

A Novel Blind and Fragile Digital Image Watermarking Technique Based on DWT-SVD

Yazan Mohammad Al-omari

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

Master of Science
in
Computer Engineering

Eastern Mediterranean University
February 2017
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Mustafa Tümer
Director

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

Prof. Dr. Işık Aybay
Chair, Department of Computer Engineering

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

Asst. Prof. Dr. Cem Ergün
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Önsen Toygar

2. Asst. Prof. Dr. Yıldıran Bitirim

3. Asst. Prof. Dr. Cem Ergün

ABSTRACT

The trade-off between the imperceptibility and the strength of the embedded watermark is one of the most difficult challenges in digital watermarking systems. In certain applications, the watermark has to be preserved from any alterations within both the embedding and extracting processes, i.e. the strength of the watermark has to be maximized in such a manner that results in an identically extracted watermark. In this context, most of the existing methods suffer from one of the two shortcomings, represented by an enormous amount of alterations that may take place along with maximizing the strength of the embedded watermark, or the inability to give an identically extracted watermark. In light of these shortcomings, this thesis proposes a new fragile and blind watermarking technique for digital images, based on two-dimensional wavelet transformation domain and singular value decomposition. In addition to this, the effects of some watermarking techniques on watermarked images were investigated and compared against the proposed method in terms of the level of imperceptibility. The key idea of the proposed method is to hide the indices that would indicate the location of certain values of a watermark instead of hiding the watermark itself. For a binary watermark, the indices of the zero elements are selected. In this way, the imperceptibility level can be enhanced in a strongly embedded watermark. Through the experimental phase, the proposed method along with the other selected methods has undergone several simulation experiments in the grayscale domain to test and compare their levels of imperceptibility. After this, the proposed method has been compared with the best of the experimented methods in the colorful domain using the HSI color space.

Keywords: Watermarking Image, Blind system, Watermark strength, DWT, SVD.

ÖZ

Gömülü dijital filigranın (gizli damga) farkedilmezliği ve dayanıklılığı arasındaki alışveriş dijital filigran sistemleriyle ilgili en önemli zorluklardan biridir. Belirli uygulamalarda, filigran, yerleştirme ve ayıklanma işlemlerinden kaynaklanabilecek bozulmalardan korunmalıdır. Diğer bir ifadeyle, orijinaliyle özdeş bir şekilde filigranı ayıklayabilmek için filigranın dayanıklılığı artırılmalıdır. Farkedilmezlik ve dayanıklılık arasındaki bu mücadelede yaygın metotlardan çoğu iki eksiklikten biriyle sonuçlanmaktadır gömülü filigranın dayanıklılığı artırılmaya çalışılırken büyük çapta bozulmalar meydana gelmekte; farkedilmezlik artırılmak istendiğinde ise özdeş bir filigran ayıklamak mümkün olmamaktadır. Bu eksikliklerin ortaya çıkardığı bilgiler çerçevesinde bu tez, dijital görüntüler için iki boyutlu dalga dönüşüm alanı ve tekil değer ayrışımına dayalı olan yeni, kırılğan ve kör bir filigran tekniği önermektedir. Buna ek olarak, farkedilmezlik seviyesi baz alınmak suretiyle bazı filigran tekniklerinin filigranlı görüntüler üzerindeki etkileri araştırılmış ve önerilen teknikle kıyaslanmıştır. Önerilen metodun ana fikri filigranın kendisini gizlemek yerine filigranın kati değerlerinin lokasyonunu imleyebilecek göstergeleri gizlemektir. İki terimli bir filigran için sıfır değerlerinin göstergeleri seçilerek güçlü bir şekilde gömülmüş filigranın farkedilmezlik seviyesi artırılabilir. Uygulama aşamasında, önerilen metod ve seçilen diğer metotlar, farkedilmezlik seviyelerinin test edilmesi ve karşılaştırılması için gri tonlu alanda pek çok deneye tabi tutulmuşlardır. İkinci aşamada ise önerilen metod ve en iyi sonuçları veren diğer metotlar HSI renkli boşluğunda karşılaştırılmıştır.

Anahtar Kelimeler: Filigranlı görüntü, kör sistem, filigran sağlamlığı, DWT, SVD.

DEDICATION

*This thesis is dedicated to my lovely parents and siblings for their
endless love, support and encouragement*

ACKNOWLEDGMENT

I would like to sincerely thank my supervisor, Asst. Prof. Dr. Cem Ergün for his guidance and support throughout this study, and especially for his confidence in me. I would also like to thank Assoc. Prof. Dr. Önsen Toygar and Asst. Prof. Dr. Yıltan Bitirim, for serving as jury members.

To all my friends, thank you for your understanding and encouragement in my moments of crisis. Your friendship makes my life a wonderful experience.

Finally, I must express my very profound gratitude to my parents and to my siblings for providing me with unfailing support and continuous encouragement throughout my period of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

TABLE OF CONTENTS

ABSTRACT.....	iii
ÖZ.....	v
DEDICATION.....	vi
ACKNOWLEDGMENT.....	vii
LIST OF TABLES.....	xi
LIST OF FIGURES.....	xii
LIST OF ABBREVIATIONS.....	xiii
1 INTRODUCTION.....	1
1.1 Watermarking Overview.....	1
1.2 Digital Watermarking Systems.....	2
1.2.1 Blind Watermarking Technique.....	2
1.2.2 Semi-Blind Watermarking Technique.....	3
1.2.3 Non-Blind Watermark Technique.....	3
1.3 Application Areas of Digital Watermarking.....	3
1.4 Characteristics of Watermarking Schemes.....	4
1.5 Thesis Organization.....	5
2 LITERATURE REVIEW.....	6
2.1 Introduction.....	6
2.2 Spatial Domain Based Watermarking Techniques.....	7
2.2.1 Least Significant Bit Technique.....	7

2.2.2 Correlation Based Watermarking Techniques	7
2.2.3 Other Spatial Domain Based Watermarking Technique.....	8
2.3 Frequency Domain Based Techniques.....	9
2.3.1 DCT Based Watermarking Techniques	9
2.4 Discrete Wavelet Transformation (DWT)	12
2.4.1 DWT-CDMA Based Watermarking Technique	14
2.5 Singular Value Decomposition (SVD)	15
3 PROPOSED DWT AND SVD BASED WATERMARKING TECHNIQUE	16
3.1 Introduction.....	16
3.2 Overview of Proposed Method	16
3.3 Embedding process	17
3.4 Extracting process	22
3.5 Priority of the Sub-bands	25
3.6 The Proposed Method in Color Space	27
3.6.1 Embedding Process in Colorful Images.....	27
3.6.2 Extracting Process in Colorful Images.....	28
4 EXPERIMENTAL RESULTS AND DISCUSSION	29
4.1 Introduction.....	29
4.2 Evaluating Efficiency of the Image Watermarking Techniques.....	29
4.2.1 Peak Signal to Noise Ratio (PSNR).....	29
4.2.2 Correlation Coefficient (CC)	30
4.3 Experimental Results Structure.....	31

4.4 Imperceptibility vs. Watermark Strength.....	32
4.5 Definition of the Parameter ‘k’ Gain Factor	32
4.6 Computational Complexity	39
4.7 Watermarking of Color Images.....	41
4.7.1 Conversion between RGB Color Space and HSI Color Space	41
4.7.2 Embedding Watermark in Colorful Images	42
4.7.3 Extracting Watermark in Colorful Images.....	43
5 CONCLUSION AND FUTURE WORK	45
5.1 Conclusion	45
5.2 Future Work	45
REFERENCES	47

LIST OF TABLES

Table 3.1: PSNR values of the reconstructed image with on zeros subband.....	26
Table 4.1: PSNR and CC Values among the All Methods	38
Table 4.2: Comparison of Imperceptibility for Proposed Method and the Selected Method Over Different Cover and Watermark Images	38
Table 4.3: Highest PSNR Values for Colorful Images in CC-Equal-To-One	43

LIST OF FIGURES

Figure 2.1: Frequency Regions in 8 x 8 DCT block	10
Figure 2.2: Standard JPEG Quantization Table [27]	11
Figure 2.3: One Level DWT “Decomposition Structure”	13
Figure 2.4: Lena Image One Level Decomposition	13
Figure 3.1: Non-overlapped Cover Image	17
Figure 4.1: a-c) Example Grayscale Cover Images	31
Figure 4.2: a-c) Example of Binary Watermarks	32
Figure 4.3: The Effect of the Gain Factor over PSNR.....	33
Figure 4.4: The Effect of the Gain Factor over CC	34
Figure 4. 5: Original Cover and Watermark	35
Figure 4. 6: Watermarked Image Using Correlation 1 PN seq. Technique	35
Figure 4. 7: Watermarked Image Using DCT-CDMA Technique.....	35
Figure 4. 8: Watermarked Image Using the Proposed Technique	35
Figure 4. 9: Watermarked Image Using DCT Middle Band Coef. Exchange	35
Figure 4. 10: Watermarked Image Using DWT-CDMA Technique	35
Figure 4. 11: The effect of the constant “alpha” over PSNR.....	36
Figure 4. 12: The Effect of the Constant “alpha” over CC	37
Figure 4.13: Transformed RGB Cover Image into HSI Color Space	42
Figure 4.14: Components of HSI Color Space of the Cover Image	42
Figure 4.15: Illustration of Embedding Process in Color Space.....	44

LIST OF ABBREVIATIONS

CC	Correlation Coefficient
CDMA	Code Division Multiple Access
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
FH	High Frequency Sub-band
FL	Low Frequency Sub-band
FM	Mid-Frequency Sub-band
HH	Diagonal Sub-band
HL	Horizontal Sub-band
HVS	Human Visual System
HSI	Hue Saturation Intensity
LH	Vertical Sub-band
LL	Approximate Sub-band
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
PN	Pseudo Noise
RGB	Red Green Blue
SVD	Singular Value Decomposition

Chapter 1

INTRODUCTION

1.1 Watermarking Overview

With the rapid development of Internet and the trend of multimedia digitization, the dissemination of information became remarkably quick and easy to conceive. This in turn, facilitated the digital form of information to be illegally copied or theft. Besides, other intellectual property extensions became exposed to many infringement behaviors.

Sharing digital images over the internet is a daily trend that exposes images to be modified imperceptibly with malicious intentions. Specifically, many advanced image processing software are being used to remove or replace features in digital images without detectable trace. These operations are considered as tamper; where prevention of unauthorized manipulations and protection of ownership rights is an open problem that attracted the interests of many researchers [1-4].

Consequently, many mechanisms have been evolved for data protection such as Steganography and Cryptography. Steganography is defined as the processes of embedding secret information within other non-secret data as a carrier. Cryptography is the process of protecting data by encrypting it in a form that makes it meaningless to unauthorized users[5-6].

Digital watermarking is a new emerging technology combining both Steganography and Cryptography by embedding invisible secret data in other data directly; hence, providing a way to protect digital data from illegitimate manipulation or copying.

Watermarking techniques are applied in a various domain of applications, such as, authentication, copy control, copyright protection, fingerprinting and others; each application requires the watermarking method to satisfy certain properties[7-8].

Watermarking methods can be categorized as *fragile* or *robust*. In a fragile watermarking scheme, the watermark is destroyed or altered when the watermarked image is exposed to any kind of modification, including both linear and non-linear transformations. This feature of fragile watermarks is usually to be used in image authentication. On the other hand, a robust watermark maintains its durability and resistance against geometric transformations such as compression, additive noise and images enhancement. This feature of robust watermarking schemes is useful in copyright and ownership verification[9].

1.2 Digital Watermarking Systems

The process of embedding/extracting watermarks varies from one scheme to another. Mainly, it depends on the purpose of using a watermarking technique [10].

1.2.1 Blind Watermarking Technique

Blind (public) watermarking schemes are considered to be the most challenging type of watermarking systems, as none of the original data (cover signal) or the original watermark are required to extract the embedded watermark makes them less robust to attacks. Merely, what is required to extract the embedded watermark using a blind

scheme is a key, which is typically a generated random sequence with certain characteristics that is used during the embedding process.

1.2.2 Semi-Blind Watermarking Technique

Semi-Blind (Semi-Private) watermarking schemes require some special information like the original watermark to detect the embedded watermark in the watermarked data, yet it does not require the original (cover data).

1.2.3 Non-Blind Watermark Technique

Non-Blind (Private) watermarking schemes are considered as the most robust technique to any kind of attack on the watermarked image as they require all original data in order to extract the embedded watermark.

1.3 Application Areas of Digital Watermarking

Watermarking is applied on a wide range of applications, we mention some of these applications next in this text [11].

Copyright Protection: Watermarking is mainly used when a corporation aims to affirm its “copyright ownership of digital objects”, e.g. ‘Big Media’ organizations, news agencies and photographers are the crucial applicants. It is commonly coveted to hide a "minimum amount of information", coupled with a maximum degree of robustness to any modification.

Copy Protection: Watermarking helps minimizing illegal copying of digitized media, as an example, embedding a watermark into a media CD prevents usual users from making unauthorized copies.

Temper Detection: Originality and integrity of data objects are necessary to be assured in many applications; photographic forensic information is a good way for

detecting tempers. A proof that an image has not been modified is required when it is desired to assure the validity of the information contained in an image. Such evidence can be conceived by building a watermarking system into digital cameras, distortion in the watermark occurs as data obtain by such systems is tempered.

Broadcast Monitoring: The watermark is used in this application to monitor unauthorized broadcast station. It is work by verifying whether the content is really broadcasted or not.

1.4 Characteristics of Watermarking Schemes

Deciding on a suitable watermarking scheme to be used in a certain application can be based on the following characteristics that vary from one watermarking scheme to another [12].

1. **Imperceptibility:** imperceptibility in terms of watermarking refers to minimal (unnoticeable) amount of distortion in the original cover following the watermark embedding process.
2. **Robustness:** robustness of the hidden watermark refers to the ability of extracting a watermark identical to the original watermark even if some manipulations happened to the watermarked image, i.e. the capability of the watermark to resist different kinds of attacks such as, cropping, rotation, histogram equalization, and additive noise.
3. **Fragility:** in contrast of the robustness property, fragility refers to the distortion or loss of the embedded watermark due to any performed manipulations on the watermarked image.

4. Capacity: capacity of the watermarking scheme refers to ratio between the number of the hidden bits to the size of the cover image.

1.5 Thesis Organization

This thesis is divided into five chapters, Chapter 1 is an introductory; it includes a brief overview of watermarking along with its different system types, application areas and characteristics. Chapter 2 is a literature review; it mainly considers digital image watermarking in spatial and frequency domains, in addition to an application oriented theory on discrete wavelet transform and singular value decomposition that serves the objectives of this thesis. Chapter 3 is titled as digital watermarking using SVD in 2D discrete wavelet domain; it mainly elucidates a proposed method for digital image watermarking in wavelet domain using singular value decomposition in detail with an illustration example. Chapter 4 is the experimental results and discussions; it discusses experimental results for the proposed method along with relative methods of comparisons from the existing literature. Finally, Chapter 5 presents a conclusion regarding the work done in this thesis, and suggests potential future works.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, a literature review on digital image watermarking is presented, which describes the essential techniques in digital image watermarking. Besides, the theory of singular value decomposition and 2D discrete wavelet transform that serves the object of this thesis is summarized. Finally, selective previous work in the same field is presented.

Recently, the research community has awarded a lot of attention to image watermarking [2-4], where watermarking can be achieved using two working domains, the transform domain and the spatial domain. Transform domain represents an image in terms of its frequencies which divides the image into multiple frequency bands, where the spatial domain represents the image pixels. In simple terms, several transforms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT) are capable to transferring an image into its frequency representation. Each of these transforms has distinct characteristics along with distinct image representation. The main procedure to embed a watermark in an image in a transform domain is by modifying the values of the transformation coefficients. While in the case of the spatial domain, the pixel values are to be modified in the watermark embedding process.

2.2 Spatial Domain Based Watermarking Techniques

2.2.1 Least Significant Bit Technique

The least significant bit technique is the most widely and commonly used technique in spatial domain which deals with the pixels of the host images directly by replacing the least significant bit values of the cover image pixels with the bit values of the watermark image. In spite of being a relatively simple scheme, yet it is full of drawbacks. LSB insertion is highly vulnerable to many of transformations, even the innocent and conventional ones. Lossy compression, such as JPEG, is very potential to ruin it entirely. Geometrical transformations, displacing the pixels and moving them around from the original grid are probable to damage the hidden message, so the simple translation is the only way that could allow recovery. Besides, any other types of image transformation such as blurring generally will crush the hidden data. Consequently, all evidences indicate that LSB technique has a limited degree of robustness for hiding data [13].

In which case concludes that LSB is a vulnerable technique even for simple or complex processing; consequently, it is almost unprofitable for digital watermarking. Furthermore, when robustness is not such a major obstacle it is considerable as a good technique for Steganography.

2.2.2 Correlation Based Watermarking Techniques

Adding a watermark to an image in the spatial domain can be done by adding a pseudo random noise pattern (watermark) to the luminance values of its pixels. Many schemes were been proposed based on this principle [14-17].

2.2.2.1 Correlation Based Technique with 1 PN Sequence:

An outstanding strategy for watermark embedding is to utilize the correlation properties of additive pseudo-random noise patterns as applied to an image [17-18].

As shown in equation (2.1).

$$I_w(x, y) = I(x, y) + k * W(x, y) \quad (2.1)$$

Where $I_w(x,y)$ is the watermarked image, $I(x,y)$ is the cover image, $W(x, y)$ is a mask pattern with the same size of the image and k is the gain factor. It is obvious that increasing gain factor k yields to better robustness of the watermark at the expense of the quality of the watermarked image.

In order to extract the embedded watermark, the same algorithm that generates the pseudo-random noise is seeded with the same key, and then the correlation between the noise pattern and possibly watermarked image is to be computed. Therefore, a single bit of the watermark is set when the correlation exceeds a certain threshold T which means the watermark is detected. Dividing the image into blocks yields to multiple-bit watermark by performing the same procedure on each block independently. Thereon, the maximum length of the watermark shall be: $(W_w * H_w) / S^2$, where W_w and H_w are the width and the height of the cover image respectively, while S represents the block size has been chosen.

2.2.3 Other Spatial Domain Based Watermarking Technique

Voyatzis, G., & Pitas, I. [19], proposed a method to embed a binary watermark image by using a spatial transform which maps every watermark's pixel to a pixel of the cover image. An appropriate function is utilized to modify the selected pixels in the embedding procedure. At the detection step, a proper function is performed on the pixels of the watermarked image to locate the binary digit (0, 1) that has been

embedded. Then reconstructing the binary image (watermark) can be done by applying the inverse spatial transform.

2.3 Frequency Domain Based Techniques

By comparing the frequency domain techniques with the spatial ones, definitely we can say that frequency domain schemes are more effective in achieving high robustness and more bits of a watermark can be embed as the results showed. Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier transform (DFT) is the most popular transforms used in image watermarking.

2.3.1 DCT Based Watermarking Techniques

A global DCT approach has presented in [21] to embed a watermark in the perceptually significant portion of the Human Visual System (HVS) because the most compression techniques remove the perceptually insignificant portion of the image which are in the frequency domain represents the high-frequency components.

DCT based watermarking method segments the cover image into 8x8 blocks, then applying forward DCT to each block, and some criteria such as Human Visual System (HVS) should be applied to select the appropriate blocks, along with other criteria to select the desired coefficient at each block (e.g select the highest coefficient), finally the embedding process is done by adjusting the elected coefficients. Thereafter, the inverse DCT transform should be applied on each block to construct a watermarked image [22].

2.3.1.1 The Middle-Band Coefficient Exchange Technique

The DCT allows an image to decompose into different frequency bands, making it much easier to hide the information of the watermark in the bands of middle

frequencies of an image. Middle frequencies bands are chosen so that they avoid the most important visual parts of the image (low frequency) without overexposure to eliminate compression and attacks noise (high frequency). This technique utilizes comparing the middle-bands frequency of DCT coefficients to encode a single bit in a DCT block [17-18]. To begin, we define middle-band frequency (FM) of an 8x8 DCT block as shown in Figure 2.1:

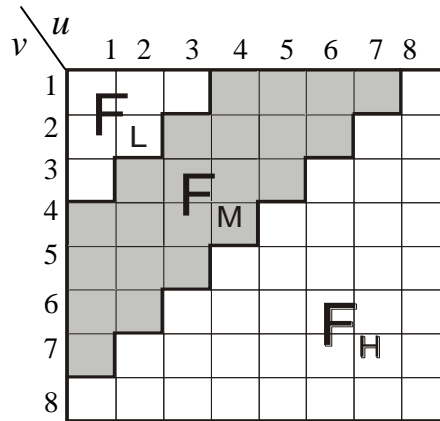


Figure 2.1: Frequency Regions in 8 x 8 DCT block

FL is used to denote the low-frequency components of the blocks, while **FM** and **FH** are used to denote the middle and high-frequency components respectively. **FM** is chosen for both hiding regions and to afford more robustness to lossy compression mechanisms with averting noticeable changes in the cover image.

To embed a watermark two locations (u_1, v_1) and (u_2, v_2) are chosen from the FM region for comparison of each 8x8 block as shown in equation (2.2).

$$\begin{aligned} & \text{DCT}(u_1, v_1) > \text{DCT}(u_2, v_2), \text{ encode "1"} \\ & \text{Otherwise,} \qquad \qquad \qquad \text{encode "0"} \end{aligned} \tag{2.2}$$

A constant “k” is introduced in this technique as appear equation (2.3) to improve the strength of the watermark:

$$\text{DCT}(u_1, v_1) - \text{DCT}(u_2, v_2) > k \quad (2.3)$$

The parameter 'k' can easily control the quality of the image and the strength of the watermark, increasing the value of this parameter will enhance the strength of the embedded watermark at the expense of the quality of the watermarked image. Thus, the basic concept of that parameter is, when the value of 'k' is large; the large coefficient will not be affected hugely even after compression. Thereafter, in order to extract the embedded watermark, the DCT transformation for the watermarked image is computed. Thus, if $\text{DCT}(u_1, v_1) > \text{DCT}(u_2, v_2)$ a "1 is decoded" else; a "0 is decoded".

So to be more robust against compression it is preferable to select the locations based on the "recommended JPEG quantization table" that shown in figure 2.2 instead of choosing arbitrarily locations.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 2.2: Standard JPEG Quantization Table [27]

2.3.1.2 DCT-CDMA Based Watermarking Technique

CDMA and DCT are a state of Code Division Multiple Access and Discrete Cosine Transform, respectively. In this scheme, the middle frequencies of the DCT block is

used to contain a pseudo noise PN sequence W (watermark), which can be modulated as follows:

$$I_{W_{x,y}}(u, v) = \begin{cases} I_{x,y}(u, v) + K * W_{x,y}(u, v), & u, v \in F_M \\ I_{x,y}(u, v) & , \quad u, v \notin F_M \end{cases} \quad (2.4)$$

After divided the cover image into 8x8 blocks; the DCT for every block is first computed. In that block, the watermark multiplied by the parameter 'K' (gain factor) is added to the middle frequency components F_M . then inverse transforming to each block to get the watermarked image I_W [17-18].

In the extraction stage, re-dividing the watermarked image into 8x8 non-overlapping blocks and computing the DCT transformation. Then, comparing the same PN sequence to the values of the middle frequency. Thus, if the correlation between the compared sequences exceeds a threshold T a value '1' is detected; else, a value '0' is detected.

2.4 Discrete Wavelet Transformation (DWT)

DWT decompose the image into four different sub bands (LL , HL , LH and HH) as shown in Figure. LL sub band represent the image which is low pass filtered horizontally and low pass filtered vertically, so, LL will occupy only one fourth of the image space because it is decimated by a factor of two in horizontal and vertical direction. HL sub band represent the image which is horizontally high passed and vertically low passed. In contrast, LH sub band represent the image which is low pass filtered horizontally and high pass filtered vertically, and the last sub band HH is horizontally and vertically high passed [23].

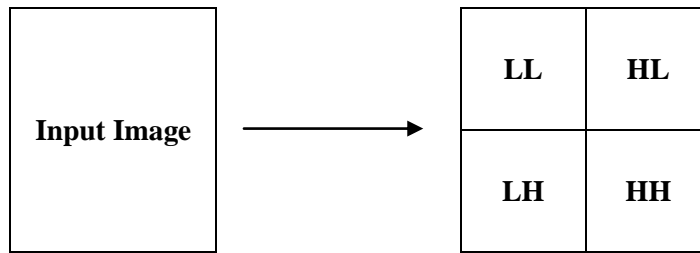


Figure 2.3: One Level DWT “Decomposition Structure”

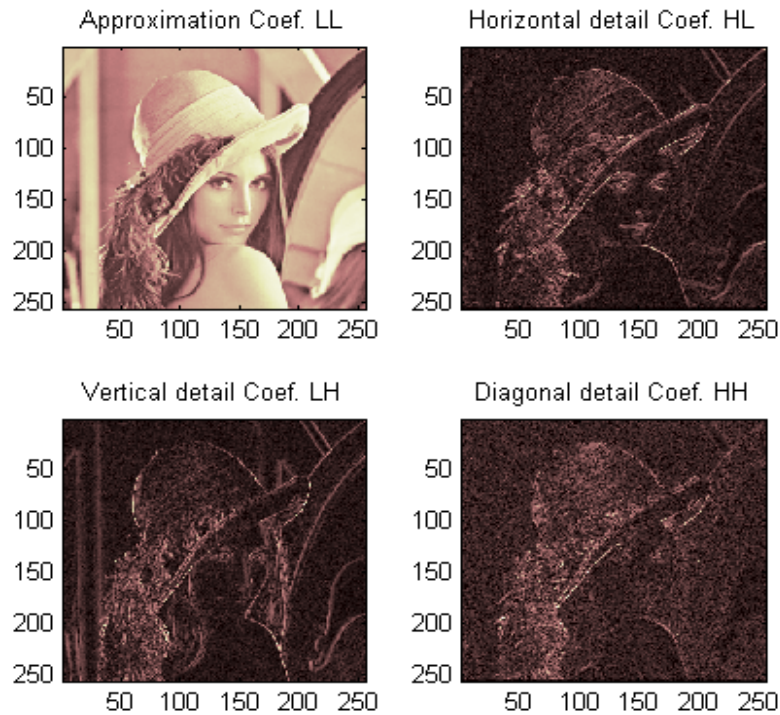


Figure 2.4: Lena Image One Level Decomposition

Kang, G. S. in [33] use of the DWT transform to initially process the image, and then to embed the mark represented in the DCT frequency domain. The method involves a visual watermark (grayscale image) which is transformed using discrete cosine transform for getting low frequency coefficients in frequency domain. Then, the original image is transformed using the discrete wavelet transform and watermark is embedded by modifying the coefficients of LL bands with appropriate imperceptibility.

2.4.1 DWT-CDMA Based Watermarking Technique

CDMA and DWT are a state of Code Division Multiple Access and Discrete Wavelet Transform, respectively. This technique is one of the simplest techniques. The concept of the embedding process is similar to that used in the DCT-CDMA technique. Equation 2.5 below shows the embedding procedure in the wavelet frequency bands.

$$I_{W_{u,v}} = \begin{cases} W_i + k |W_i| x_i, & u, v \in HL, LH \\ W_i, & u, v \in LL, HH \end{cases} \quad (2.5)$$

Where W_i indicates to the coefficient of the cover image in the wavelet transformation domain. x_i denotes to the bit of the watermark. ' k ' is the gain factor parameter.

To extract the embedded watermark; first of all, generating a pseudo-random (PN) sequence identical to that used in CDMA generation and determining the correlation with the two wavelet frequency bands of the watermarked image. The watermark is detected if the correlation exceeds some threshold T .

Embedding multiple-bit watermarks using this technique can be done by using a separate seed for each PN sequence and adding it to the frequency coefficient. In extracting, the correlation will be computed and if it exceeds a threshold ' T ' a value '1' is detected else a value '0' is detected. Accordingly, the extracted process will iterates over the entire PN until all the bits of the embedded watermark have been detected.

2.5 Singular Value Decomposition (SVD)

SVD is a linear algebra tool, that factorize a matrix A into three matrices U , S and V , where U and V are orthogonal matrices and S is a diagonal matrix in descending order, where SVD of a matrix of size $M \times N$ is decomposition of the form:

$$A_{(M \times N)} = U_{(M \times N)} S_{(M \times N)} V_{(M \times N)}^T \quad (2.6)$$

Hence, the singular values of A are the diagonal entries of the matrix S which they are the positive square roots of the Eigen values of AA^T [24].

Chapter 3

PROPOSED DWT AND SVD BASED WATERMARKING TECHNIQUE

3.1 Introduction

Imperceptibility and strength of watermarks are highly correlated; the interest in the strength should not be at the expense of the imperceptibility, in contrast, in the enhancement of the imperceptibility level of a watermarking scheme the strength level should not be affected. Imperceptibility enhancement is the essence of this research, and it is obtained by reducing the level of distortion in watermarked image.

This chapter introduces a new blind and fragile technique for digital image watermarking in frequency domain to meet the aforementioned requirements, and its efficiency will be discussed in Chapter 4.

3.2 Overview of Proposed Method

As it has been shown in section 2.3, transforming the image into a wavelet domain offers four different and unique transformation sub-bands: *LL*, *HL*, *LH*, and *HH*. Section 2.4 emphasizes how the singular value decomposition factorizes a matrix into two orthogonal matrices U and V , together with a diagonal matrix S . It will be shown in section 3.5, that the singular values in the diagonal matrix are exclusive and normally represent the power of an image. According to this hypothesis, diagonal matrix S of the sub-bands transformation will be used as a resort for the hidden data in the proposed method.

3.3 Embedding process

For illustration, consider the case of a 512x512 sized image and a 64x64 sized binary watermark, the concealment process can be explained as follows:

Step 1: Divide the cover image into 8x8 non-overlapping blocks as in Figure 3.1, where every block will have 64x64 pixels, so that the total number of blocks will be 64 which is the same number of rows in the watermark.

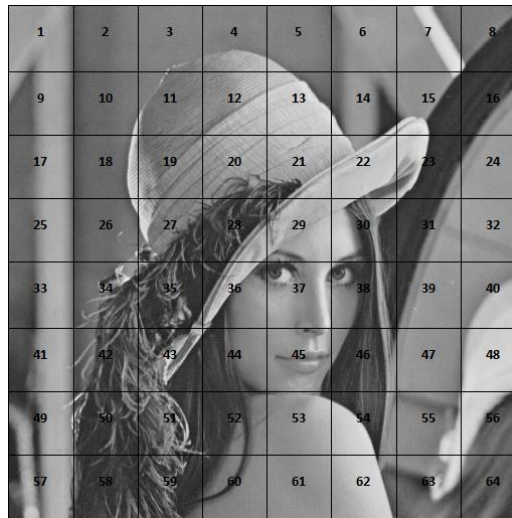


Figure 3.1: Non-overlapped Cover Image

Step 2: Transform each block to the wavelet domain using Haar filters to get its four 32x32 sized transformation subbands.

At this stage, the SVD function is applied to factorize every subband into U , V^T and S matrices to get four diagonal matrices for each block, S_{LL} , S_{HL} , S_{LH} , and S_{HH} .

All applied methods and techniques until now are represented in Figure 3.2

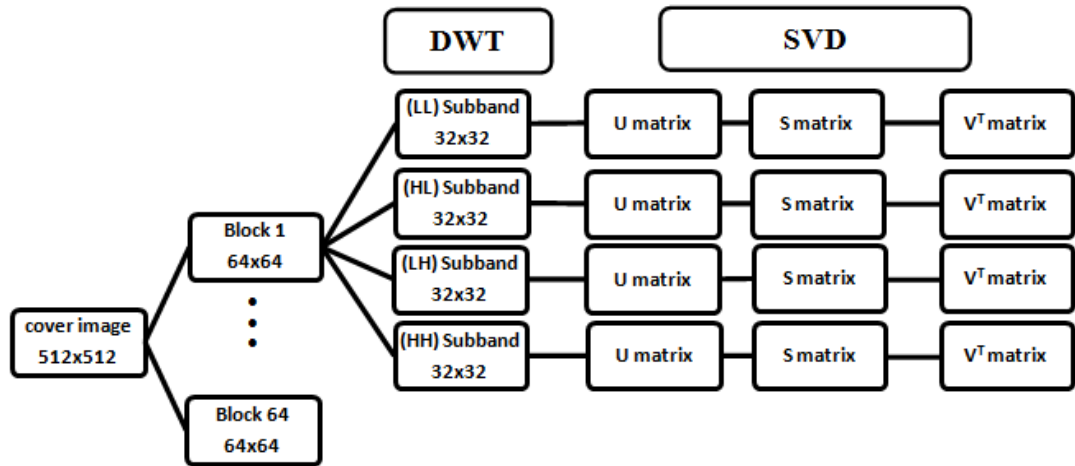


Figure 3.2: Cover Image Decomposition

The watermark is a binary image with a size of 64x64, where each and every row consists of 64 binary bits. It is easy to rebuild the watermark by knowing the indices of one kind of the binary data (0's or 1's), for instance if the locations of the zeros (0's) are known, then the locations of the ones (1's) can be easily computed and the watermark found easily.

In the proposed technique, the watermark itself or its values are not hidden, implicitly if the zeros (0's) of the watermark are known, then it should be understood that the remaining locations will be ones (1's). Hence the indices of the zeros bits for each row are known and it is the data which is to be hidden correspondingly, Figure 3.3 clarifies this technique

	1	2	3	4	5	6	7
1	0	1	0	1	1	0	0
2	1	1	0	1	0	1	1
3	0	0	0	0	1	1	1
4	0	1	1	1	0	0	0
5	1	0	1	1	1	0	0
6	1	0	0	0	0	1	1
7	0	1	0	1	1	0	0

Figure 3.3: Example of a Binary Watermark of Size 7x7

It will be seen from Figure 3.3, that the first row has four zeros with indices 1, 3, 6 and 7, the second row has two zeros with indices 3 and 5. Extraction of all the indices that consists zero value in each row can be achieved by following the same procedure for all rows.

As described before, there are 64 blocks for cover image and 64 rows for watermark. Therefore, each block will hide the indices for one row of the watermark.

By applying this method, the number of indices achieved of the range 0 to 64 as shown in Figure 3.4 below

	1	2	3	...	64
R 1	0	1	0	...	1
R 2	1	1	1	...	0
R 3	0	0	0	...	0
⋮	1	1	1	...	1
R 64	0	1	1	...	0

Figure 3.4: Binary Watermark of Size 64x64

The diagonal entries of matrix in each sub-band in Figure 3.5 contain 32 different values in descending order. It is important to note that, the results shown that changing the small values to convergent values will not destroy the image.

Accordingly, the values of last 16 diagonal entries in each sub-band are used to hide the indices. There are four sub-bands, which mean there are four diagonal matrices. The last 16 locations for each matrix are allocated with some values. Thus we have at most 64 locations to hide our extracted indices from the first row. The values of these

diagonal matrices are in descending order, while the indices of each row are in ascending order, in that way we have reversed the indices order.

$$\begin{bmatrix} S1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & \cdots & S8 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & S16 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & S32 \end{bmatrix} \Rightarrow \begin{bmatrix} S1 \\ \vdots \\ S8 \\ \vdots \\ S16 \\ \vdots \\ S24 \\ \vdots \\ S32 \end{bmatrix}$$

Figure 3.5: Extracting Diagonal singular values

Therefore, four cases have been classified according to the number of the computed indices:

- If the number of indices is between 0 and 16. Only *HH* sub-band is used while preserving the others.
- If the number of indices is between 17 and 32. Two sub-bands are used (*HH*, *HL*).
- If the number of indices is between 33 and 48. Here three sub-bands are being used (*HH*, *HL*, *LH*).
- If the number of indices is greater than 48 and less than or equal to 64. All the sub-bands are used (*HH*, *HL*, *LH* and *LL*).

Choosing the order of the subbands in each case is not random, and after examining the impact of each sub-band on the image separately as illustrated in section 3.5. It is found that, in case one only *HH* subband were used while preserving others, in the second case *HH* subband were used before *HL* subband, while *HH*, *HL* and *LH* were

used sequentially in case three, while in the last case *HH*, *HL*, *LH* and *LL* subbands were used respectively.

Before embedding the indices, one pre-process must, which depends on changing the last 16 values of each diagonal matrix to be zero in the used subband according to the cases mentioned before. For instance, 11 indices considered in first case, then only one subband will be used which is *HH*, the last 16 values of the diagonal matrix of this subband will be zeros, and hence all 11 indices will be the replacement of these values. This process will be useful in extraction phase. Figure 3.6 showing this process more clearly:

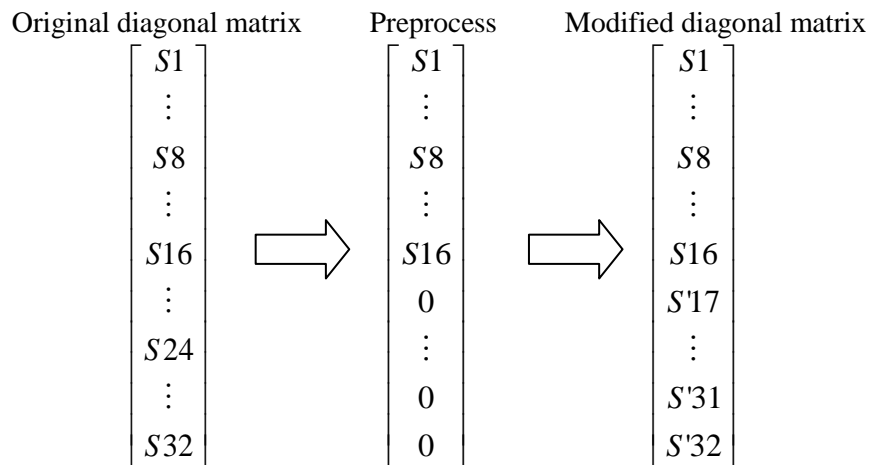


Figure 3.6: Modification of Diagonal Matrix

It is important to note that the values in diagonal matrix are much smaller than the indices values. Consequently, the indices values are multiplied by a small constant number 'alpha', to make the indices values somehow convergent to the original singular values as mentioned in equation 3.1. In this way, the degradation amount will be small and data will be prevented from being lost.

$$S'_n = I_n * \text{alpha} \tag{3.1}$$

In equation 3.1, S' denotes the new singular value result of multiplication the index I by constant alpha and n represents the block number.

The data may be lost, if the largest indices value S'_n is greater than the value of S_{16} in the first 16 preserved values in the diagonal matrix. It is because when applying inverse SVD to the modified diagonal matrix, it will be changed again to descending order and data of the watermark will get other locations. To enumerate the above procedures more clearly, Figure 3.7 represents the embedding process in all cases.

After embedding the indices with the appropriate subbands among all blocks, the inverse SVD operation will be performed with the modified diagonal matrices. After SVD operation, inverse wavelet transformation will be applied for all modified and unmodified subbands. Finally, all the blocks will be reconstructed to build the watermarked image. Such a method is known as a *blind* method that is why the constant 'alpha' is the only parameter, which should be known in order to extract the watermark.

3.4 Extracting process

At the extracting stage, the watermarked image is divided into 8x8 non-overlapping blocks and then each block is transformed into wavelet domain using Haar filter, after that, SVD will be applied on each subband to extract the diagonal matrices for all subbands.

As it is already known, the second 16 values in each diagonal matrix were targeted to hide the data of the watermark. The priority of the sub-bands has been given to *HH* subband, followed by *HL*, *LH* and *LL* subbands respectively.

Starting with *HH* subband and reading the last 16 diagonal entries in the diagonal matrix until finding the value zero, or finding a value that is greater than 64 when divided by ‘alpha’. In this case the hidden indices are found, for second sub-case the data is not an index.

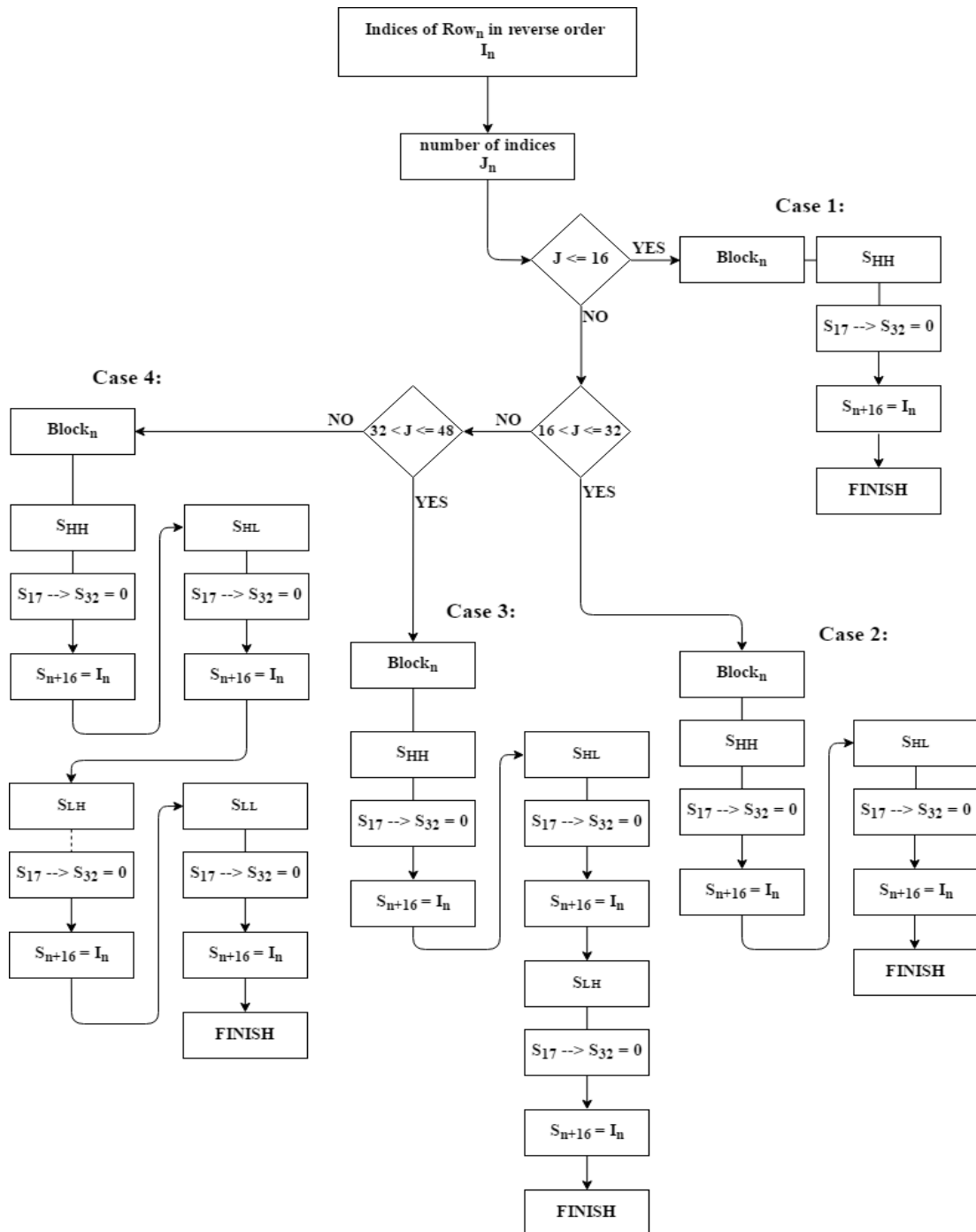


Figure 3.7: Embedding Process

If the condition is not true then moving towards the diagonal matrix of *HL* sub-band and reading the last 16 values until the condition is met for the new matrix, if not, the diagonal matrix of *LH* sub-band will be used, and lastly using the *LL* sub-band if the condition has not met in *LH* sub-band.

When the condition is true, it means that this is the all hidden indices in that block, after that the same reading procedure will be performed in the next block and so on until covering all blocks. It is worth mentioning that each block contains a data for one row only, which means when moving towards the next block, we are reading a data for the next row. It is important to separate the values that have been read from each block.

Clarifying the extracting process has been done in Figure 3.8 to show the steps sequentially. When the extracting process for all singular values is done over all blocks and their order have been separated and reversed correctly, the constant ‘alpha’ is used to be divided by the all extracted values. Then they become in range [0 to 64], these values represent the indices that contain the value zero in the original watermark.

$$I_{[1...n]} = S'_{[1...n]} / \text{alpha} \quad (3.2)$$

Where *I* denotes the computed index, *S'* represents the extracted value and alpha is a constant. To build the watermark, a 64x64 matrix with ones (1's) value is created, then using the extracted indices to change the values with the same number of the indices to zero (0).

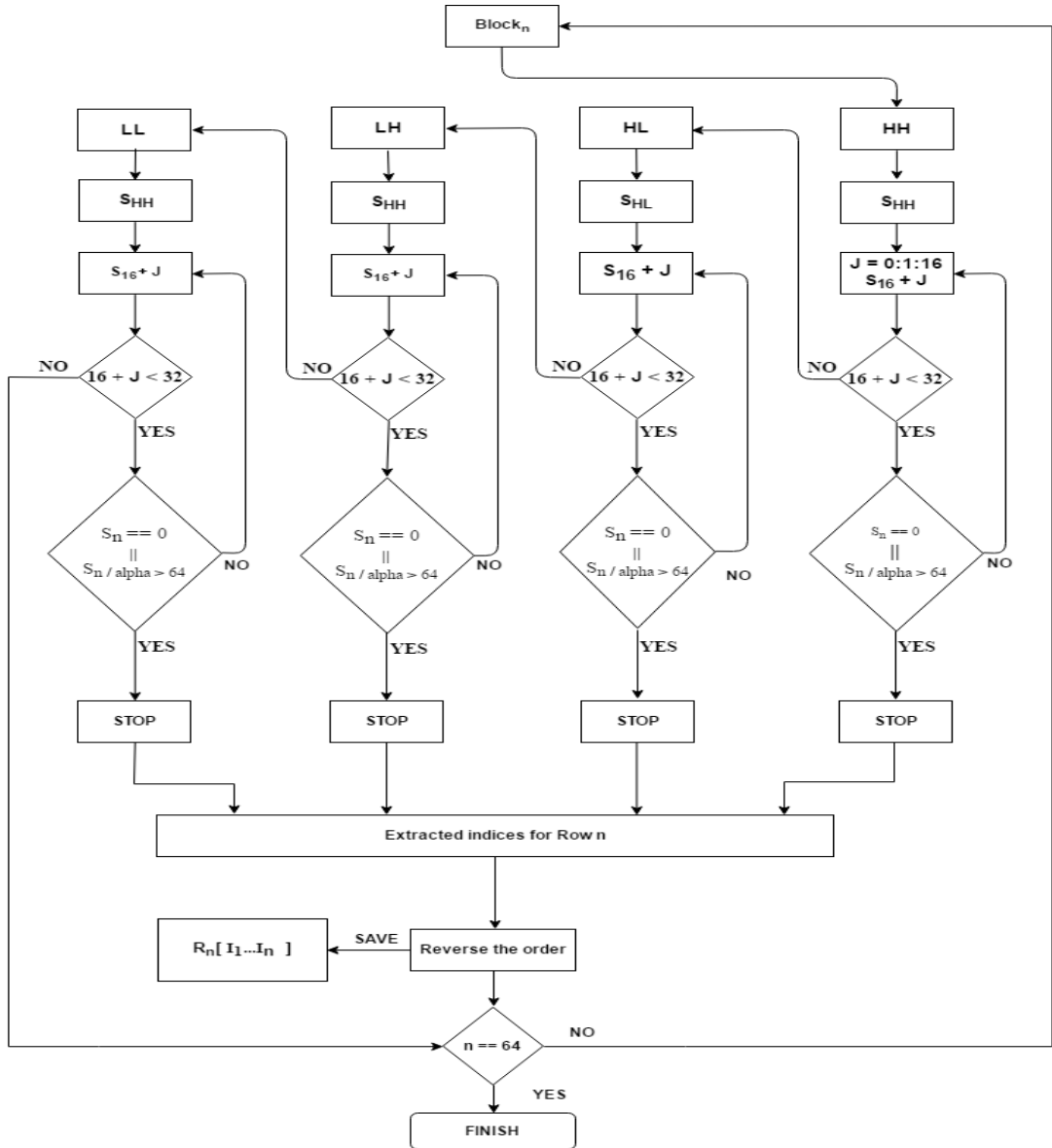


Figure 3.8: Extracting Process

3.5 Priority of the Sub-bands

It is noticeable that “*HH*” sub-band has the highest priority when trying to hide the data, in case that the data is greater than the second part of the singular values of the “*HH*” sub band then we hide a part of the data in “*HH*” sub-band before moving towards “*HL*” sub-band which has the second priority to hide the rest amount of data, same scenario will happen if the second part of the second sub band is not enough, we move again to “*LH*” sub band to hide the rest amount of the data, finally

we are using “*LL*” sub band if the first three sub bands could not accommodate the data which is going to be hide.

We adopted the order of sub bands [*HH*, *HL*, *LH* then *LL*] to hide the data. The main reason behind this choice is based on the result that, a simple strategy has got be applied to measure the impact strength of each sub-band on the image. The measurement is done by making the values of the singular values of each sub-band separately equal to zero then, computing peak to signal noise ratio (defined in section 4.2.1) as shown in table 3.1. It was found out that ‘*HH*’ sub-band which represents the diagonal details coefficients has the minimum effect on the image, while it has the highest PSNR value. The second place is occupied by “*HL*” sub-band which represents the horizontal details coefficients, with its influence slightly higher than “*HH*” sub-band and less than “*LH*” sub-band which represents a vertical details coefficients, while “*LL*” sub-bands has the highest effect on the image which naturally represents the approximation coefficients.

Table 3.1: PSNR Values Of the Reconstructed Image with One Zeros Subband

Subbands	PSNR Value
When the singular values of <i>HH</i> sub-band is equal to zeros with preserving the others	42.9857 dB
When the singular values of <i>HL</i> sub-band is equal to zeros with preserving the others	37.5967 dB
When the singular values of <i>LH</i> sub-band is equal to zeros with preserving the others	34.3428 dB
When the singular values of <i>LL</i> sub-band is equal to zeros with preserving the others	-4.3567 dB

3.6 The Proposed Method in Color Space

The process of using watermarking technique should not be limited to the only grayscale images. Color images used in many areas, which requires an efficient watermarking technique to hide a watermark in colorful images. Thus, the efficiency of the watermarking scheme is not only measured in the grayscale images. Accordingly, in this section, applying the proposed method over colorful images has been presented.

The available colorful images are in RGB color space which consists of three primary red, green and blue additive colors, many color spaces have been designed such as YCbCr, HSV, HSI and CMYK, etc. for different purposes.

3.6.1 Embedding Process in Colorful Images

Firstly, transforming the RGB cover image into HSI color space which is the most frequently used application oriented color space. HSI color space is based on human visual perception theory and is suitable for describing and interpreting color [25]. *H*, *S*, and *I* components represent hue, saturation, and intensity respectively. Intensity component is normally used for embedding the watermark instead of hue & saturation components that correspond to human perception.

Secondly, treating the intensity component matrix as a grayscale image and applying the aforementioned embedding procedure. Then, concatenate the modified intensity component along with the hue and saturation components to get a watermarked image in HSI color space. At the end, transforming the HSI watermarked image into RGB color space.

3.6.2 Extracting Process in Colorful Images

In order to extract the hidden watermark, firstly, transforming the RGB watermarked image into HSI color space, then, applying the aforementioned extracting process to the intensity component.

Chapter 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, the results obtained by four techniques along with the proposed one are presented. Multi-phases of comparison were accomplished to show the efficiency per technique and to achieve a more accurate understanding with a better knowledge of the mechanism of these methods.

4.2 Evaluating Efficiency of the Image Watermarking Techniques

The inclusion of a watermark within an image may cause unnoticed distortion to the image which requires the use of mathematical methods for calculating this distortion. The peak signal-to-noise ratio (PSNR) between the watermarked image and the original cover image is computed to measure one efficiency point of the image watermarking technique.

On the other hand, extracting a watermark identical to the original watermark is another point of the efficiency measurement which has been done by computing the correlation coefficient between the extracted watermark and the original watermark.

4.2.1 Peak Signal to Noise Ratio (PSNR)

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation [28]. It is defined in term of the Mean Squared Error and usually it is expressed in terms of the logarithmic decibel scale (dB).

In case that there is a two $m \times n$ images $I(x,y)$ and $J(x,y)$, one of these images considered as a noisy approximation of the other image. Thereafter, MSE is computed as follows:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|I(i,j) - J(i,j)\|^2 \quad (4.1)$$

The PSNR is defined as:

$$PSNR = 10 \log_{10} \left(\frac{N^2}{MSE} \right) \quad (4.1)$$

For colorful images, the PSNR can be defined as:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE(R) + MSE(G) + MSE(B)} \right) \quad (4.2)$$

Where N represents the number of bits per pixel, $MSE(R)$, $MSE(G)$ and $MSE(B)$ denote to mean squared error for Red, Green and Blue colorful image components respectively. Moreover, the larger the Peak Signal to Noise Ratio (PSNR), the less distortion of the quality of the original host images [23].

4.2.2 Correlation Coefficient (CC)

“The correlation coefficient, a concept from statistics, is a measure of how well trends in the predicted values follow trends in past actual values” [29]. In watermarking term, Correlation coefficient was used to find the strength of the similarity between the extracted and the original watermark. An identical match gives a coefficient of 1. The CC is defined as:

$$CC = \frac{\sum_{M,N} [I_1(m,n) \cdot I_2(m,n)]}{\sqrt{\sum_{M,N} [I_1(m,n)]^2 \cdot \sum_{M,N} [I_2(m,n)]^2}} \quad (4.3)$$

Where M and N denotes the size of the input image, I_1 represent the original watermark and I_2 represent the extracted watermark.

4.3 Experimental Results Structure

The first experiment is carried out over all methods to show how the parameter 'K' known as gain factor, which was mentioned in equations (2.1), (2.3), (2.4) and (2.5) will control the quality of the watermarked image and the strength of the embedded watermark. In addition to the explanation of how does the parameter 'alpha' used in the proposed method work.

In the second experiment, peak signal-to-noise ratio and correlation coefficient values have been computed for all the methods, the experiment is done using same cover and watermark image, comparing these methods based on a fixed correlation coefficient value to show which method that could achieve the highest peak signal-to-noise ratio value, in addition to trying a different cover and watermark images.

The latest experiment is carried out based on colorful cover images and shows the computed values of PSNR and CC for the proposed technique, along with the best one among the methods compared previously. All the selected methods with the proposed method are simulated using MATLAB software.

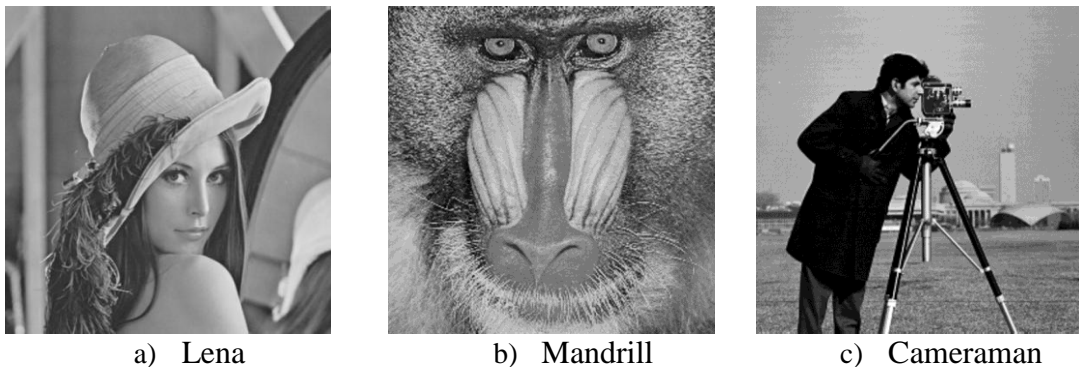


Figure 4.1: a-c) Example Grayscale Cover Images

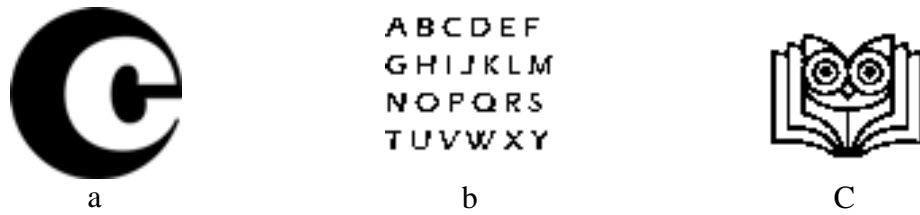


Figure 4.2: a-c) Example of Binary Watermarks

4.4 Imperceptibility vs. Watermark Strength

Imperceptibility of watermarked images is defined as to which extent the watermark is perceptible in the cover images. Normally, it is measured by the amount of distortion that occurred during the embedding process; which in turn affects the strength of the watermark in an inverse relation, i.e. increasing the imperceptibility of the watermarked image will decrease the strength of the watermark. The strength of the watermark is known as to what extent the embedded watermark is strong in the watermarked image which in turn yields to extract a watermark without distortion.

4.5 Definition of the Parameter ‘k’ Gain Factor

As noticed from equations (2.1), (2.3), (2.4) and (2.5) the parameter 'k' which is known as 'gain factor' is a constant number to be multiplied with the watermark to control the imperceptibility in the watermarked images and the strength of the embedded watermark.

The experiment below presents graphs that illustrate the working principle of this parameter in each method and shows how it can affect the imperceptibility and the strength of the watermark.

Measuring the imperceptibility is achieved by computing the PSNR value for each method over different values of the parameter ‘k’, whereas measuring the strength of

the watermark is carried out by calculating the correlation coefficient value for each technique over different values of the parameter 'k' as shown in figure 4.2.

It is worth mentioning that, in the proposed method a parameter called 'alpha' has been used to resize the hidden data as defined in section 3.2; this parameter is somehow similar to the declared parameter 'k'.

In this experiment as in Figure 4.3, different values of the parameter 'alpha' are used and illustrated in other graphs to show how this constant can affect the imperceptibility and the strength.

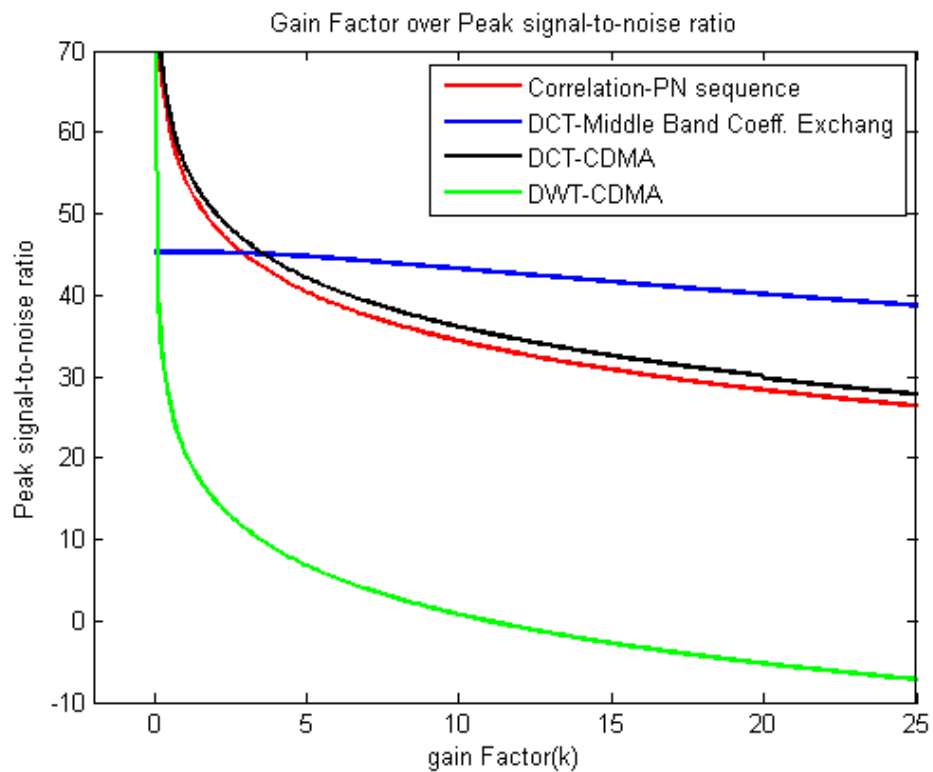


Figure 4.3: The Effect of the Gain Factor over PSNR

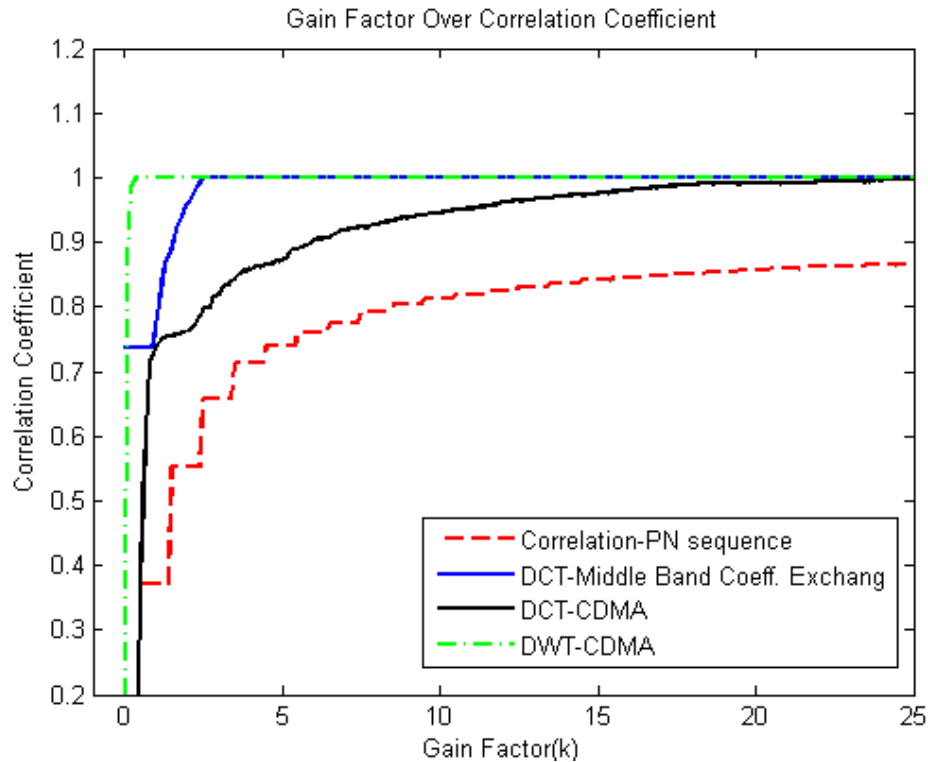


Figure 4.4: The Effect of the Gain Factor over CC

Figure 4.3 together with Figure 4.4 show PSNR-Vs-CC-based comparisons for commonly used watermarking schemes known as: Correlation-based method with 1 PN sequence, DCT-CDMA, DWT-CDMA and DCT Based Middle Band Coefficient Exchange. In the following discussion, comparisons are oriented regarding the PSNR of the host (the cover image) which corresponds to CC-equal-to-one for the extracted watermark. These figures indicate that the “Correlation-based method with 1 PN sequence” was not able to preserve the watermark at CC equal to one whereas its host has good PSNR values over different gain factors. In contrast, “DCT-CDMA” could reach the desired watermark CC value on the expense of its host PSNR. Consequently, “DWT-CDMA” was found superior to the aforementioned methods in this regard, where it preserved a better host PSNR against the desired CC for its watermark. Evidently, the best host PSNR against the desired watermark CC was achieved by “DCT Based Middle Band Coefficient Exchange”. For convenience, the

latter method will be used as a scalar of comparison with the proposed method hereafter.



(a) 'Lena' Cover Image (b) watermark
Figure 4.5: Original Cover and Watermark

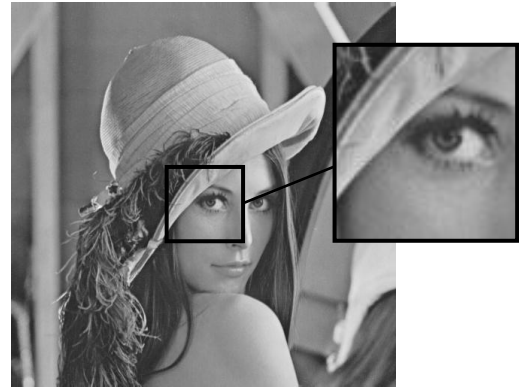


Figure 4.6: Watermarked Image Using the Proposed Technique

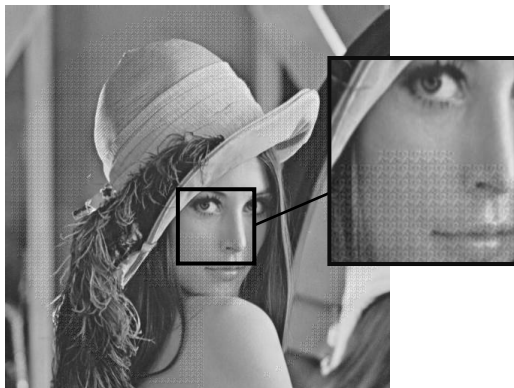


Figure 4.7: Watermarked Image Using Correlation 1 PN seq. Technique



Figure 4.8: Watermarked Image Using DCT Middle Band Coef. Exchange

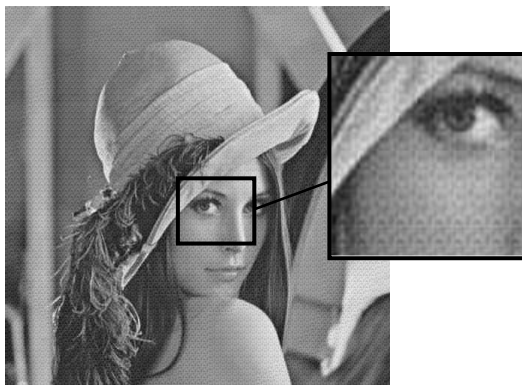


Figure 4.9: Watermarked Image Using DCT-CDMA Technique

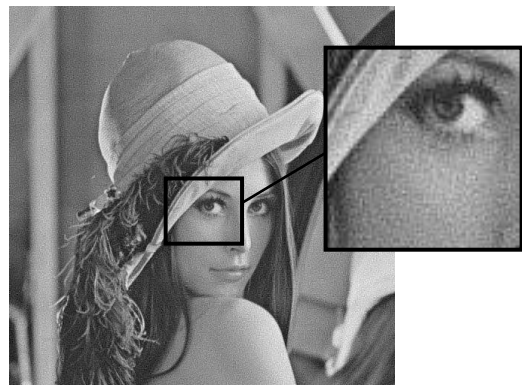


Figure 4.10: Watermarked Image Using DWT-CDMA Technique

The figures shown above represent the results of embedding a binary watermark of size 64x64 within a grayscale cover image of size 512x512. The amount of degradation in the watermarked images is noticeable in the compared methods as obvious in the patches. In contrast, this distortion is unnoticeable in the proposed technique.

As noticed from the comparison above, we could not mention the proposed method, this is due to the gain factor named ‘alpha’ having to be in the range (0,1] while the gain factor in the other methods could be greater than one. Figures 4.11, 4.12 show the behavior of the proposed method over different values of the parameter ‘alpha’.

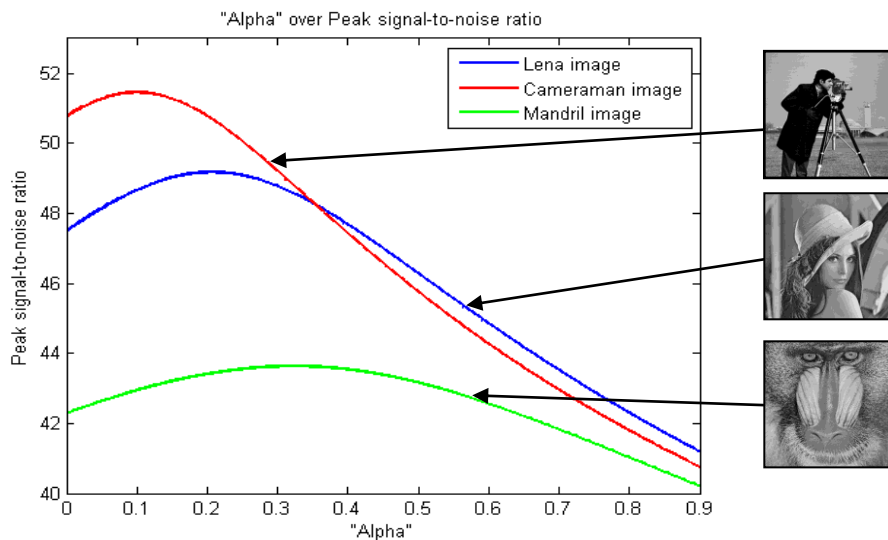


Figure 4.11: The Effect of the Constant “alpha” over PSNR

As Figures 4.11 and 4.12 demonstrate, the first graph shows PSNR values over different values of ‘alpha’, the highest PSNR value for ‘Lena’ image achieved by the proposed method was equal to 49.1798 when ‘alpha’ equal to 0.211, with 0.9312 CC value for the extracted watermark. With “cameraman” image the highest PSNR value was equal to 51.4618 with CC value equal to 0.8109 for the extracted watermark

when alpha value was 0.1. Figure 4.12 illustrates CC values over different values of alpha.

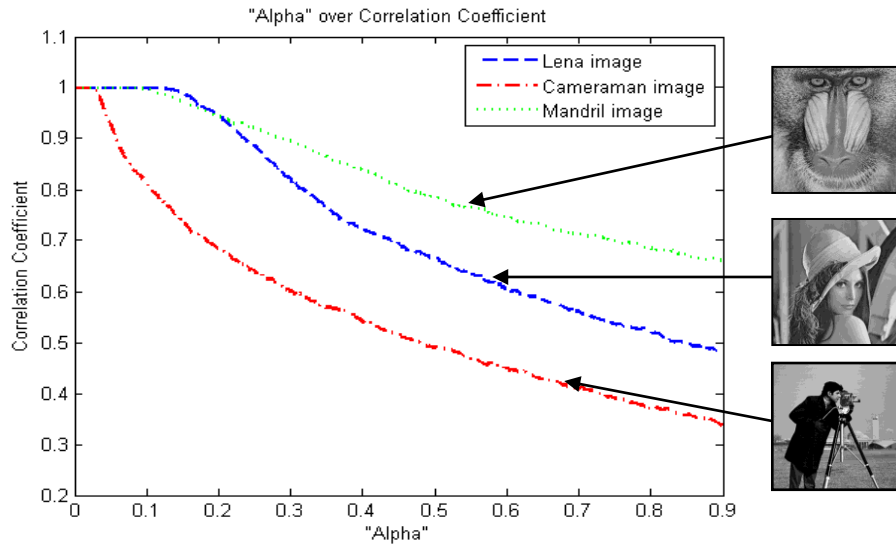


Figure 4.12: The Effect of the Constant “alpha” over CC

The aforementioned standard images (Lena, Mandrill and Cameraman) have been used since these standard images have a different level of details i.e Lena image has a medium level of details where Mandrill and Cameraman have the highest and the lowest level of details respectively.

The reason for this behavior of PSNR; is that when we have multiplied the indices values with the constant “alpha”, one value of “alpha” can give a convergent values to the replaced singular values, while the other values may give divergent values rather than the original values. On the other hand, the correlation coefficient values decreased because of the loss of the hidden data as discussed in section 3.3. To clarify the experiment, Table 4.3 presents the highest PSNR value reached by each method at the desired CC value using benchmark Lena.



As can be seen in the Table 4.1, the proposed technique has proved its superiority over the other methods by achieving the highest PSNR value at the desired CC value. According to the “Correlation-based method with 1 PN sequence” the highest reached CC value was equal to 0.8753 with PSNR value equal to 22.4129. The proposed technique has been compared with Kang, G. S. technique as obvious in [33], in Kang technique the watermark is a binary of size 32x32. Accordingly the proposed technique has been adapted to embed a watermark of the same size. Therefore, the proposed technique has proved its superiority over the compared technique.

Table 4.1: PSNR and CC Values among the All Techniques

Schemes	The highest PSNR value when CC_equal_to_one in all methods
Correlation-based method with 1 PN sequence	<i>this method FAILS to achieve CC = 1</i>
DCT Middle-band coefficient Exchange	45.1806 dB
DCT-CDMA	25.2240 dB
DWT-CDMA	26.7557 dB
Proposed Technique	48.6114 dB
Proposed Technique 32x32 watermark	56.8971 dB
Kang, G. S. in [33] 32x32 watermark	54.0600 dB

Therefore, different cover images along with various watermarks have been used. Table 4.2 shows the highest PSNR values reached in the desired CC value for the proposed method and the “DCT Based Middle Band Coefficient Exchange” method over different watermarks, cover images of size (512x512) and (64x64) watermarks.

Table 4.2: Comparison of Imperceptibility for Proposed Method and the Selected Method over Different Cover and Watermark Images

Proposed Technique		DCT Based Middle Band Coefficient Exchange Technique[17]		
		Lena	Mandrill	
	PSNR	PSNR	PSNR	PSNR
	48.6114 dB	41.7823 dB	45.1806 dB	33.8524 dB
	50.3779 dB	44.1059 dB	45.0140 dB	33.7213 dB
	48.8977 dB	43.4898 dB	44.3549 dB	33.9078 dB

It is noticeable that PSNR value for the watermarked digital images in the proposed method is diverse from one watermark to another; this is referring to reason that the number of indices that hold value zero is different in each watermark. For instance, the number of the concerned indices in the second watermark is obviously less than it in the other watermarks which in turns affected its PSNR value.

4.6 Computational Complexity

The high performance, speedy digital image capabilities are required in the watermarking domain, which yields to measure the computational complexity for the proposed technique and the compared one. In this case, the complexity of the 2D-DWT transformation have been measured according to [30], and it seems that it has complexity $O(4N^2 \log N)$. While the SVD tools of $m \times n$ matrix has complexity of $O(m^2 n + n^3)$ according to [31]. Therefore, the complexity of the proposed technique will be as follow

$$\text{Number of operation} = b \left[\underbrace{j \cdot b}_I + i \left(\underbrace{4 \left(\frac{N}{8} \right)^2 \log \left(\frac{N}{8} \right)}_{II} \right) + i \underbrace{\left(\frac{N}{8} \right)^3}_{III} \right] = O \left(\frac{N}{8} \right)^3 \quad (4.4)$$

Where b denotes to the number of blocks, j represents the number of the used sub-bands, and i is a variable represent the number of using DWT operation and SVD tool. and 8 denotes to the size of the block which is 8x8. The first part (*I*) of equation 4.4 represents the operations that happened on the used sub-bands in each block, the second part (*II*) denotes to the complexity of the 2D DWT multiplied with a variable i , (*III*) part represents the complexity of the SVD tool multiplied with a variable i .

The DCT coefficient exchange algorithm the same complexity as the proposed technique, where the 2D DCT transformation has the complexity $O(n)^3$ according to [32], therefore the complexity of the mentioned technique will be as follow

$$\text{Number of operation} = b \left[\underbrace{i \left(\frac{N}{8} \right)^3}_I + \underbrace{i \cdot b}_{II} \right] = O \left(\frac{N}{8} \right)^3 \quad (4.5)$$

Where b represent the number of blocks, i is a variable denotes to the number of the swap operation. And the constant number 8 number represents the block size is 8x8. The first part (*I*) denotes the complexity of the 2D DCT transformation multiplied with a variable i , the second part represents a number of operation based on the number of blocks b multiplied with a variable i .

Computational time for the aforementioned techniques is measured using a 2.30 GHz dual core CPU with 2 GB RAM PC. The proposed technique spent 2.1 sec

(embedding and the extracting process). While DCT middle band coefficients exchange technique spent 2.4 sec (embedding and extracting process).

4.7 Watermarking of Color Images

As mentioned in section 3.6, intensity component of HSI color space have been used to contain a watermark after transforming the RGB cover image into HSI color space as appear in Figure 4.13. In this experiment, “Lena” colorful cover image have been tested over different binary watermarks to measure and compare the imperceptibility of the proposed and the selected methods.

4.7.1 Conversion between RGB Color Space and HSI Color Space

The RGB color space can be transferred into HSI color space as follows [25]:

$$\begin{cases} I = \frac{1}{3} (R + G + B) \\ S = 1 - \frac{3}{(R + G + B)} [\min(R, G, B)] \\ H = f(x) = \begin{cases} \theta, & B \leq G \\ 2\pi - \theta, & B > G \end{cases} \end{cases} \quad (4.4)$$

$$\theta = \arccos \left\{ \frac{\frac{1}{2} [(R - G) + (R - B)]}{[(R - G)^2 + (R - B)(G - B)]^{\frac{1}{2}}} \right\} \quad (4.5)$$

The HSI color space can be transferred into RGB color space as follows:

$$\text{If } 0 \leq H < \frac{2}{3}\pi \text{ then:} \quad \begin{cases} B = \frac{1}{3}(1 - S) \\ R = \frac{1}{3} \left[1 + \frac{S \cdot \cos H}{\cos \left[\frac{1}{3} \pi - H \right]} \right] \\ G = 1 - (R + B) \end{cases} \quad (4.6)$$

$$\begin{aligned} &\text{If } \frac{2}{3}\pi \leq H < \frac{4}{3}\pi \text{ then} \\ &H = H - \frac{2}{3}\pi, \text{ and:} \end{aligned} \quad \begin{cases} R = \frac{1}{3}(1 - S) \\ G = \frac{1}{3} \left[1 + \frac{S \cdot \cos H}{\cos \left[\frac{1}{3} \pi - H \right]} \right] \\ B = 1 - (R + G) \end{cases} \quad (4.7)$$

$$\begin{aligned}
 & \text{If } \frac{4}{3}\pi \leq H < 2\pi \text{ then} \\
 & H = H - \frac{4}{3}\pi, \text{ and:}
 \end{aligned}
 \quad
 \left\{
 \begin{array}{l}
 G = \frac{1}{3}(1 - S) \\
 B = \frac{1}{3} \left[1 + \frac{S \cdot \cos H}{\cos \left[\frac{1}{3}\pi - H \right]} \right] \\
 R = 1 - (G + B)
 \end{array}
 \right.
 \quad (4.8)$$

In Figure 4.14, three components, *Hue*, *Saturation* and *Intensity* are the result of factorizing the HSI transformed image based on equations (4.4 – 4.8).



Figure 4.13: Transformed RGB Cover Image into HSI Color Space

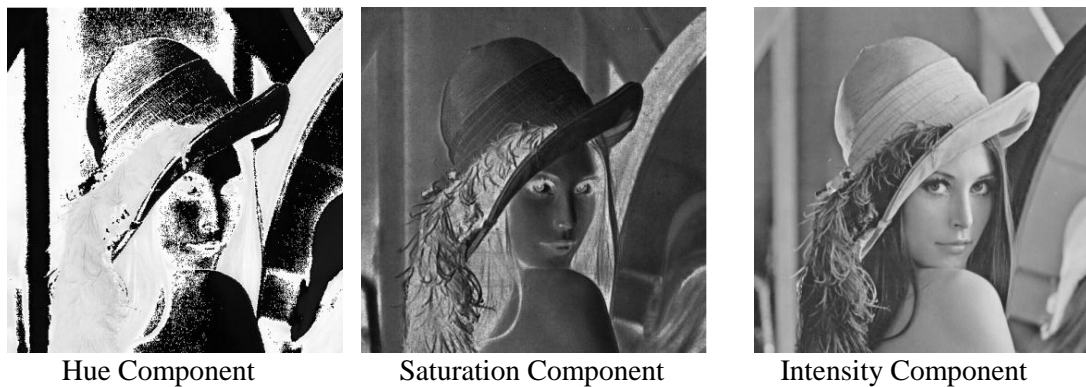


Figure 4.14: Components of HSI Color Space of the Cover Image

4.7.2 Embedding Watermark in Colorful Images

The watermarked image in HSI color space was created by concatenating the modified intensity component with the preserved hue and saturation components. As



appear in Figure 4.15 below. Therefore, transforming the HSI watermarked image into RGB color space to get the final watermarked image.

As can be seen from Table 4.3, different watermarks of size 64x64 have been experimented along with the colorful cover image ‘Lena’. The results appear below shows that the proposed method achieved a better PSNR value than the method that is used for comparison.

4.7.3 Extracting Watermark in Colorful Images

To extract the watermark from the colorful watermarked image, the same transformation of the HSI color space is used. After that, the basic components *Hue*, *saturation* and *intensity* are computed to extract the watermark from the *intensity* component following the proposed technique steps

Table 4.3: Highest PSNR Values for Colorful Images in CC-Equal-To-One

Proposed Technique		DCT Based Middle Band Coefficient Exchange Technique[17]
	Lena	Lena
	PSNR	PSNR
	47.1289 dB	43.9165 dB
	52.0320 dB	43.7638 dB
	48.9876 dB	43.2697 dB

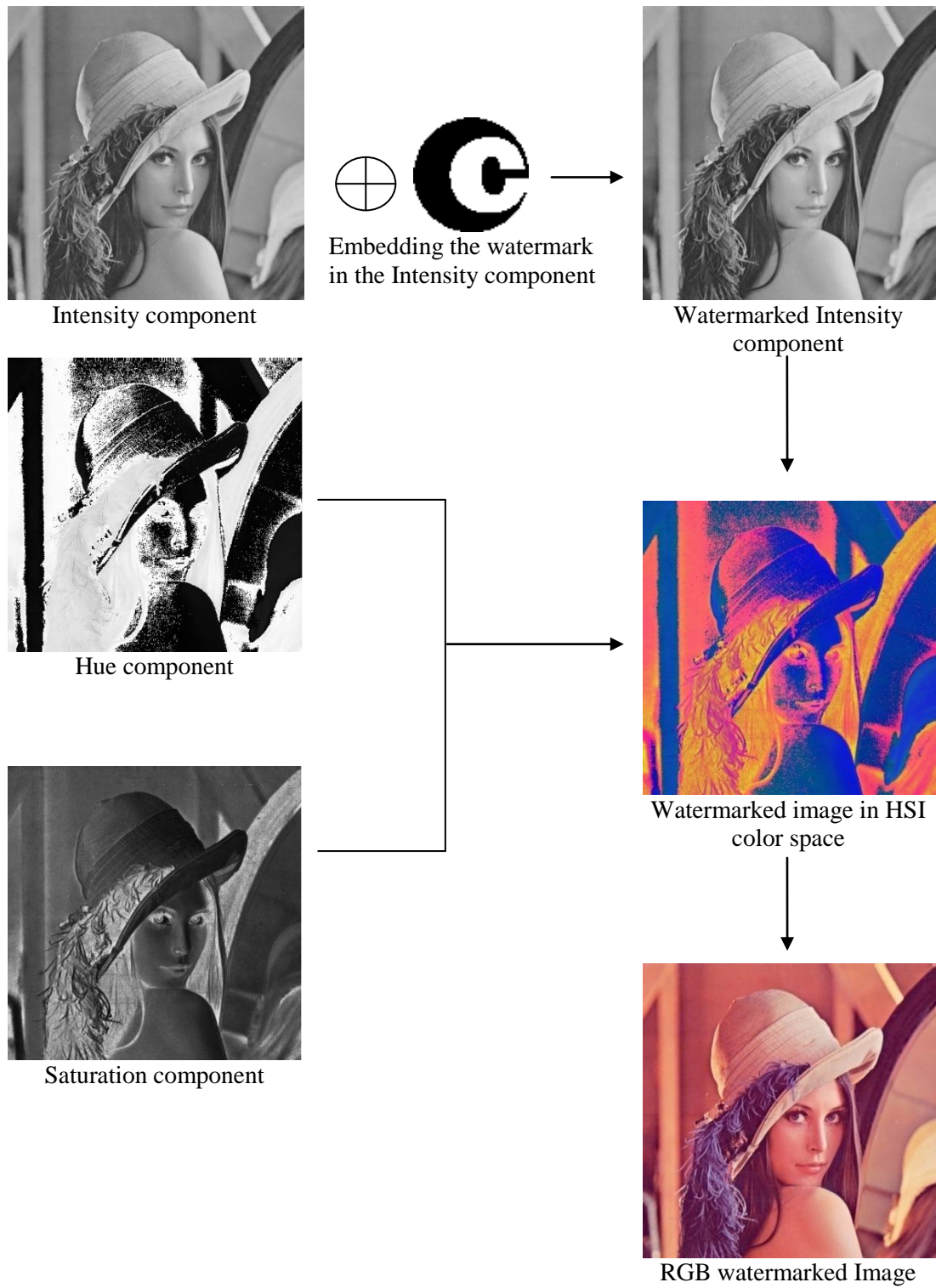


Figure 4.15: Illustration of Embedding Process in Color Space

Chapter 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this thesis, a novel fragile and blind watermarking technique based on 2D Wavelet Transformation domain and Singular Value Decomposition is presented, in addition to documenting the mathematical formulations and the experimental simulations for the proposed technique along with some existing watermarking techniques. Both the proposed technique and the compared techniques were vividly experimented over multiple setup of their parameter (gain factor), where the best result that achieved by the parameter (gain factor) in each method has been considered in the comparison. The experimental tests in the grayscale and the colorful domain have been proved the superiority of the proposed method over the compared methods in extracting a watermark identical to the original watermark with a better imperceptibility level. Consequently, the proposed technique is applicable on many areas such as content authentication, medical imaging and forensic image archiving.

5.2 Future Work

As mentioned in the proposed technique, the index values have been multiplied with the constant 'alpha' to fit these values with the replaced values in the diagonal matrices. As known, the range of the replaced values may be diverse among the all diagonal matrices. Thus, a multiple value of the parameter 'alpha' could be calculated in each of the wavelet transformation sub-bands, which in turns will enhance the imperceptibility level. Moreover, cryptography algorithms can be used

to encode the watermark, which in turns yields to increase the security level in the proposed watermarking technique. Furthermore, the digital videos are popular and commonly used in many areas. Thus, the proposed technique can be expanded to be adapted and useful in digital video watermarking. By the same token, many types of images are popular as well, such as, panoramic, 3D and thermal images, which can be used in the watermarking area. Therefore, accommodating the proposed technique to be convenient with these types of images will be of interest work.

REFERENCES

- [1] Yalcin, M. T. E., & Vandewalle, J. (2002, July). Fragile watermarking and unkeyed hash function implementation for image authentication on CNN-UM. In *Cellular Neural Networks and Their Applications, 2002.(CNNA 2002). Proceedings of the 2002 7th IEEE International Workshop on* (pp. 399-406). IEEE.
- [2] Jabade, V. S., & Gengaje, D. S. R. (2011). Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications, 31*(1), 28-35.
- [3] Sinha, M. K., Rai, R., & Kumar, G. (2014). Literature survey on digital watermarking. *International Journal of Computer Science and Information Technologies, 5*(5), 6538-6542.
- [4] WU, Y., & ZHANG, M. (2007). Survey of Digital Image Watermarking. *Modern Electronics Technique, 21*, 028.
- [5] Lim, Y., Xu, C., & Feng, D. D. (2001, May). Web based image authentication using invisible fragile watermark. In *Proceedings of the Pan-Sydney area workshop on Visual information processing-Volume 11* (pp. 31-34). Australian Computer Society, Inc..

- [6] Yeung, M. M., & Mintzer, F. (1997, October). An invisible watermarking technique for image verification. In *Image Processing, 1997. Proceedings., International Conference on* (Vol. 2, pp. 680-683). IEEE.
- [7] Li, Y., Guo, H., & Jajodia, S. (2004, October). Tamper detection and localization for categorical data using fragile watermarks. In *Proceedings of the 4th ACM workshop on Digital rights management* (pp. 73-82). ACM.
- [8] Cox, I. J., Miller, M. L., & Bloom, J. A. (2000, March). Watermarking applications and their properties. In *itcc* (pp. 6-10).
- [9] Zhao, Y. (2003). *Dual domain semi-fragile watermarking for image authentication* (Doctoral dissertation, University of Toronto).
- [10] Chawla, G., Saini, R., & Yadav, R. (2012). Classification of watermarking based upon various parameters. *International Journal of Computer Applications & Information Technology*, 1, 16-19.
- [11] Mintzer, F., Braudaway, G. W., & Bell, A. E. (1998). Opportunities for watermarking standards. *Communications of the ACM*, 41(7), 57-64.
- [12] Pan, J. S., Huang, H. C., & Jain, L. C. (Eds.). (2004). *Intelligent Watermarking Techniques:(With CD-ROM)*. World scientific.
- [13] Panchal, U. H., & Srivastava, R. (2015, April). A Comprehensive Survey on Digital Image Watermarking Techniques. In *Communication Systems and*

Network Technologies (CSNT), 2015 Fifth International Conference on (pp. 591-595). IEEE.

- [14] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM systems journal*, 35(3.4), 313-336.
- [15] Das, T. K., & Maitra, S. (2004). Cryptanalysis of correlation-based watermarking schemes using single watermarked copy. *IEEE Signal Processing Letters*, 11(4), 446-449.
- [16] Fridrich, J. (1999, July). Robust bit extraction from images. In *Multimedia Computing and Systems, 1999. IEEE International Conference on* (Vol. 2, pp. 536-540). IEEE.
- [17] Johnson, N. F., & Katzenbeisser, S. (2000). A survey of steganographic techniques. In *Information hiding* (pp. 43-78).
- [18] Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). Watermarking digital image and video data. A state-of-the-art overview. *IEEE Signal processing magazine*, 17(5), 20-46.
- [19] Voyatzis, G., & Pitas, I. (1998). Digital image watermarking using mixing systems. *Computers & Graphics*, 22(4), 405-416.
- [20] Pitas, I. (1998). A method for watermark casting on digital image. *IEEE Transactions on Circuits and Systems for Video Technology*, 8(6), 775-780.

- [21] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, 6(12), 1673-1687.
- [22] Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005*. (pp. 709-716). IEEE.
- [23] Gunjal, B. L., & Mali, S. N. (2011). Comparative performance analysis of DWT-SVD based color image watermarking technique in YUV, RGB and YIQ color spaces. *International Journal of Computer Theory and Engineering*, 3(6), 714.
- [24] Jadav, R. A., & Patel, S. S. (2010). Application of singular value decomposition in image processing. *Indian Journal of Science and Technology*, 3(2), 148-150.
- [25] Kong, F., & Peng, Y. (2010, July). Color image watermarking algorithm based on HSI color space. In *Industrial and Information Systems (IIS), 2010 2nd International Conference on* (Vol. 2, pp. 464-467). IEEE.
- [26] Zhang, Y., Wang, J., & Chen, X. (2012, May). Watermarking technique based on wavelet transform for color images. In *2012 24th Chinese Control and Decision Conference (CCDC)* (pp. 1909-1913). IEEE.
- [27] Kornblum, J. D. (2008). Using JPEG quantization tables to identify imagery processed by software. *Digital Investigation*, 5, S21-S25.

- [28] Dey, N. (Ed.). (2016). *Classification and clustering in biomedical signal processing*. IGI Global.
- [29] Soleimannejad, F. (2004). *Six sigma, basic steps & implementation*. Author House.
- [30] Porwik, P., & Lisowska, A. (2004). The Haar-wavelet transform in digital image processing: its status and achievements. *Machine graphics and vision*, 13(1/2), 79-98.
- [31] Pan, V. Y., & Chen, Z. Q. (1999, May). The complexity of the matrix eigenproblem. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing* (pp. 507-516). ACM.
- [32] Shatnawi, M. K. A., & Shatnawi, H. A. (2014, September). A performance model of fast 2D-DCT parallel JPEG encoding using CUDA GPU and SMP-architecture. In *High Performance Extreme Computing Conference (HPEC), 2014 IEEE* (pp. 1-6). IEEE.
- [33] Kang, G. S. (2010, September). Blind digital image watermarking using adaptive casting energy in different resolutions of wavelet transform. In *Computer and Communication Technology (ICCCT), 2010 International Conference on* (pp. 210-215). IEEE.