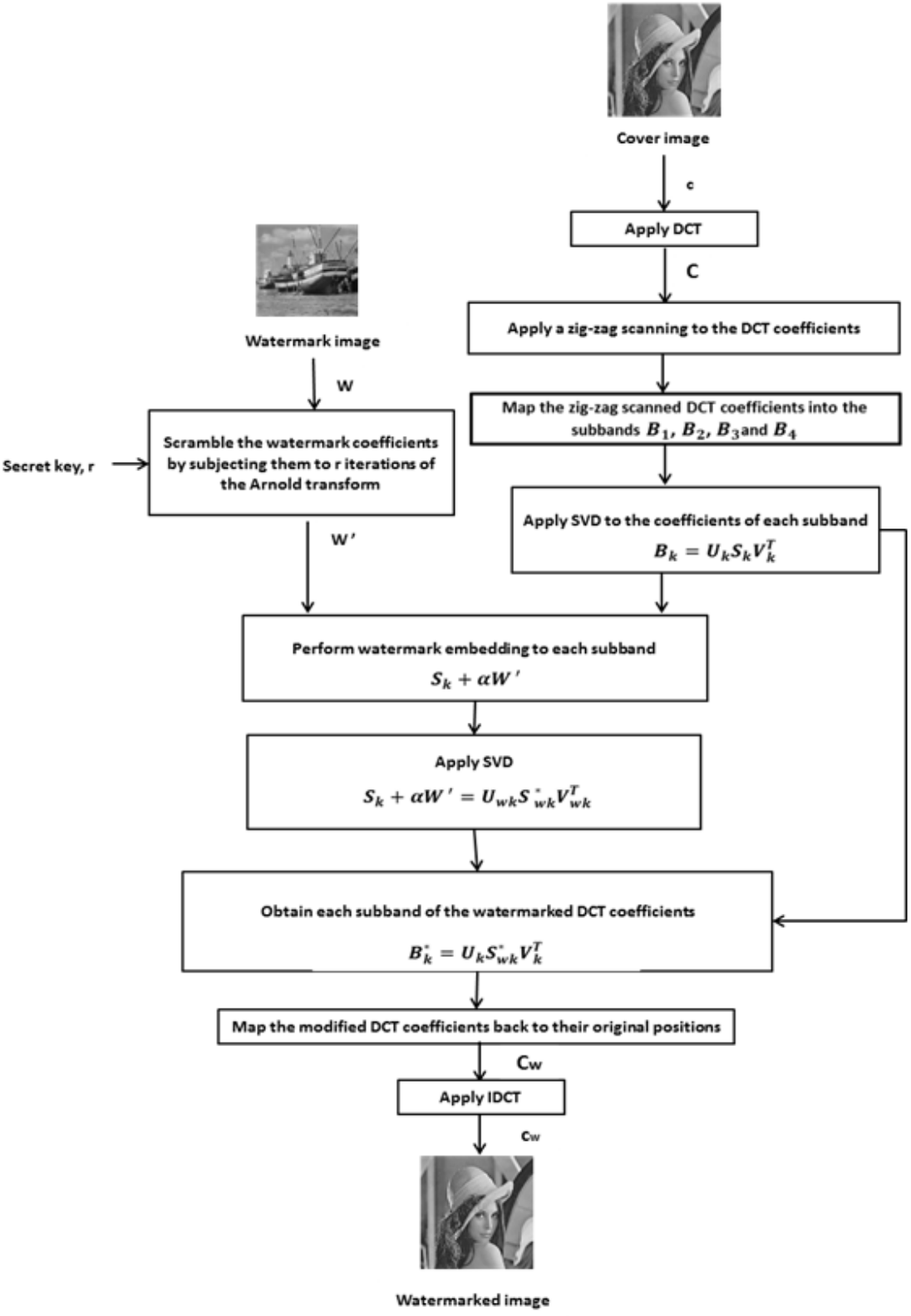
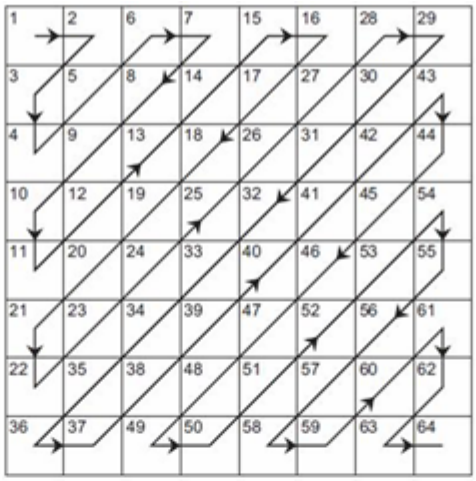
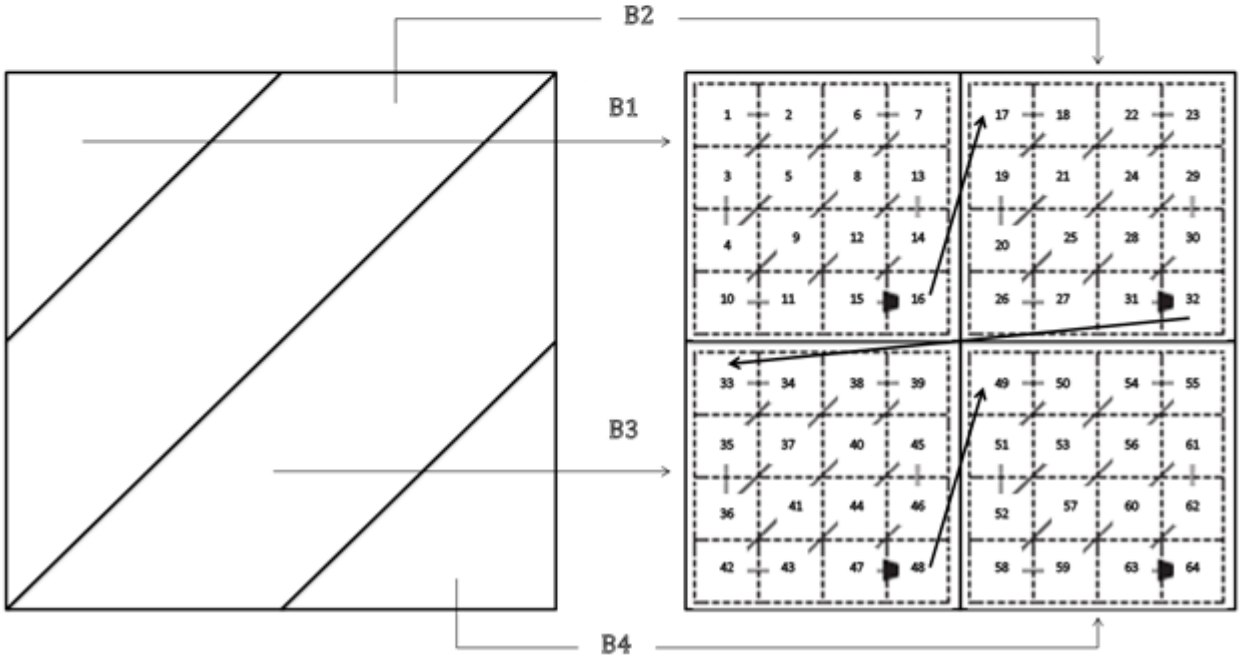


Figure 3.4: Block diagram of the proposed watermark embedding scheme.



(a)



(b)

Figure 3.5: (a) Zig-zag scanning of the 2D- discrete cosine transform coefficients.
(b) Mapping of the scanned DCT coefficients into four subbands.

Algorithm 3.1: Watermark embedding algorithm

Step 1	Apply the discrete cosine transform to the cover image $\boldsymbol{c}$.
Step 2	Rearrange the 2-D DCT coefficients into four subbands: B_1, B_2, B_3 and B_4, through a zig-zag scanning of the DCT coefficients.
Step 3	Apply an SVD operation to each subband: $B_k = U_k S_k V_k^T, k = 1, 2, \dots, 4$.
Step 4	Apply r iterations of the Arnold transform given by (3.1) on the watermark image W to obtain scrambled watermark image W'.
Step 5	Modify each subband singular value matrix S_k through a watermark embedding as $S_k + \alpha W'$, where α is a scaling factor.
Step 6	Apply the SVD operation to $S_k + \alpha W'$ as $S_k + \alpha W' = U_{wk} S^*_{wk} V^T_{wk}$.
Step 7	Augment the singular value matrix S^*_{wk} with U_k and V_k to obtain the watermarked DCT coefficients as $B^*_k = U_k S^*_{wk} V^T_k$
Step 8	Map the watermarked DCT coefficients of the subbands back to their original positions, obtaining $\boldsymbol{C_w}$.
Step 9	Apply the inverse discrete cosine transform to obtain the watermarked image $\boldsymbol{c_w}$.

3.3.2 Watermark extraction

Figure 3.6 shows a block diagram of the proposed watermark extraction scheme. In this scheme, the discrete cosine transform operation is applied to the watermarked (possibly attacked) image $\boldsymbol{C_w}$, followed by a re-arranging of the DCT coefficients into four subbands B_{w1}, B_{w2}, B_{w3} and B_{w4} through a zig-zag scanning of the coefficients. Then, each subband is individually made to undergo an SVD operation. Next, the singular value matrix of each subband S'_{wk} is augmented with U_{wk} and V^T_{wk} to obtain $D'_k = U_{wk} S'_{wk} V^T_{wk}$. A scrambled watermark image is extracted from each subband as $W_k'^* = (D'_k - S_k)/\alpha$, followed by an

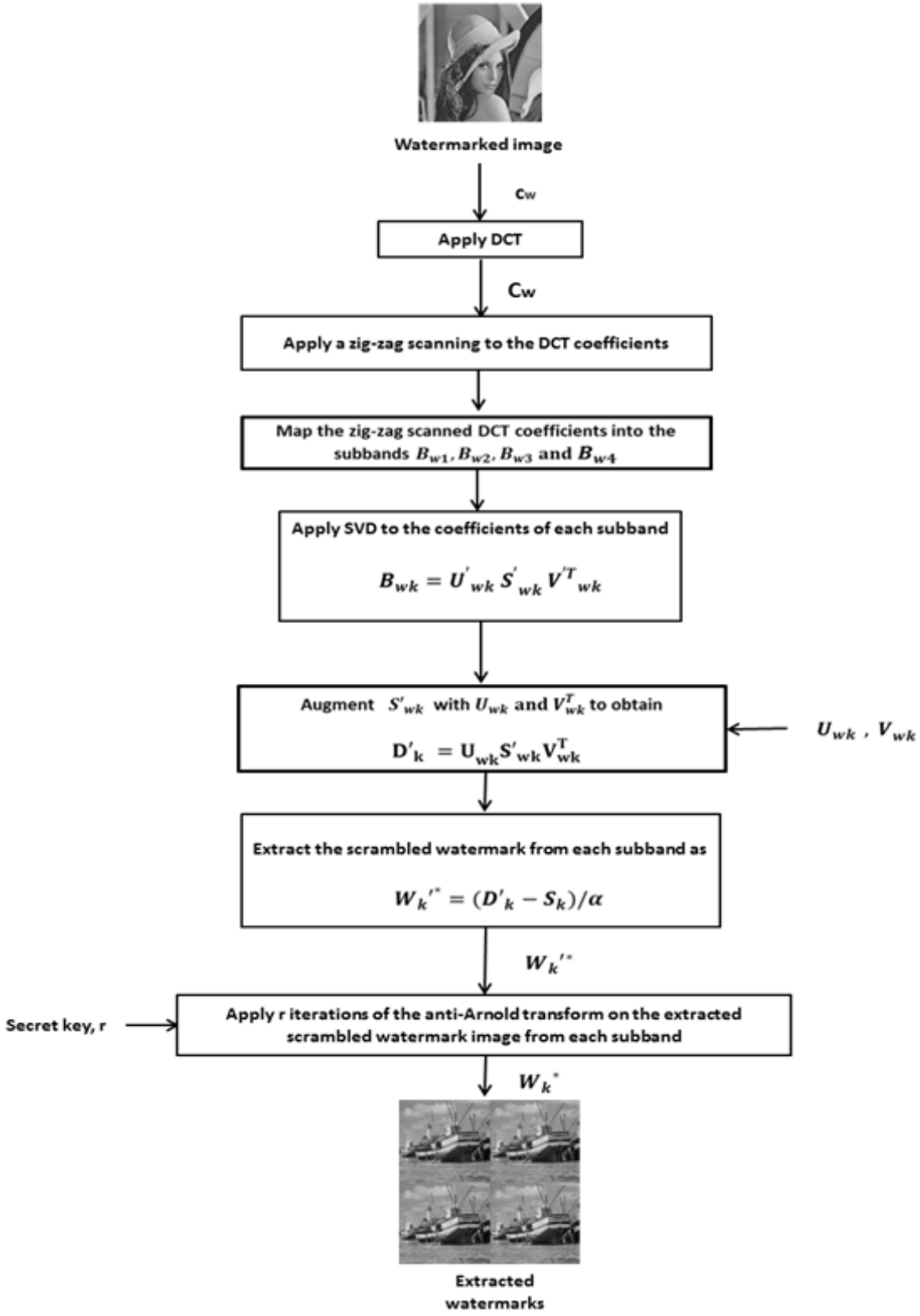


Figure 3.6:Block diagram of the proposed watermark extraction scheme.

application of r iterations of the anti-Arnold transform to obtain the original watermark image.It should be noted that the number of iterations r of the anti-Arnold transform is used as a secret key during the extraction process. The steps of the proposed watermark extraction scheme are presented as Algorithm 3.2.

Algorithm 3.2: Watermark extraction algorithm

Step 1	Apply the discrete cosine transform to the watermarked image $\boldsymbol{c_w}$.
Step 2	Rearrange the 2-D DCT coefficients into four subbands: B_{w1}, B_{w2}, B_{w3} and B_{w4}, through a zig-zag scanning of the DCT coefficients.
Step 3	Apply an SVD operation to each subband: $B_{wk} = U'_{wk} S'_{wk} V'^{T}_{wk}$, $k = 1, 2, \dots, 4$.
Step 4	Augment S'_{wk} with U_{wk} and V_{wk}^T to obtain : $D'_k = U_{wk} S'_{wk} V_{wk}^T$
Step 5	Extract the scrambled watermark image from each subband as $W_k'^* = (D'_k - S_k)/\alpha$.
Step 6	Apply r iterations of the anti-Arnold transform given by (3.2) on the scrambled watermark image $W_k'^*$ to obtain the original watermark image W_k^*.

3.4 Experimental Results and Discussion

The proposed watermarking scheme is implemented using MATLAB (R2012a) on a PC with a1.6-GHz AMD E-350 processor, 3-GB RAM, and Microsoft Windows 7 operating system. Extensive experiments are conducted to demonstrate the performance of the proposed watermarking scheme. Three gray-scale cover images, *Lena*, *Pirate*, and *Couple*, and three watermark images, *Boat*, *Peppers*, and *Cameraman*, as depicted in Figure 3.7, are used in these experiments. The size of each cover image is 256 × 256 and that of each watermark image is 128 × 128.

Figure 3.7: Cover images: (a) *Lena*, (b) *Pirate*, and (c) *Couple*. Watermark images: (d) *Boat,* (e) *Peppers*, and (f) *Cameraman*.

In all the experiments, the scaling factor is set to 0.25 for watermark embedding of the B_1 subband and to 0.05 for the embedding of the other three subbands. The reason behind using a higher value for the B_1 subband coefficients and a lower value for the other three subbands is as follows. The coefficients in the B_2, B_3, and B_4 subbands represents the pixel coefficients of the cover image with progressively rapid changes in texture. Therefore, by embedding the coefficients in these bands with a lower scaling factor would help in preserving the perceptual quality of the cover image.

Figure 3.8 shows an example of a watermarked image and the extracted watermark image obtained by applying the proposed scheme of watermarking; Figure 3.8 (a) and (b) show, respectively, an original cover image *Lena* and an original watermark image *Boat*, and Figure 3.8 (c) and (d) show, respectively, the watermarked image and the watermark images extracted from the un-attacked watermarked image of Figure 3.8 (c) using the proposed watermarking scheme. It is seen from Figure 3.8 that the embedded watermark dose not degrade the perceptual quality of the cover image, and the proposed scheme is able to extract the watermark images successfully from the un-attacked watermarked image.

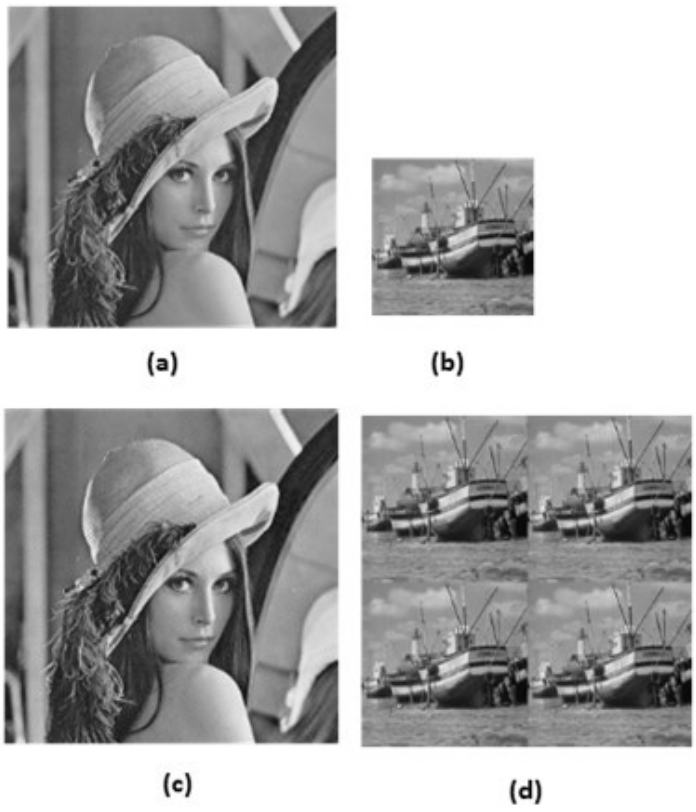


Figure 3.8: (a) Cover image, *Lena*. (b) Watermark image, *Boat*. (c) Watermarked image. (d) Watermark images extracted from each of the four subbands of the watermarked image.

For objective evaluation of the perceptual quality of watermarked image, the peak signal-to-noise ratio (PSNR) is used [42-45]. The PSNR is given by

$$PSNR = 10 \log_{10} \left(\frac{MAX^{2}}{MSE} \right) \tag{3.3}$$

where MAX represents the maximum pixel value in the watermarked image, and MSE is the mean squared error between the original cover image and the watermarked image and it is given by

$$MSE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} [C_{i,j} - C'_{i,j}]^2}{M \times M} \tag{3.4}$$

with $C_{i,j}$ and $C'_{i,j}$ denoting the pixel values in the original cover image and the watermarked image, respectively. In general, a PSNR value is higher than 30 dB is considered to be an indication of good perceptual quality of the watermarked image [42-45]. Table 3.2 gives the PSNR values of the various watermarked images obtained by using the proposed watermarking scheme. This table clearly indicates that the embedded watermark does not degrade the perceptual quality of the cover image, and thus the proposed embedding scheme guarantees the imperceptibility of the watermark.

Table 3.2: The PSNR values (in dB) of various watermarked images obtained by using the proposed watermarking scheme

Watermark image / Cover image	*Boat*	*Peppers*	*Cameraman*
Lena	32	32.53	32.79
Couple	31.18	32.13	32.55
Pirate	31.67	32.38	32.83

To investigate the robustness of the proposed watermarking scheme, the watermarked image is subjected to various types of attacks. The attacks used in our robustness study are JPEG compression, Gaussian noise, blurring, cropping, rescaling, translation, rotation, brightness adjustment, sharpening, gamma correction, contrast adjustment, histogram equalization, and median filtering. For each of these attacks, we extract four watermarks using the proposed watermark extraction scheme from the four subbands, then we select the one having the largest normalized correlation coefficient between the extracted and the original watermark images. The normalized correlation (NC) between the original watermark image W and an extracted watermark image W^* is given by [46-48]

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(W_{ij})\ \ (W_{ij}^{*})}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(W_{ij})^{2}}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(W_{ij}^{*})^{2}}} \tag{3.5}$$

Figure 3.9 shows the original of the cover image, *Lena* and the original watermark image, *Boat* to be embedded in the cover image using the proposed watermarking scheme.

Figures 3.10-3.23 show the watermarked *Lena* images, each subjected to one type of attack, and the watermark images extracted from the attacked images. It is seen from these figures that the proposed scheme yield watermarked images with a perceptual quality very similar to that of the original cover image and that it effectively resists different types of attacks leading to the extraction of the watermark images with high perceptual quality.

(a) (b)

Figure 3.9: (a) Original cover image, *Lena*. (b) Original watermark image, *Boat*.

JPEG compression (Q = 10)
(a) **(b)**

Figure 3.10: (a) Watermarked *Lena* image attacked by JPEG compression. (b) Extracted watermark image.

Gaussian noise contamination (σ^2= 0.3)
(a) **(b)**

Figure 3.11: (a) Watermarked *Lena* image attacked by Gaussian noise. (b) Extracted watermark image.

Cropping (left and right sides by 25 columns each)

(a) **(b)**

Figure 3.12: (a) Watermarked *Lena* image attacked by cropping. (b) Extracted watermark image.

Re-scaling (256-128-256)

(a) **(b)**

Figure 3.13: (a) Watermarked *Lena* image attacked by re-scaling. (b) Extracted watermark image.

Translation (horizontally and vertically by 20 lines each)

(a) **(b)**

Figure 3.14: (a) Watermarked *Lena* image attacked by translation. (b) Extracted watermark image.

Rotation (rotated by 2° and restored to the original size)
(a) **(b)**

Figure 3.15: (a) Watermarked *Lena* image attacked by rotation. (b) Extracted watermark image.

Darkening (70%)
(a) **(b)**

Figure 3.16: (a) Watermarked *Lena* image attacked by darkening. (b) Extracted watermark image.

Brightening (70%)
(a) **(b)**

Figure 3.17: (a) Watermarked *Lena* image attacked by brightening. (b) Extracted watermark image.

Sharpening (80%)

(a) **(b)**

Figure 3.18: (a) Watermarked *Lena* image attacked by sharpening. (b) Extracted watermark image.

Blurring using 9x9 Gaussian filter with σ = 1

(a) **(b)**

Figure 3.19: (a) Watermarked *Lena* image attacked by blurring. (b) Extracted watermark image.

Contrast adjustment (reduced by 20%)

(a) **(b)**

Figure 3.20: (a) Watermarked *Lena* image attacked by contrast adjustment. (b) Extracted watermark image.

Gamma correction
(γ = 0.6)
(a) **(b)**

Figure 3.21: (a) Watermarked *Lena* image attacked by gamma correction. (b) Extracted watermark image.

Median filtering (3x3)
(a) **(b)**

Figure 3.22: (a) Watermarked *Lena* image attacked by median filtering. (b) Extracted watermark image.

Histogram equalization
(a) **(b)**

Figure 3.23: (a) Watermarked *Lena* image attacked by histogram equalization. (b) Extracted watermark image.

In order to have an objective investigation of the robustness of the proposed watermarking scheme, we consider three different cover images, *Pirate, Couple,* and *Lena,* and three different watermark images, *Pepper, Cameraman,* and *Boat.* Each watermarked image obtained by using the proposed watermark embedding scheme is subjected to various types of attacks. The watermark image is then extracted from an attacked image using the proposed watermark extraction scheme. The normalized correlation coefficient between the extracted and the original watermark images is computed. Table 3.3 gives the values of the correlation coefficient between the extracted and original watermark images using the cover images, *Pirate, Couple,* and *Lena,* and the same watermark image, *Boat.* Table 3.4 lists the values of the correlation coefficient for which the watermark images, *Pepper, Cameraman,* and *Boat* are used for embedding the same cover image, *Lena*. It is seen from these tables that the values of the correlation coefficient are almost invariably larger than 0.9 for the various attacks regardless of the watermark and cover images used in our experiments.

In order to investigate the performance of the proposed watermarking scheme, we also implement the DWT-SVD based watermarking scheme [37], and the DCT-SVD image watermarking scheme [41], for performance comparison in terms of the PSNR of the watermarked image measuring the imperceptibility of the watermark and the correlation coefficient between the original and extracted watermark images measuring the robustness of the watermarking schemes. The performance comparison is given in Table 3.5. It is seen from this table that the proposed watermarking scheme preserves the perceptual quality of the cover image, and provides an improved robustness against

various types of attacks. Thus, the proposed scheme outperforms the other two algorithms used for comparison.

Table 3.3: Values of the correlation coefficient between the extracted and original watermark images. The watermark image *Boat* is embedded into the cover images *Pirate, Couple,* and *Lena* and extracted using the proposed watermark embedding and extraction schemes

Cover image / Attack	*Pirate*	*Couple*	*Lena*
Rotation 2°	0.9643	0.9489	0.9381
JPEG compression (Q = 10)	0.9974	0.9992	0.9993
Histogram Equalization	0.9665	0.9359	0.9371
Gaussian Noise ($\sigma^2 = 0.3$)	0.9870	0.9892	0.9875
Re-scaling (256-128-256)	0.9862	0.9831	0.9955
Contrast adjustment (-20%)	0.9886	0.9956	0.9841
Sharpening (80%)	0.8137	0.9078	0.8315
Gamma correction ($\gamma = 0.6$)	0.9937	0.9997	0.9998
Cropping (left and right sides by 25 columns)	0.9947	0.9970	0.9998
Blurring (using Gaussian filter)	0.9207	0.9284	0.9530
Median filter (3×3)	0.9805	0.9754	0.9909
Brightening (70%)	0.9991	0.9994	0.9990
Darkening (70%)	0.9800	0.9960	0.9979
Contrast adjustment (+20%)	0.9705	0.9939	0.9871

Table 3.4: Values of the correlation coefficient between the extracted and original watermark images. The watermark images *Pepper, Cameraman,* and *Boat* are embedded into the cover *Lena* and extracted using the proposed watermark embedding and extraction schemes

Watermark image / Attack	*Pepper*	*Cameraman*	*Boat*
Rotation 2°	0.9315	0.9271	0.9381
JPEG compression(Q=10)	0.9988	0.9990	0.9993
Histogram Equalization	0.9328	0.9316	0.9371
Gaussian Noise ($\sigma^2 = 0.3$)	0.9885	0.9875	0.9875
Re-scaling (256-128-256)	0.9940	0.9938	0.9955
Contrast adjustment (-20%)	0.9826	0.9818	0.9841
Sharpening (80%)	0.8233	0.8222	0.8315
Gamma correction ($\gamma = 0.6$)	0.9997	0.9998	0.9998
Cropping (left and right sides by 25 columns)	0.9998	0.9997	0.9998
Blurring (using Gaussian filter)	0.9426	0.9383	0.9530
Median filter (3×3)	0.9853	0.9876	0.9909
Brightening (70%)	0.9987	0.9984	0.9990
Darkening (70%)	0.9972	0.9966	0.9979
Contrast adjustment (+20%)	0.9859	0.9856	0.9871

Table 3.5: Performance, in terms of PSNR and normalized correlation coefficient, of the proposed and two other watermarking schemes against various types of attacks (cover image: *Lena,* watermark image: *Boat*)

Scheme	Proposed scheme	Scheme of Sushila *et al.* [37]	Scheme of Gupta *et al*. [41]
PSNR	**32**	24.26	24
Attack	Normalized correlation coefficient, NC		
Rotation 2°	**0.9381**	0.9292	0.8157
JPEG compression(Q=10)	0.9993	0.9981	**0.9998**
Histogram Equalization	**0.9371**	0.5983	0.7492
Gaussian Noise ($\sigma^2 = 0.3$)	**0.9875**	0.9767	0.9853
Re-scaling (256-128-256)	0.9955	0.9928	**0.9964**
Contrast adjustment (-20%)	**0.9841**	0.9006	0.9504
Sharpening (80%)	**0.8315**	0.8105	0.7898
Gamma correction ($\gamma = 0.6$)	**0.9998**	-0.7115	0.9460
Cropping (left and right sides by 25 columns)	**0.9998**	0.0155	0.9969
Blurring (using Gaussian filter)	**0.9530**	0.9350	0.9521
Translation (20,20)	**0.9955**	0.8693	0.7101
Brightening (70%)	**0.9990**	0.9408	0.9678
Darkening (70%)	**0.9979**	-0.9287	0.9927
Contrast adjustment (20%)	**0.9871**	0.9550	0.9816

Table 3.6 gives the execution times of running the proposed watermarking algorithms and that of running the schemes developed in [37] and [41]. A comparison of the proposed scheme with the scheme of [41] indicates that the use of the Arnold and anti-Arnold

transforms for the embedding and extraction of the watermark in the proposed scheme does not add to its computation time. However, the data scrambling using the Arnold transform in the proposed scheme significantly improves its robustness. It is also seen from this table the proposed scheme provides savings of 24.7% and 42% in the execution times of its embedding and extraction parts, respectively, over those of the scheme of [37] that also uses the Arnold transform.

Table 3.6: Execution times of running the proposed and two other watermarking schemes

Watermark embedding/extraction	Execution time in second		
	Proposed scheme	Scheme of Sushila *et al*. [37]	Scheme of Gupta *et al*. [41]
Embedding	2.145	2.848	2.061
Extraction	0.339	0.585	0.327

3.5 Summary

In this chapter, an Arnold transform integrated DCT-SVD based watermarking scheme has been proposed. The DCT coefficients of the cover image are zig-zag scanned and mapped in a zig-zag manner into four frequency subbands, LL, LH, HL, and HH, individually. The watermark image is scrambled using the operation of the Arnold transform, and then embedded into the singular value matrices of the four subbands of the array of the re-arranged DCT coefficients. The watermark image is extracted by reversing the steps of the watermark embedding.

Extensive experiments have been conducted using the proposed scheme and two other watermarking schemes. The performance of these schemes has been obtained in terms of the PSNR of the watermarked image measuring the imperceptibility of the watermark and the correlation coefficient between the original and extracted watermark images measuring the robustness of the watermarking schemes. The results of the experiments have demonstrated that the proposed watermarking scheme yields a performance superior to that of the other two schemes in preserving the perceptual quality of the cover image, and in providing an improved robustness against various types of attacks. It has also been shown that using the Arnold and anti-Arnold transforms for embedding and extraction of the watermark in the proposed algorithm does not add an overhead to its computation time.

Chapter 4

Visual Cryptography Based Digital Image Watermarking Scheme

4.1 Introduction

As discussed in Chapter 1, a variety of transform domain watermarking schemes have been proposed in order to provide robustness against different types of attacks and to preserve the perceptual quality of the cover image [14-18]. In an effort to improve the robustness of these schemes further, a number of watermarking schemes have been developed in which an SVD is performed on the transformed image and its singular values are altered by embedding a watermark. In [53], Naor and Shamir proposed a technique for binary image encryption called visual cryptography, where an image is divided into two unintelligible shares that individually do not carry any information about the encrypted image, and therefore, prevent unauthorized users from understanding its true content. An authorized user can obtain the encrypted image by simply stacking the two separately received shares. Visual cryptography is simple and the encrypted image is robust against attacks on individual shares [55, 56]. It is because of these properties, a number of visual cryptography based watermarking schemes [49-52], in which one of the two shares of a

binary image is used as a watermark, have been proposed. In [49], the authors have proposed a watermarking scheme based on visual cryptography in the spatial domain; however, the robustness of this scheme tends to decrease, as the JPEG compression ratio increases. In 2005, Hsu and Hou [50] proposed a sampling distribution of means (SDM) and visual cryptography based watermarking scheme. In this scheme, the mean value (μ) of all pixels in the cover image is first calculated. Then, a number of pixels are selected randomly from the cover image and the mean value of these selected pixels are computed ($\bar{X}$). Finally, the two shares are constructed using visual cryptography and the relation between the mean values. Since μ and $\bar{X}$ could be affected because of image processing, this method is vulnerable to some kinds of attacks. In [52], a watermarking scheme based on singular value decomposition and visual cryptography has been proposed. This scheme provides a good robustness against common image processing attacks, such as JPEG compression, noise addition, burring and filtering. A limitation of the schemes described in [49-52] is that they, in general, lack good robustness against geometrical attacks such as, rotation and translation.

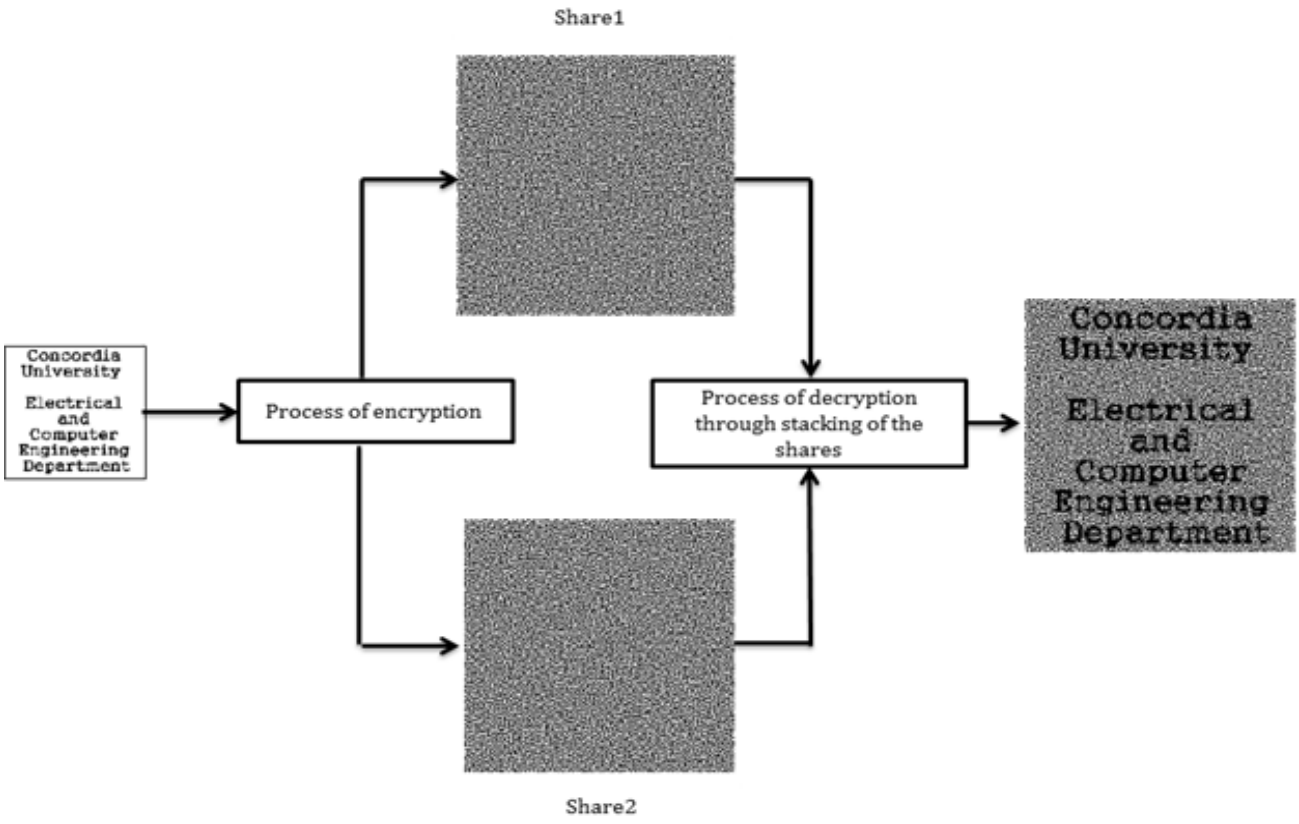
In this chapter, a DWT-SVD digital image watermarking scheme that makes use of visual cryptography is developed with a view to providing improved robustness against the various types of attacks while preserving the perceptual quality of the cover image.

In Section 4.2, visual cryptography is briefly discussed. In Section 4.3, a new DWT-SVD based image watermarking scheme that by making use of visual cryptography divides the watermark image into two shares prior to its embedding is proposed. In Section 4.4, experimental results demonstrating the performance of the proposed algorithm are

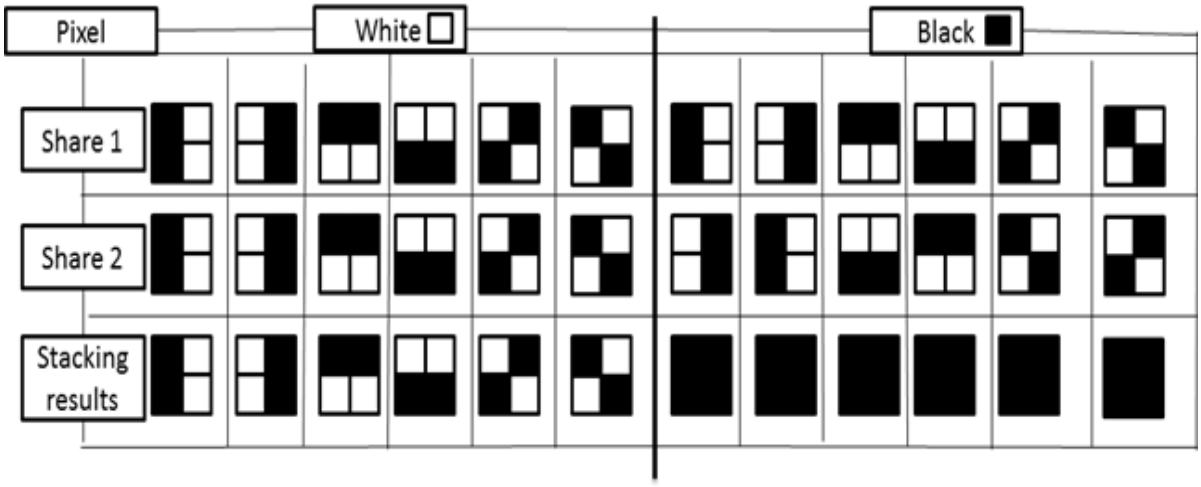
presented. The performance of the proposed algorithm is also compared with those of other existing algorithms. Section 4.5, summarizes the work presented in this chapter.

4.2 Visual Cryptography

Visual cryptography (VC) is a technique introduced by Naor and Shamir [53] for binary image encryption in such a way that the decryption process can be done directly by human visual system without the aid of computers. In this scheme, a binary watermark image of size $N \times N$ gets divided into two shares each of size $2N \times 2N$. The basic idea of the scheme is depicted in Figure 4.1(a). Each pixel of a binary watermark image is transformed into four pixels in a share. For a pixel, depending on whether it is a white or black pixel, the corresponding four pixels in each of the two shares are chosen randomly from one of the six possibilities as specified in Figure 4.1(b). Note that for a white pixel in the watermark image, the corresponding four pixels, two white and two black, in the two shares are identical. On the other hand, for a black pixel in the watermark image, the corresponding four pixels, still two white and two black, are complimentary in the two shares. For the purpose of decryption the two shares are stacked. The results of stacking four pixels of one share to the corresponding four pixels of the other share are also shown in Figure 4.1(a). Naor and Shamir's scheme is simple, since it does not require any complicated computation, and it is secure, since anyone who holds only one share is unable to reveal any information about the watermark image.



(a)



(b)

Figure 4.1: The basic scheme of Naor and Shamir [53] for visual cryptography. (a) Encryption and decryption. (b) Codebook.

4.3 Proposed Watermarking Algorithm

The proposed watermarking scheme consists of a watermark embedding process and a watermark extraction process.

4.3.1 Watermark embedding

Figure 4.2 shows a block diagram of the proposed watermark embedding scheme. In this scheme, the discrete wavelet transform is first applied to an $M \times M$ cover image A, to decompose the cover image into four subbands (LL, LH, HL, and HH). Then, the middle subbands LH and HL are made to undergo an SVD operation individually to obtain $A_k = U_k S_k V_k^T$ (k=1, 2). Next, an $N \times N$ binary watermark image is divided into two shares, $Share1$ and $Share2$, using visual cryptography [53]. $Share1$ is used as a watermark and $share2$ is saved as a secret key, to be used during the extraction process to recover the original watermark image. The $\frac{M}{2} \times \frac{M}{2}$ singular value matrices denoted by S_1 and S_2 of the middle subbands LH and HL, respectively, are then modified, individually, by adding to these matrices $share1$ of the watermark image to obtain $S_k + \alpha\ share1$, where α is a positive scaling factor. Note that for this addition to be possible, $N = \frac{M}{4}$. This subband image is singular value decomposed to obtain the singular value matrix S_{wk}^* of the watermarked subband. The subband watermarked DWT coefficients are obtained by augmenting S_{wk}^* with U_k and V_k^T as $A_k^* = U_k S_{wk}^* V_k^T$. Finally, the watermarked image is obtained by an inverse discrete wavelet transform operation on the entire wavelet coefficients image that contains two modified middle subbands and the two unmodified

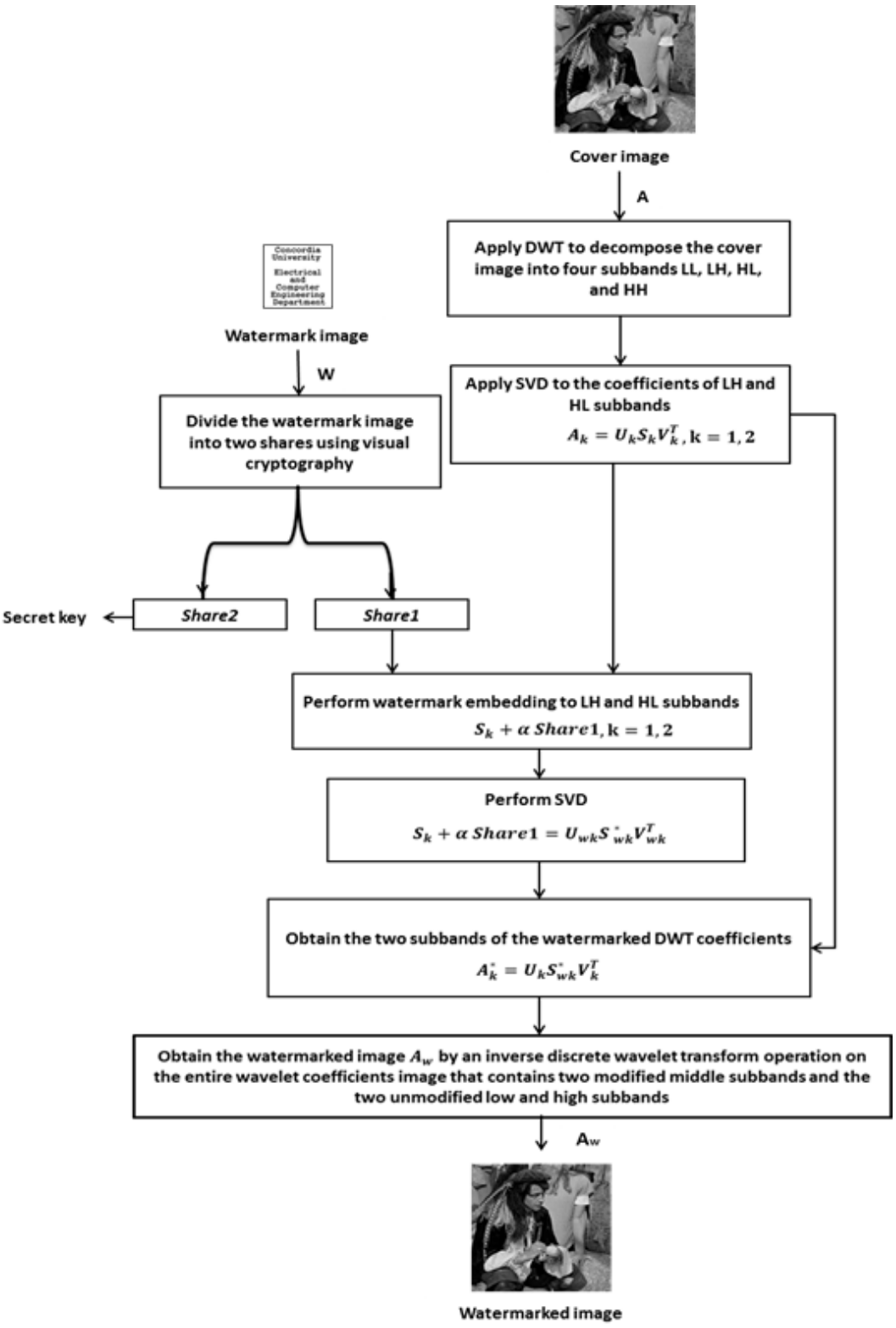


Figure 4.2: Block diagram of the proposed watermark embedding scheme.

low and high subbands. The proposed watermark embedding scheme is summarized as Algorithm 4.1.

Algorithm 4.1: Watermark embedding algorithm

Step 1	Decompose the cover image A into four subbands (LL, LH, HL, and HH) using the discrete wavelet transform.
Step 2	Perform SVD operation on the LHand HL subbands: $A_k = U_k S_k V_k^T, k = 1, 2.$
Step 3	Divide the watermark image W into two shares ($share1$ and $share2$) using visual cryptography.
Step 4	Modify the singular value matrices S_k corresponding to of LH and HL subbands through a watermark embedding as $S_k + \alpha\ share1$, where α is a scaling factor.
Step 5	Perform the SVD operation on the embedded subband singular value matrices as $S_k + \alpha share1 = U_{wk} S^*_{wk} V^T_{wk},\ k = 1, 2.$
Step 6	Augment the singular value matrix S^*_{wk} with U_k and V_k to obtain the watermarked subband DWT coefficients as $A^*_k = U_k S^*_{wk} V^T_k,\ k = 1, 2.$
Step 7	Obtain the watermarked image A_w by an inverse discrete wavelet transform operation on the entire wavelet coefficients image that contains two modified middle subbands and the two unmodified low and high subbands.

4.3.2 Watermark extraction

Figure 4.3 shows a block diagram of the proposed watermark extraction scheme. In this scheme, the discrete wavelet transform operation is applied to the watermarked (possibly attacked) image A_w, to decompose the watermarked image into four subbands (LL, LH, HL, and HH). Then, the LH and HL subbands are made to undergo an SVD operation individually. Next, the singular value matrix of each subband (LH and HL) $S'_{wk}(k = 1, 2)$ is augmented with $U_{wk}$and V^T_{wk} to obtain $D'_k = U_{wk} S'_{wk} V^T_{wk}$.

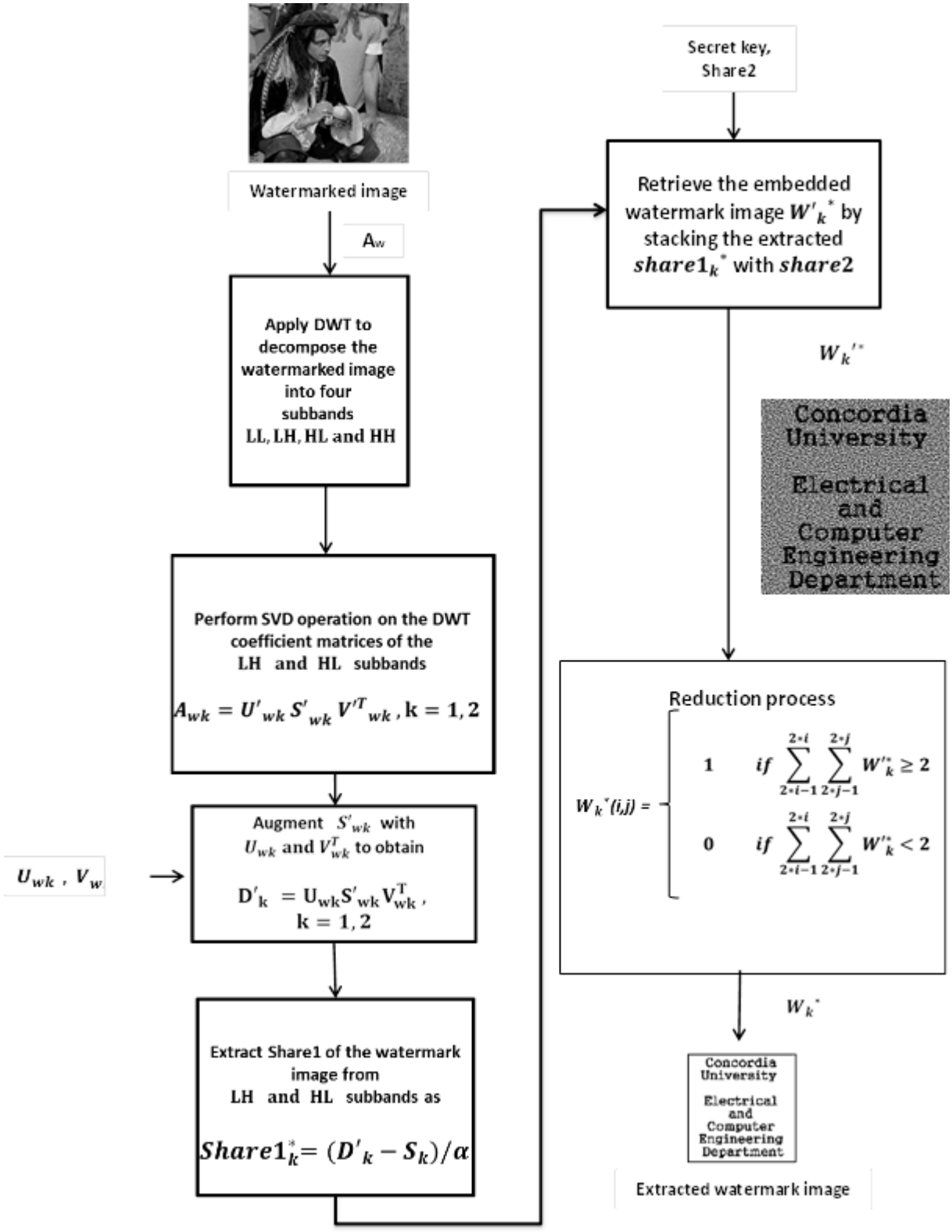


Figure 4.3: Block diagram of the proposed watermark extraction scheme.

$Share1_k^*$ of the watermark image is extracted from each of the two middle subbands as $share1_k^* = (D'_k - S_k)/\alpha$, followed by stacking it with $share2$ to retrieve the embedded watermark image $W'_k{}^*$. Finally, a size reduction process is performed on $W'_k{}^*$ to obtain the watermark image $W_k{}^*$. It should be noted that $Share2$ is used as secrete key during the extraction process. The proposed steps of the watermark extraction scheme are summarized as Algorithm 4.2.

Algorithm 4.2: Watermark extraction algorithm

Step 1	Decompose the watermarked image A_w into four subbands (LL, LH, HL and HH) using the discrete wavelet transform.
Step 2	Apply SVD operation on the matrices representing the coefficients of LH and HL subband: $A_{wk} = U'_{wk} S'_{wk} V'^T_{wk}$, k = 1, 2.
Step 3	Augment S'_{wk} with U_{wk} and V_{wk}^T to obtain: $D'_k = U_{wk} S'_{wk} V_{wk}^T$, where U_{wk} and V_{wk}, are as obtained in Step5 in Algorithm 4.1.
Step 4	Extract $share1$ of the watermark image from the LH and HL subbands as $share1_k^* = (D'_k - S_k)/\alpha$, k = 1, 2.
Step 5	Retrieve the embedded watermark image $W'_k{}^*$ (k = 1, 2) by staking the extracted $share1_k^*$ with $share2$.
Step 6	Perform the reduction process to obtain the original-sized watermark image $W_k{}^*$ as

$$W_k{}^*(i,j) = \begin{cases} 1 & if \sum_{2*i-1}^{2*i} \sum_{2*j-1}^{2*j} W'^*_k \geq 2 \\ 0 & if \sum_{2*i-1}^{2*i} \sum_{2*j-1}^{2*j} W'^*_k < 2 \end{cases}$$

4.4 Experimental Results and Discussion

The proposed watermarking scheme is implemented using MATLAB (R2012a) on a PC with a1.6-GHz AMD E-350 processor, 3-GB RAM, and Microsoft Windows 7 operating system. Extensive experiments are conducted to demonstrate the performance of the proposed watermarking scheme. Three gray-scale cover images, *Pirate*, *Boat*, and *Elaine,* and a binary watermark image, as depicted in Figure 4.4, are used in these experiments. The size of each cover image is 512 × 512 and that of the watermark image is 128 × 128.

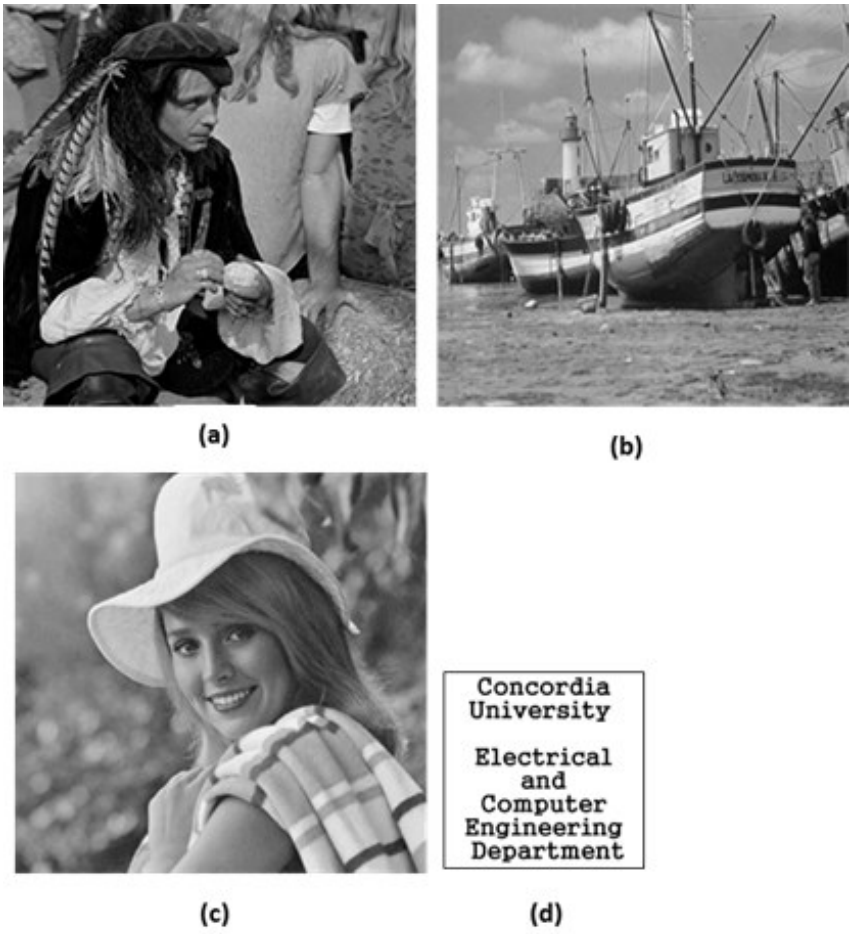


Figure 4.4: Cover images: (a) *Pirate*, (b) *Boat*, and (c) *Elaine*. (d) Watermark image.

Since the middle subbands(LH and HL) have very similar wavelet coefficients values, for simplicity, we use one scaling factor for both. In all experiments, the scaling factor is set to 0.02 for watermark embedding of the LH and HL subbands. Figure 4.5 shows an example of a watermarked image and the extracted watermark image obtained by applying the proposed scheme of watermarking. Figures 4.5 (a) and (b) show, respectively, the original cover image *Pirate* and the original binary watermark image, and Figures 4.5 (c) and (d) show, respectively, the watermarked image and the watermark images extracted from the un-attacked watermarked image of Figure 4.5 (c) using the proposed watermarking scheme. It is seen from this figure that the embedded watermark dose not degrade the perceptual quality of the cover image, and the proposed scheme is able to extract the watermark images successfully from the un-attacked watermarked image.

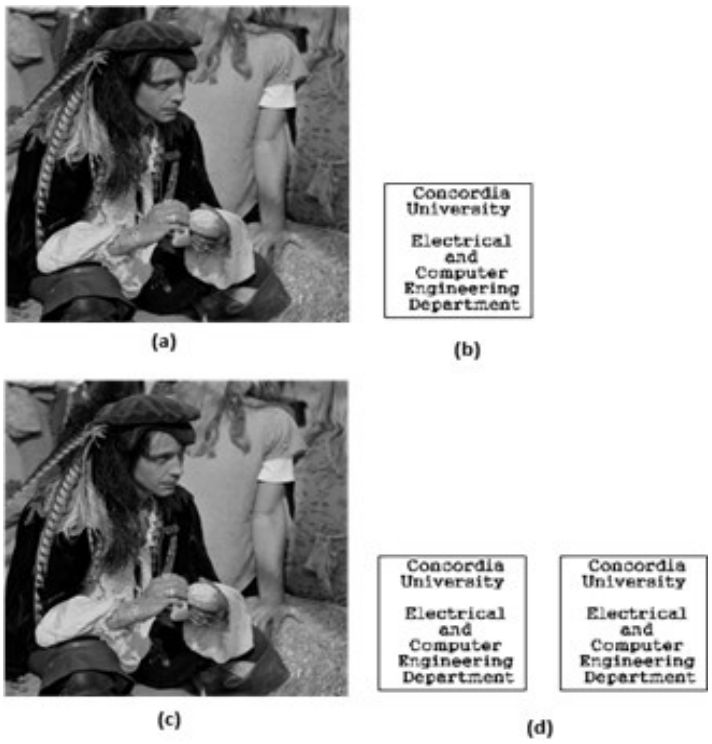


Figure 4.5: (a) Cover image, *Pirate*. (b) Watermark image. (c) Watermarked image. (d) Watermark images extracted from the LH and HL subbands of the watermarked image.

For objective evaluation of the perceptual quality of watermarked image, the peak signal-to-noise ratio (PSNR) defined in (3.3) is used. Table 4.1 gives the PSNR values of the various watermarked images obtained by using the proposed watermarking scheme. This table clearly indicates that the embedded watermark does not degrade the perceptual quality of the cover image, and thus the proposed embedding scheme guarantees the imperceptibility of the watermark.

Table 4.1: The PSNR values (in dB) of various watermarked images obtained by using the proposed watermarking scheme

Cover image	*Pirate*	*Boat*	*Elaine*
PSNR	51.55	53.1	47.67

To investigate the robustness of the proposed watermarking scheme, each watermarked image obtained by using the proposed watermark embedding scheme is subjected to different types of attacks. The attacks used in our robustness study are JPEG compression, Gaussian noise, cropping, rescaling, translation, rotation, brightness adjustment, gamma correction, blurring, contrast adjustment, histogram equalization, and median filtering. After each of these attacks, we extract two watermarks from the middle subbands, LH and HL, using the proposed watermark extraction scheme and then select the one having the largest normalized correlation coefficient between the extracted and the original watermark images. The normalized correlation (NC) between the original $N \times N$ watermark image W and the extracted watermark image W^* is given by [50-52]

$$NC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} \overline{p_{i,j} \oplus p_{i,j}^*}}{N \times N} \tag{4.2}$$

where $p_{i,j}$ and $p^*_{i,j}$ denotes the pixel values in the original watermark image and the extracted watermark image, respectively, and $\oplus$ denotes the exclusive-OR operation.

Figure 4.6 shows the original cover image, *Pirate,* and the original watermark image to be embedded in the cover image using the proposed watermarking scheme. Figures 4.7-4.21 show the watermarked *Pirate* images, each subjected to one type of attack, and the watermark images extracted from the attacked images. It is seen from these figures that the proposed scheme effectively resists different types of attacks and is able to extract the watermark images with high perceptual quality. It is noted that the watermark image extracted from some of the attacked images, for example those attacked by Gaussian noise, histogram equalization and rotation, have a visible diagonal line. This artifact for certain attacks is typical of the methods in which the watermark is embedded into the singular values [54]. However, such an artifact has little effect on the legibility of the binary watermark text utilized in the proposed visual cryptography based watermarking scheme.

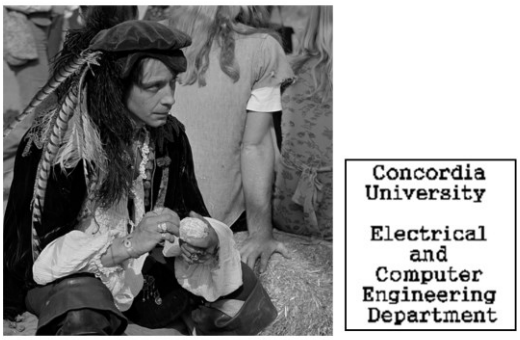


Figure 4.6: (a) Original cover image, *Pirate*. (b) Original watermark image.

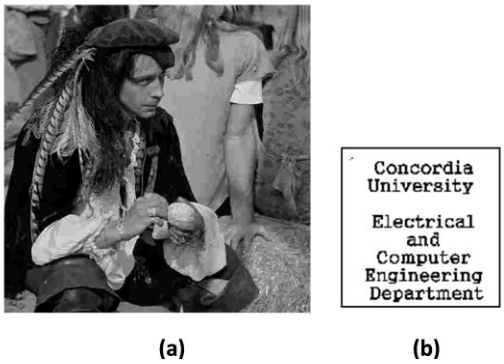


Figure 4.7: (a) Watermarked *Pirate* image attacked by JPEG compression (Q=10). (b) Extracted watermark image.

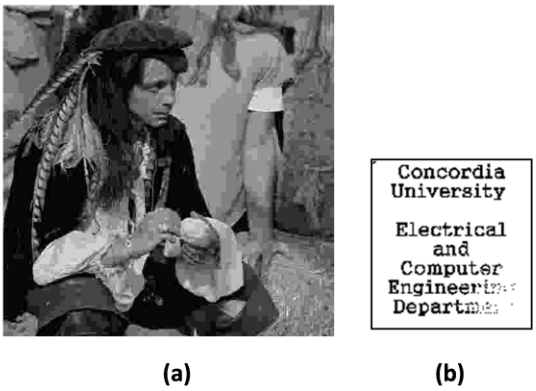


Figure 4.8: (a) Watermarked *Pirate* image attacked by JPEG compression (Q = 5). (b) Extracted watermark image.

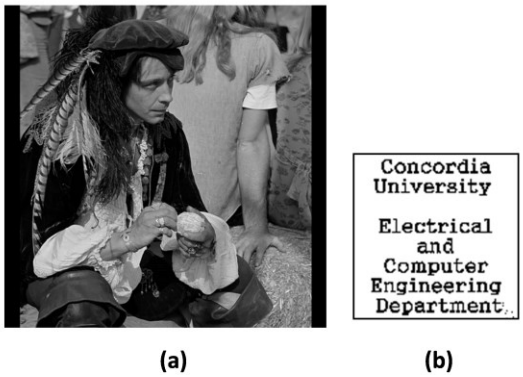


Figure 4.9: (a) Watermarked *Pirate* image attacked by cropping (left and right sides by 25 columns each). (b) Extracted watermark image.

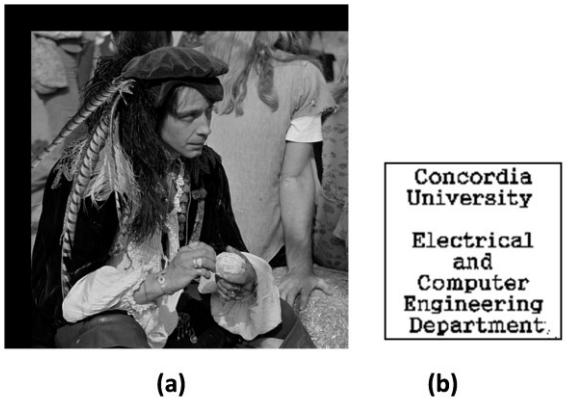


Figure 4.10: (a) Watermarked *Pirate* image attacked by translation (horizontally and vertically by 40 lines each). (b) Extracted watermark image.

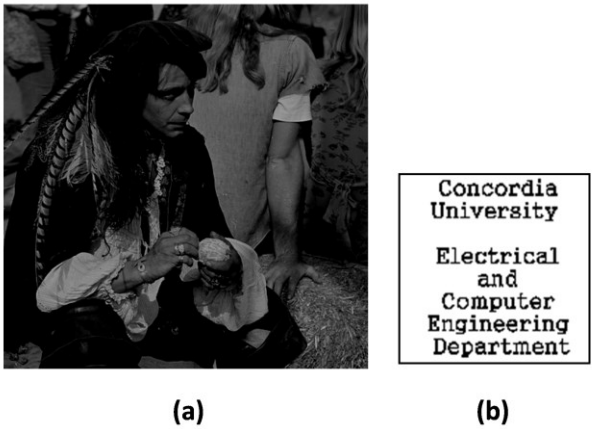


Figure 4.11: (a) Watermarked *Pirate* image attacked by darkening (70%). (b) Extracted watermark image.

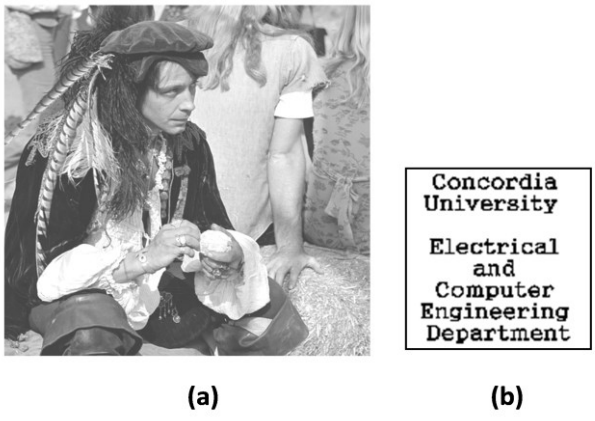


Figure 4.12: (a) Watermarked *Pirate* image attacked by brightening (70%). (b) Extracted watermark image.

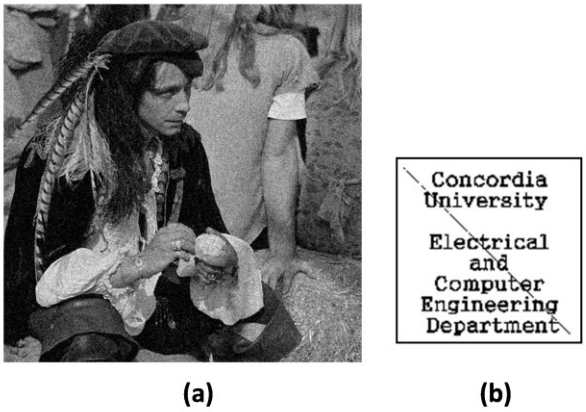


Figure 4.13: (a) Watermarked *Pirate* image attacked by Gaussian noise contamination (σ^2 = 0.3). (b) Extracted watermark image.

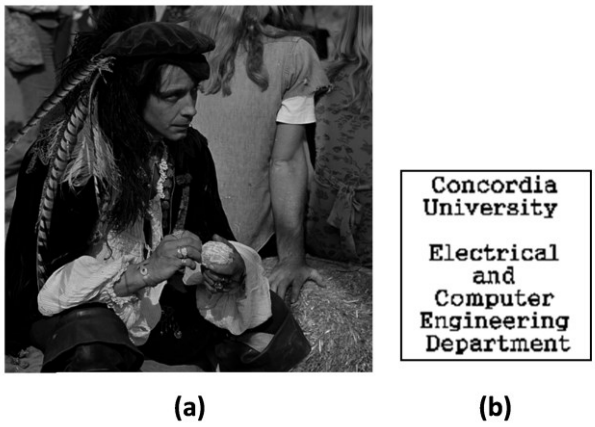


Figure 4.14: (a) Watermarked *Pirate* image attacked by gamma correction (γ = 0.6). (b) Extracted watermark image.

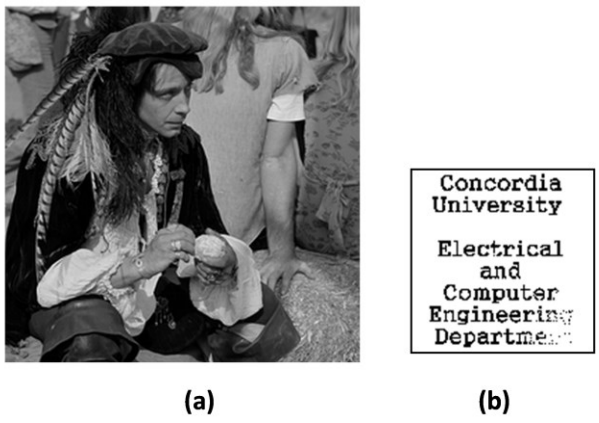
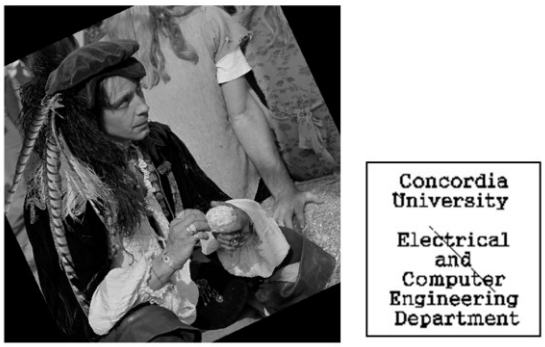
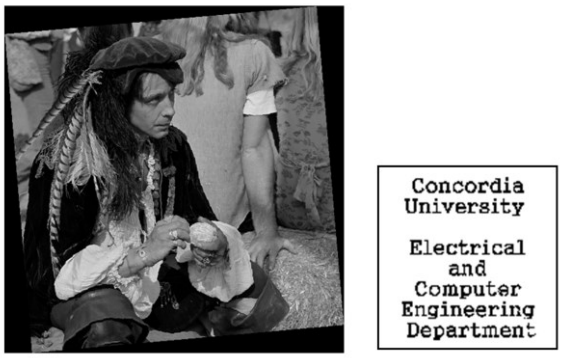


Figure 4.15: (a) Watermarked *Pirate* image attacked by re-scaling (512-256-512). (b) Extracted watermark image.



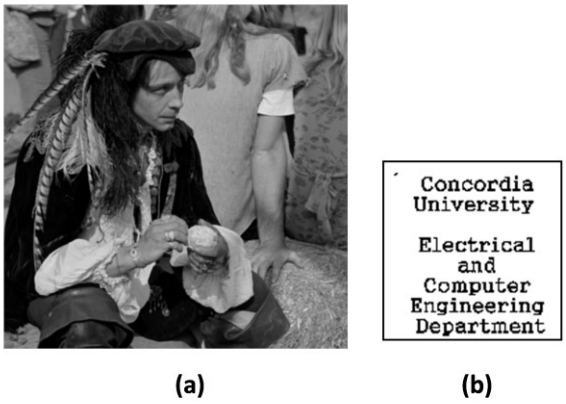
(a) (b)

Figure 4.16: (a) Watermarked *Pirate* image attacked by rotation (25°). (b) Extracted watermark image.



(a) (b)

Figure 4.17: (a) Watermarked *Pirate* image attacked by rotation (rotated by 5° and restored to the original size). (b) Extracted watermark image.



(a) (b)

Figure 4.18: (a) Watermarked *Pirate* image attacked by blurring using 3×3 Gaussian filter with $\sigma = 1$. (b) Extracted watermark image.

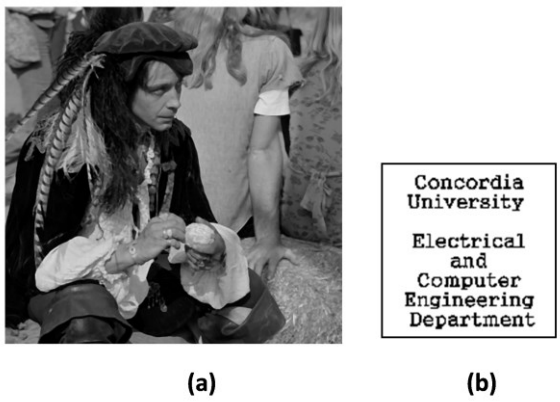


Figure 4.19: (a) Watermarked *Pirate* image attacked by median filtering (3×3). (b) Extracted watermark image.

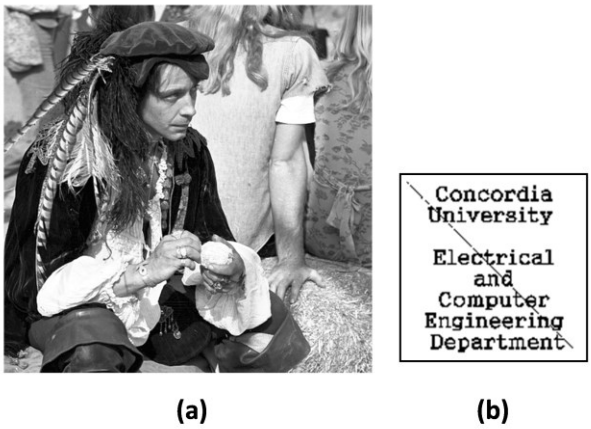


Figure 4.20: (a) Watermarked *Pirate* image attacked by histogram equalization. (b) Extracted watermark image.

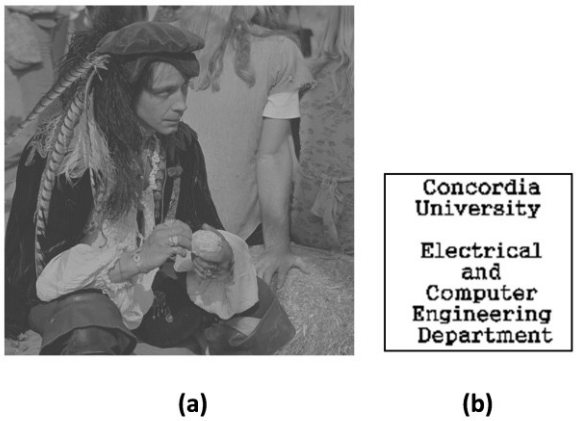


Figure 4.21: (a) Watermarked *Pirate* image attacked by contrast adjustment (decreased by 60%). (b) Extracted watermark image.

In order to provide an objective analysis of the robustness of the proposed watermarking scheme, the normalized correlation coefficient between the extracted and the original watermark images is computed. Table 4.2 gives the values of the correlation coefficient using the cover images, *Pirate, Elaine,* and *Boat,* and the same watermark image. It is seen from this table that the values of the correlation coefficient are invariably larger than 0.9 for the various attacks regardless of the cover images used in our experiments.

Table 4.2: Values of the correlation coefficient between the extracted and original watermark images. The watermark image is embedded into the cover images *Pirate, Elaine,* and*Boat,* and extracted using the proposed watermark embedding and extraction schemes

Cover image / Attack	*Pirate*	*Elaine*	*Boat*
Rotation 5°	0.9998	0.9987	0.9997
Rotation 25°	0.9977	0.9955	0.9953
JPEG compression (Q = 5)	0.9861	0.9265	0.9832
JPEG compression (Q = 10)	0.9996	0.9611	0.9983
Median filtering (3×3)	0.9998	0.9990	0.9998
Histogram equalization	0.9949	0.9948	0.9948
Contrast adjusting (-60%)	0.9998	0.9998	0.9998
Gaussian noise (σ^2 = 0.3)	0.9948	0.9948	0.9946
Gamma correction (γ = 0.6)	0.9998	0.9969	0.9972
Lighting (70%)	0.9999	0.9999	0.9998
Darkening (70%)	0.9998	0.9999	0.9999
Translation (40,40)	0.9995	0.9998	0.9998
Cropping (left and right sides by 25 columns)	0.9993	0. 9998	0.9996
Re-scaling (512-256-512)	0.9905	0.9680	0.9990
Blurring (using Gaussian filtering)	0.9996	0.9995	0.9662

We also implement the DWT-SVD based watermarking scheme [9], the VC-SDM based watermarking scheme [50] and the VC-SVD image watermarking scheme [52], in order to compare the performance of the proposed scheme with these schemes in terms of the correlation coefficient between the original and extracted watermark images measuring the robustness of the watermarking schemes. The performance comparison is given in Table 4.3. It is seen from this table that the proposed watermarking scheme outperforms the other three algorithms in providing higher robustness against the various types of attacks. A comparison of the proposed scheme with the scheme of [9] that like the proposed scheme uses the DWT and SVD transforms but does not use visual cryptography, indicates that the use of visual cryptography in the watermark embedding process in the proposed scheme significantly improves its robustness.

Finally, we compare the watermarking scheme (Scheme 2) presented in this chapter with the Arnold transform integrated DCT-SVD based watermarking scheme (Scheme 1) proposed in Chapter 3. For this purpose, we use *Pirate* as the cover image and the image of Figure 4.4 (d) as the watermark image and compare the performance of the two schemes against the various types of attacks by computing the values of correlation coefficients between the original and the extracted watermark images. The results are given in Table 4.4. It is seen from these results that the two schemes provide almost the same robustness against the various types of attacks on the watermarked images. As an example of visual comparison of the performance of the two proposed schemes, Figure 4.22 shows the original *Pirate* image and the versions of this image watermarked by the two proposed schemes, as well as the corresponding watermarked images attacked by JPEG compression, histogram equalization and translation and the watermark images extracted by using the

two proposed schemes. It is seen from this figure that the two proposed schemes effectively resist the various types of attacks leading to the extraction of the watermark images with high perceptual quality.

Table 4.3: Performance, in terms of normalized correlation coefficient, of the proposed and three other watermarking schemes against various types of attacks (cover image:*Pirate*)

Scheme / Attack	Proposed scheme	Scheme of Lai *et al*. [9]	Scheme of Wang *et al*. [52]	Scheme of Hsu *et al*. [50]
Rotation 5°	**0.9998**	0.9445	0.8406	0.6528
Rotation 25°	**0.9977**	0.8475	0.6355	0.5391
JPEG compression (Q = 5)	**0.9861**	0.9729	0.9844	0.9177
JPEG compression (Q = 10)	**0.9996**	0.9905	0.9871	0.9397
Median filtering (3×3)	**0.9998**	0.9833	0.9949	0.9586
Histogram equalization	0.9949	**0.9991**	0.9802	0.9688
Contrast adjusting (-60%)	**0.9998**	0.9834	0.9724	0.9959
Gaussian noise (σ^2 = 0.3)	**0.9948**	0.8912	0.9883	0.8949
Gamma correction (γ = 0.6)	**0.9998**	0.9960	0.9500	0.9315
Brightening (70%)	**0.9999**	0.9975	0.9697	0.9826
Darkening (70%)	**0.9998**	0.9898	0.9277	0.8873
Translation (40,40)	**0.9995**	0.9967	0.6052	0.5619
Cropping (left and right sides by 25 columns)	**0.9993**	0.9812	0.9475	0.8423
Re-scaling (512-256-512)	0.9905	0.9358	**0.9954**	0.9545
Blurring (using Gaussian filtering)	**0.9996**	0.9939	0.9961	0.9544

It should be pointed out that in the scheme of Chapter 3, any gray-level image can be used as watermark, in contrast to only binary watermark images in the visual cryptography based watermarking scheme proposed in this chapter. However, the second proposed scheme provides security to the content of the watermark.

Table 4.4: Performance comparison of the two proposed watermarking schemes , in terms of normalized correlation coefficient, against various types of attacks (cover image:*Pirate*)

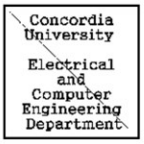
Attack	Scheme 1 (Chapter 3)	Scheme 2 (Chapter 4)
Rotation 5°	0.9953	0.9998
Rotation 25°	0.9959	0.9977
JPEG compression (Q = 5)	0.9955	0.9861
JPEG compression (Q = 10)	0.9955	0.9996
Median filtering (3×3)	0.9957	0.9998
Histogram equalization	0.9995	0.9949
Contrast adjusting (-60%)	0.9927	0.9998
Gaussian noise (σ^2 = 0.3)	0.9980	0.9948
Gamma correction (γ=0.6)	0.9992	0.9998
Brightening (70%)	1.0000	0.9999
Darkening (70%)	0.9975	0.9998
Translation (40,40)	0.9942	0.9995
Cropping (left and right sides by 25 columns)	1.0000	0.9993
Re-scaling (512-256-512)	0.9958	0.9905
Blurring (using Gaussian filtering)	0.9957	0.9996


Watermarked images



Watermarked *Pirate* images attacked by JPEG compression (Q = 5)





Watermarked *Pirate* images attacked by histogram equalization



Watermarked *Pirate* images attacked by translation (horizontally and vertically by 40 lines each)

(a) (b)

Figure 4.22: Watermarked and attacked watermarked *Pirate* images using (a) Scheme 1 and (b) Scheme 2.

4.5 Summary

In this chapter, a DWT- SVD digital image watermarking scheme that makes use of visual cryptography has been proposed. The cover image is decomposed into four subbands, LL, LH, HL and HH, using the discrete wavelet transform. The watermark image is divided into two shares, share1 and share2, using visual cryptography, and then share1 of the watermark image is embedded into the singular value matrices of the middle subbands, LH and HL, of the transformed cover image. The watermark image is extracted by reversing the steps of the watermark embedding, followed by stacking the extracted share1 with share2 to retrieve the watermark image. Finally, a size reduction process is performed to restore the original size of the watermark image.

Extensive experiments have been conducted to evaluate the performance of the proposed scheme. The results of the experiments have demonstrated that the proposed embedding scheme ensures the imperceptibility of the watermark and that the embedded watermark does not degrade the perceptual quality of the cover image. It has also been shown that the proposed extraction scheme is able to extract the watermark images successfully from the watermarked image. The objective quality of the extracted watermark image has been measured in terms of the correlation coefficient between the original and extracted watermark image. The performance of the proposed scheme has also been compared with three other watermarking schemes. The results of comparison have demonstrated that the proposed watermarking scheme effectively resists the various types of attacks and yields a performance superior to that of the other three schemes in extracting the watermark image from the attacked watermarked images.

Chapter 5

Conclusion

5.1 Concluding Remarks

Digital watermarking techniques have attracted considerable attention as means for hiding the owner's information in the multimedia to provide a proof of their ownership. A variety of digital image watermarking schemes have been proposed. These schemes either provide good imperceptibility of the watermark without sufficient resilience to certain types of attacks or provide good robustness against various types of attacks at the expense of a degraded perceptual quality of the cover image. The objective of this thesis has been to develop efficient watermarking schemes with performance that is superior to those of others in terms of their robustness against the various types of attacks while preserving the perceptual quality of the cover image. With this objective, in this thesis two new digital image watermarking schemes have been proposed.

In the first scheme, a DCT-SVD based image watermarking that makes use of the Arnold transform has been developed. In this scheme, the zig-zag scanned DCT coefficients of the cover image are mapped into four frequency subbands. The watermark image is scrambled using the operation of the Arnold transform, and then embedded into the singular value

matrices of the four subbands. The watermark image is extracted by reversing the steps of the watermark embedding. Experimental results have been presented to show that the proposed watermarking scheme provides a superior performance in terms of robustness against various types of attacks while preserving the perceptual quality of the cover image. It has also been shown that using the Arnold and anti-Arnold transforms for embedding and extraction of the watermark in the proposed algorithm does not add an overhead to its computation time. However, the data scrambling using the Arnold transform in the proposed scheme significantly improves its robustness against the various types of attacks.

In the second scheme, a visual cryptography based digital image watermarking has been developed. In this scheme, the cover image is decomposed into the LL, LH, HL and HH subbands using the discrete wavelet transform. The watermark image is divided into two shares using visual cryptography, and then one of the shares is embedded into the singular value matrices of the middle subbands, LH and HL, of the transformed cover image. The other share is saved as a secret key and used during the extraction process to recover the watermark image. The watermark image is extracted by reversing the steps of the watermark embedding, followed by stacking the extracted share with the other share to retrieve the watermark image. Finally, a size reduction process is performed to restore the original size of the watermark image. The experimental results have shown that the proposed watermarking scheme yields watermarked images with a perceptual quality very similar to that of the original cover image and that it effectively resists the various types of attacks by allowing the extraction of the watermark images with high perceptual quality.

Finally, it should be pointed out that in the first watermarking scheme proposed in this thesis, any gray-level image can be used as a watermark. In contrast, only binary watermark images can be used in the second proposed scheme. However, this second scheme is capable of providing more security to the content of the watermark.

5.2 Scope for Further Research

In this study, two non-blind watermarking schemes that provide improved robustness against the various types of attacks, while preserving the perceptual quality of the cover image, have been developed. Specifically in both the schemes, the singular value matrices of the original cover images are required for the extraction of the watermark. A study on developing of robust blind watermarking schemes based on the ideas proposed in this thesis could also be undertaken as a future study.

References

[1] I.J. Cox, M.L. Miller, and J.A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufman, 2001.

[2] V. Potdar, S. Han, and E. Chang, "A Survey of Digital Image Watermarking Techniques," in *Proc. of the 3rd Inter. IEEE Conf. on Industrial Informatics*, Perth, Australia, Aug. 2005, pp. 709-716.

[3] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal Electronic Imaging*, vol. 7, no. 2, pp. 326-332, Apr. 1998.

[4] R.B. Wolfgang and E.J. Delp, "A watermark for digital images," in *Proc. Int. Conf. Image Process.*, Lausanne, Switzerland, Sep. 1996, vol. 3, pp. 219–222.

[5] R. Liu and T. Tan, "A SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[6] F. Liu and Y. Liu. "A watermarking algorithm for digital image based on DCT and SVD." in *Proc. Cong. on Image and Signal Process., CISP '08*, Sanya, Hainan, May 2008, vol. 1, pp. 380-383.

[7] S. Alexander, D. Scott, and M.E. Ahmet, "Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies," in *Proc. European Signal Processing Conf.*, Antalya, Turkey, 2005.

[8] E. Ganic and A.M. Eskicioglu, "Robust DWT-SVD domain image watermarking: Embedding data in all frequencies," in *Proc. AMC Multimedia and Security Workshop*, pp. 166–174, 2004.

[9] C.C. Lai and C.C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. on instrumentation and measurement*, vol. 59, no. 11, pp. 3060-3063, Nov. 2010.

[10] M. Herandez, M. Miyatake, and H. Meana, "Analysis of a DFT-based watermarking algorithm," in *Proc. of the IEEE 2nd Int. Conf. on Electrical and Electronics Eng*., Sep. 2005, pp. 44-47.

[11] Y. Xing and J. Tan, "A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation," in *Proc. Second IEEE Workshop on Digital Media and its*

Application in Museum and Heritage, Chongqing, China, Dec. 2007, pp. 3–8.

[12] I.J. Cox, J. Killian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.

[13] S.D. Lin and C.F. Chen, "A robust DCT-based watermarking for copyright protection," *IEEE Trans. on Consumer Electronics*, vol. 46, no. 3, pp. 415-421, Aug. 2000.

[14] F. Deng and B. Wang, "A novel technique for robust image watermarking in the DCT domain," in *Proc. IEEE Int. Conf. on Neural Networks and Signal Processing*, Nanjing, China, Dec. 2003, vol. 2, pp. 1525-1528.

[15] F. Gu, Z. Lu and J. Pan "Multipurpose Image Watermarking in DCT Domain using Subsampling," in *Proc. 2005 IEEE Inter. Symposium on Circuits and Systems*, Kobe, Japan, May 2005, vol. 5, pp. 4417-4420.

[16] X. Xia, C. Boncelet, and G. Arce, "A multi resolution watermark for digital images," in *Proc. IEEE Int. Conf. Image Processing,* Santa Barbara, CA, Oct. 1997, vol. 1, pp. 548–551.

[17] R. Mehul and R. Priti, , "Discrete wavelet transform based multiple watermarking scheme", in *Proc. Conf. on Convergent Technologies for Asia-Pacific Region (TENCON),* Oct. 2003, vol. 3, pp. 935 - 938.

[18] P. Tao and A.M. Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain," in *Internet Multimedia Management Systems, Proc. SPIE*, vol. 5601, pp. 133-144, Oct. 2004.

[19] A. Al-Haj, "Combined DWT-DCT digital image watermarking," *Journal of Computer Science,* vol. 3, no. 9, pp. 740-746, 2007.

[20] J.J. Eggers, J.K. Su, and B. Girod, "Robustness of a blind image watermarking scheme," in *Proc. IEEE Int. Conf. Image Processing*, Vancouver, Canada, Sep. 2000, vol. 3, pp. 17-20.

[21] E. Elbasi and A. Eskicioglu, "A DWT-based robust semi-blind image watermarking algorithm using two bands," in *Proc. IS&T/SPIE, Security, Steganography, and Watermarking Multimedia Contents VIII Conf.*, San Jose, CA, Jan. 2006.

[22] E. Lin and E.J. Delp, "A review of fragile image watermarks," in *Proc. ACM Multimedia and Security Workshop*, Orlando, Florida, Nov. 1999, pp. 35–40.

[23] J.M. Shieh, D.C. Lou and M.C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," *Computer Standards & Interfaces*, vol. 28, pp. 428–440, April 2006.

[24] X. Qi and X. Xin, "A quantization-based semi-fragile watermarking approach for image content authentication," *Journal Vis. Commun. Image R.,* vol. 22, pp. 187–200, 2011.

[25] S.J. Lee and S.H. Jung, "A survey of watermarking techniques applied to multimedia," in *Proc. IEEE Int. Symp. Industrial Electronics (ISIE)*, Pusan, Korea, June. 2001, vol. 1, pp. 272–277.

[26] V.C. Klema and A.J. Laub, "The singular value decomposition: Its computation and some applications," *IEEE Trans. Autom. Contr.,* vol. AC-25, no. 2, pp. 164-176, Apr. 1980.

[27] E. Lars, *Matrix Methods in Data Mining and Pattern Recognition*. Philadelphia: SIAM, 2007.

[28] H. Yanai , K. Takeuchi, and Y. Takane, *Projection Matrices, Generalized Inverse Matrices, and Singular Value Decomposition.* New York: Springer Science and Business Media, 2011.

[29] F. Pérez-González and J.R. Hernández, "A tutorial on digital watermarking," in *Proc. IEEE Annu. Carnahan Conf. Security Technol.*, 1999, pp. 286–292.

[30] C.I. Podilchuk and E.J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.

[31] Z.D. Zhou, B. Tang, and X.H. Liu, "A block-SVD based image watermarking method," in *Proc. of the 6thWorld Congress on Intelligent Control and Automation*, Dalian, China, June 2006, vol. 2, pp.10347-10351.

[32] S.P. Mohanty, K.R. Ramakrishnan, and M.S. Kankanhalli, "A DCT domain visible watermarking technique for images," in *Proc. IEEE Int. Conf. Multimedia and Expo.*, New York, USA, Aug. 2000, vol. 2, pp. 1029–1032.

[33] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing,* vol. 66, no. 3, pp. 385–403, May 1998.

[34] S.G. Mallat, "A theory for multi resolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Machine Intell.,* vol. 11, pp. 674-693, July. 1989.

[35] Y. Wang and T. Li, "Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System," in *Proc*. *Intelligent System Design and Engineering Application International Conference*, Changsha, China, Oct. 2010*,* vol. 2, pp. 449-451.

[36] Z. Liu, M. Gong, Y. Dou, F. Liu, S. Lin, M. Ashfaq Ahmad, J. Dai, and S. Liu, "Double image encryption by using Arnold transform and discrete fractional angular transform," *Optics and Lasers in Engineering*, vol. 50, no.2, pp. 248-255, Feb. 2012.

[37] K. Sushila, V. Maheshkar, S. Agarwal, and K. Srivastava, "DWT-SVD based robust image watermarking using Arnold map," *Inter. Journal of Information Technology,* vol. 5, no. 1, pp. 101-105, June 2012.

[38] V. Arnold and A. Avez, *Ergodic Problems in Classical Mechanics.* New York: Benjamin, 1968.

[39] F.J. Dyson and H. Falk, "Period of a discrete cat mapping," *Amer. Math. Mon.*, vol. 99, pp. 603–624, Aug.-Sept. 1992.

[40] L. Wu, J. Zhang, W. Deng and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," in *Proc. Information Science and Engineering Inter. Conf.*, Nanjing, China, Dec. 2009, pp. 1164-1167.

[41] P.K. Gupta and S.K. Shrivastava, "Improved RST-Attacks Resilient Image Watermarking Based on Joint SVD-DCT," in *Proc. Int. Conf. on Computer and Communication Technology*, Allahabad, India, Sep. 2010, pp. 46-51.

[42] C.C. Chang, K.F. Hwang, and M.S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics," *IEEE Proc.* on *Vision, Image, and Signal Processing.,* vol. 149, no. 1, pp. 43-50, Feb. 2002.

[43] C.C. Chang, C.C. Lin, and Y.S. Hu, "An SVD oriented watermark embedding scheme with high qualities for the resorted images," *Inter. Journal of Innovative Computing, Information and Control*, vol. 3, pp. 609-620, June 2007.

[44] M.S. Emami, G.B. Sulong, and J.M. Zain, "A New Performance Trade-Off Measurement Technique for Evaluating Image Watermarking Schemes," *Communications in Computer and Information Science*, Springer, vol. 179, pp. 567-580, June 2011.

[45] C. Yaw Low, A.B. Jin Teoh and C. Tee, "Fusion of LSB and DWT Biometric Watermarking for Offline Handwritten Signature," in *Proc. of Congress on Image and*

Signal Processing, Sanya, China, May 2008, vol. 5, pp. 702-708.

[46] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," in *Proc. 4th IEEE Int. Conf. Image Processing '97*, Santa Barbra, CA, Oct. 1997, vol. 1, pp. 544–547.

[47] S.H. Wang and Y.P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 154–165, Feb. 2004.

[48] C. Yongchang, W. Yu, and J. Feng, "A digital watermarking based on discrete fractional fourier transformation DWT and SVD," in *Proc. Control and Decision Conf.*, Taiyuan, China, May 2012, pp. 1383-1386.

[49] C.C. Chang and J.C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recognit. Lett.*, vol. 23, no. 8, pp. 931–941, June 2002.

[50] C.S. Hsu and Y.C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Optical Engineering,* vol. 44, no. 7, Jul. 2005.

[51] T.H. Chen, G. Horng, and W.B. Lee, "A publicly verifiable copyright proving scheme resistant to malicious attacks," *IEEE Trans. on Industrial Electronics*, vol. 52, pp. 327-334, Feb. 2005.

[52] M.S. Wang and W.C. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition," *Optical Engineering,* vol. 46, no. 6, June 2007.

[53] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Advances Cryptol. EUROCRYPT94,* Perugia, Italy, vol. 950, pp. 1–12, May 1995.

[54] P. Kapoor, K.K. Sharma, S.S. Bedi, A. Kumar, "Colored image watermarking technique based on HVS using HSV color model," *ACEEE Inter. Journal on Network Security,* vol. 2, no. 3, pp. 20-24, July 2011.

[55] W.Q. Yan, J. Duo, and M. Kankanhalli, "Visual cryptography for print and scan applications," in *Proc. IEEE Int. Symp. Circuits Syst.*, Vancouver, Canada, May 2004, vol. 5, pp. 572–575.

[56] A. Ashwathimesangla, "Visual Cryptography for Color Images," *Inter. Journal of Electrical and Electronics Engineering*, vol. 2, no. 1, pp. 31 – 33, 2012.