ROBUST IMAGE-ADAPTIVE WATERMARKING SCHEME WITH STRENGTH FACTOR ANALYSIS

A thesis submitted

in fulfillment of the requirement for the award of degree

of

DOCTOR OF PHILOSOPHY

Submitted By:

NAVNEET YADAV

REGISTRATION NUMBER: 950906012

UNDER THE SUPERVISION OF

DR. KULBIR SINGH

ASSOCIATE PROFESSOR, ECED

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

THAPAR UNIVERSITY, PATIALA-147004

AUGUST 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "**Robust Image-Adaptive Watermarking Scheme with Strength Factor Analysis**", for the award of degree of **Doctor of Philosophy** in Electronics and Communication Engineering Department (ECED), Thapar University, Patiala, is an authentic record of my own work carried out under the supervision and guidance of Dr. Kulbir Singh, Associate Professor, ECED, Thapar University, Patiala.

The results presented in this thesis have not been submitted in part or in full to any other University or Institute for the award of any degree or diploma.

(NAVNEET YADAV)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge and the contents of the thesis have reached the requisite standard.

Dr. Kulbir Singh
Associate Professor, ECED
Thapar University,
Patiala, India

ACKNOWLEDGEMENTS

I thank almighty **GOD** and my spiritual Guru **Shri Ashutosh Maharaj ji** for the beginning and completion of this research work. The divine blessings have helped me throughout this work. I would like to express my sincere, humble and deep sense of gratitude to my supervisor **Dr. Kulbir Singh**, Associate Professor, Department of Electronics and Communication Engineering, Thapar University, Patiala, for his continuous motivation and support throughout the course of this work. During the years of research, I remember no occasion when he could not spare time to discuss my research problems. I understood the depth and improvement in research work through his patient and persistent advisories. The enthusiastic guidance and constructive comments during stimulating discussions aided a lot to the success of this thesis.

I am highly thankful to **Dr. Sanjay Sharma**, Professor and Head, Department of Electronics and Communication Engineering, Thapar University, Patiala and **Dr. Rajesh Khanna**, Professor, Department of Electronics and Communication Engineering, Thapar University, Patiala for their continuous support and encouragement in my research work. I would like to thank **Dr. Anil Verma**, Associate Professor, Department of Computer Science and Engineering, Thapar University, Patiala for his guidance and cooperation. I am also thankful to **Dr. Ankush Kansal**, **Dr. Sanjay Kumar** and **Dr. Navdeep Goel** , my fellow researchers at Thapar University, Patiala.

My special thanks are due for my friends **Dr. Harpal Singh**, Professor, Chandigarh Engineering College, Chandigarh and **Mr. R. K. Choudhary**, Asst. Professor, Maharaja Agrasen Institute of Technology, Delhi. They have very generously obliged me with their valuable time for the discussions on my research work.

I am thankful to my parents for their blessings and encouragement. Last but not the least I am highly indebted to my wife **Sadhana** for her unflinching support throughout the period of my research work. In fact I have no words to express my gratitude towards her. She made me concentrate on my work while taking very good care of all other things. I would like to acknowledge the support and love of my ten years old son **Vassu**, to whom I could not give enough time because of my research work.

Navneet Yadav

ABSTRACT

Towards the end of 20th century digitalization had started to spread in all forms of the technology related areas. Around the same time internet had also begun to turn the whole world into a global village. Though digital form of data had many benefits over its analog counterpart like ease of storage and transmission, still a lot of multimedia content providers were skeptical of it due to the fear of probable copyright violation by the high quality duplication possible with the digital data. As necessity breeds the invention, watermarking techniques came in the forefront to tackle this problem. In watermarking a secret and invisible data is hidden in the digital content. This secret data could be a logo or some other information for correctly identifying the original owner of the content. At the time of conflict the original owner could easily prove his ownership by extracting the hidden information from the digital content.

A lot of research work carried out in the watermarking field, emphasized the use of perceptually significant areas of the image for robust watermarking. HVS models facilitated the use of certain frequencies and chromatic components for embedding the watermark, towards which the human eyes have low sensitivity. Many image-adaptive techniques espousing these two doctrines of robustness and imperceptibility have been proposed. Following the footsteps of the preceding researchers, the presented work is an effort to provide better and less complicated robust watermarking techniques by applying image-adaptive measures.

In the available literature there is no study to suggest if any one size of block segmentation in image could provide better robustness than the other size of block segmentation for the same watermarking technique. In the presented work three sizes of block segmentations (8×8, 16×16 and 32×32) have been used in the proposed DWT based semi-blind image-adaptive watermarking technique. By comparing the results of these block segmentations it was found that 8×8 sized block segmentation is most predisposed to augment the robustness of an embedded watermark.

Dynamic strength factor is used in the presented technique for better control over the quality of the watermarked image. By using the dynamic strength factor watermarked image of any desired quality can be obtained. In this thesis all the watermarked images have been kept at PSNR value of 45 dB, because PSNR value of 45 dB is an acceptable measure of very good visual quality for the images. The value of dynamic strength factor for a particular block depends

on the standard deviation of the low frequency DWT coefficients belonging to that block. In this way the image-adaptivity propagates to the very basic building blocks of the image and hence helping to make the watermarking technique more robust. The proposed technique outperforms many techniques in literature by providing better robustness of the extracted watermark when exposed to various watermarking attacks.

A hybrid watermarking technique which uses DWT, SVD and DCT is proposed next. Dynamic strength factor in this technique is derived from the standard deviations of the DCT coefficients belonging to the selected blocks for watermark embedding. When exposed to the common watermarking attacks this hybrid technique shows better performance than the DWT based technique and two established techniques of literature.

In the quest to find an even better robust watermarking another hybrid watermarking technique is proposed which uses DWT, SVD and WHT. Three local properties of the image are used to derive three dynamic strength factors of the proposed technique. Out of the three versions of the proposed technique using three strength factors, one version that uses entropies of the watermarking blocks provides the best results. This version of the proposed technique called as DWT-SVD-WHT (entropy) shows much better performance than the previously proposed two techniques and many of the other watermarking techniques of literature. So this could be termed as the most robust watermarking technique presented in this thesis.

As the proposed techniques are semi-blind in nature, side information generated in the watermark embedding is used in the extraction of watermark. Security of the side information has been provided by an innovative method. This method ensures that even if side information gets intercepted illegitimately, there is only less than half percent chance that it can be used to detect and destroy the watermark. An encoding method has also been used which provides an additional security to the side information.

List of Publications

Accepted/ Published

[P1]. Yadav N. and Singh K., (2013), Robust image-adaptive watermarking using an adjustable dynamic strength factor, *Signal, Image and Video Processing*. DOI 10.1007/s11760-013-0607-2. (**SCI Indexed, Impact Factor 1.43**)

[P2]. Yadav N. and Singh K., (2015), An efficient robust watermarking scheme for varying sized blocks, *Turkish Journal of Electrical Engineering and Computer Sciences*. (**SCI Indexed, Impact Factor 0.407**)

[P3]. Yadav N. and Singh K., (2015), Transform domain robust image-adaptive watermarking: Prevalent techniques and their evaluation, *IEEE International Conference on Computing, Communication and Automation* (*ICCCA 2015*), Galgotias University, Uttar Pradesh, India, May 15-16, pp. 1121-1126, DOI 10.1109/CCAA.2015.7148543

Communicated

[P4]. Yadav N. and Singh K., Hybrid watermarking algorithm based on DWT, SVD and Walsh-Hadamard transform using strength factors derived from image properties, *Journal of Communications Technology and Electronics.* (**SCI Indexed, Impact Factor 0.388**)

[P5]. Yadav N. and Singh K., DWT, SVD and DCT based hybrid watermarking using flexible strength factors derived from local image properties, *Malaysian Journal of Computer Science*. (**SCI Indexed, Impact Factor 0.5**)

LIST OF ABBREVIATIONS

2D	Two Dimensional
BER	Bit Error Rate
CDMA	Code Division Multiple Access
CHT	Complex Hadamard Transform
DCT	Discrete Cosine Transform
DMT	Discrete Multiwavelet Transform
DRPE	Double Random Phase Encoding
DTCWT	Dual Tree Complex Wavelet Transform
DWT	Discrete Wavelet Transform
FRIT	Finite Ridgelet Transform
FWHT	Fast Walsh-Hadmard Transform
FWT	Fractional Wavelet Transform
GA-BPN	Genetic Algorithm-Back Paradigm Network
GMM	Gaussian Mixture Model
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
JND	Just Noticeable Difference
JPEG	Joint Photographic Expert Group
KLT	Karhunen-Loeve transform
LFR	Local Feature Region
MSE	Mean Square Error

MWT	Multiband Wavelets Transformation
NUJNCD	Non-Uniform Just Noticeable Color Difference
OFDM	Orthogonal Frequency Division Multiple Access
PSNR	Peak Signal to Noise Ratio
PSO	Particle Swarm Optimization
QFT	Quaternion Fourier Transform
QIM	Quantization Index Modulation
RDM	Rational Dither Modulation
RDWT	Redundant Discrete Wavelet Transform
SCDFT	Spatiochromatic Discrete Fourier Transform
SDE	Self-adaptive Differential Evolution
SDMI	Secure Digital Music Initiative
SIFT	Scale Invariant Feature Transform
SVD	Singular Value Decomposition
SVR	Support Vector Regression
WHT	Walsh Hadamard Transform

LIST OF SYMBOLS

$f(x,y)$	Input image signal
$F(k,l)$	2D-DCT
$\psi_l(x)$	Wavelet Function
W_φ	Approximation coefficients of 2D-DWT
W_ψ^i	Detailed coefficients of 2D-DWT
U	Left singular vector
V	Right singular vector
S	Diagonal vector
V^T	Transpose of V
Π	Product representation
Σ	Summation representation
$H(u,v)$	2D Hadamard transform
Θ	Kronecker product representation
$T_L[i,j]$	Visual sensitivity matrix
$T_L[i,j,k]$	Watson's modified luminance based threshold matrix
$s[i,j,k]$	Watson's contrast masked threshold matrix
$t_{\lambda,\theta}$	Visibility threshold value
λ	Decomposition level
θ	Orientation angle
f	Spatial frequency of level λ

a, k, f_0	Constant values determined via psychological experiments in Watson's DWT based perceptual model
g_θ	Experimentally determined constant for each orientation θ
$S_l^\theta(i, j)$	Weighting function in Barni's HVS model
$\Theta(l, \theta)$	Sensitivity to noise change in the frequency bands
$\Lambda(l, i, j)$	Local brightness
$\Xi(l, i, j)$	Local texture activity
β (i, j)	Noise sensitivity coefficient in Podilchuk's HVS model
$f(i, j)$	Noise free host image
$g(i, j)$	Watermarked image
Max_f	Maximum pixel value in the host image
σ	Standard deviation
$\bar{x}$	Mean Value of the Observations
DSF	Dynamic strength factor
ρ	Adjusting parameter of the denominator of *DSF*
H	Walsh-Hadamard coefficient matrix before embedding watermark bit
H_{emb}	Modified Walsh-Hadamard coefficient matrix after embedding watermark bit
μ_i	Mean of a WHT coefficients matrix obtained from any one of the 8×8 high entropy blocks
μ_{max}	Maximum mean among all the WHT coefficients matrices
ε_i	Entropy value of any one of the selected 8×8 high entropy blocks
ε_{max}	Maximum entropy among all the selected 8×8 high entropy blocks

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

IN the last few years there has a been tremendous growth of internet. Now the internet is being used in every stratum of society and it has reached to the very remote parts of the world also (Ali, 2015). The growth of internet has helped the multimedia content owners to distribute their image, audio or video data around the world very efficiently and economically. But it has also made the distribution of unauthorized and pirated copies of the proprietary data very easy (Hartung and Kutter, 1999). Previously piracy of music or movies required some kind of physical exchange. But in the today's times, an unauthorized media of any type existing on a computer can be distributed very easily to anyone irrespective of the distance. Digital watermarking is a technology which provides deterrence against this menace. By using robust digital watermarking, an authentic owner hides his logo, digital signature or any other information in his digital content, which he can retrieve easily whenever there is a need to prove his ownership (Wolfgang and Podilchuk, 1999).

1.1 HISTORICAL PERSPECTIVE

History of the watermarking runs parallel with the history of paper. Paper industry started to use the watermarking right from its inception. The earliest known usage has been to keep track of the brand of paper and the mill producing it, in order to clearly identify the authenticity of the paper. Afterwards watermarking was used to verify the composition of paper. As the paper currency came into circulation and a large number of commercial exchanges were being done by using it, the problem of counterfeit currency also began. Watermarking proved quite handy to deal with this problem. Presently watermarking of paper, currencies and postage stamps is being done in a large number of countries to make counterfeiting more difficult.

In the modern times, similar problems have cropped up in the digital world. Protection of intellectual property rights of the genuine owner and authentication of the digital content

has become a huge concern. The concept of watermarking was therefore adapted to the digital world and christened as digital watermarking. Digital watermarking became an active field of research in the early nineties. Komatsu and Tominaga (1988) used digital watermarking for identifying the unauthorized copies. They embedded a clandestine label into an authorized copy using slight modification on redundant information. Although there were several publications after that, a major paper (Cox *et al.*, 1997) was the starting point of more intensified research. This paper recommended image-adaptive watermarking to increase the robustness of the watermark. Some other noticeable papers were also published in the quick succession advocating the use of image-adaptive watermarking for enhanced robustness of the watermark (Podilchuk and Zeng, 1998; Wolfgang and Podilchuk, 1999 etc.). Various kinds of image-adaptive techniques have been proposed in recent years to increase the robustness of watermark (Li and Cox, 2007; Moon *et al.*, 2007; Akhaee *et al.*, 2009; Liu and She, 2010; Maity and Kundu, 2011; Niu *et al.* 2011; Ali and Ahn, 2014 etc.).

The vigorous scientific interest in digital watermarking has propelled its use in the industries also. The music industry came up with the Secure Digital Music Initiative (SDMI) in 1999, in order to create an environment for the legitimate distribution of digital music. In addition, several companies (e.g. Digimarc Corporation, Alpvision and Alpha-Tec) specializing in digital watermarking have also come into existence.

1.2 DIFFERENCE IN WATERMARKING, STEGANOGRAPHY AND ENCRYPTION

In steganography information is communicated from one place to other in a covert manner. The goal in a steganography technique is to hide the information in an innocuous message in such a way that no one could suspect the very existence of any hidden information. Although both steganography and watermarking use information hiding still their objectives and conditions are quite different from each other. In watermarking, host data (i.e. image and voice etc.) and embedded data (i.e. watermark) are both equally important while in steganography the embedded data or the hidden information is the only important entity.

The main difference in watermarking and encryption lies in the fact that watermarking does not confine the data access while in encryption the messages are encoded to make them

illegible for any unauthorized person. But once decrypted, there remains no protection for the data. In the case of watermarking, if the proprietorship of a digital document comes under suspicion, then embedded watermark can be extracted to recognize the identity of real owner.

1.3 WATERMARKING VS. COMMUNICATIONS

Any watermarking scheme is very similar to a communications system as described by Arnold *et.al*. (2003). The goal in the watermarking system is basically the same as in the communication system i.e. introducing some information into a medium (called a channel) and then trying to extract it as reliably as possible. A watermark embedder could then be seen as the transmitter in the communication chain, the watermark extractor as the receiver and the host signal as the communication channel.

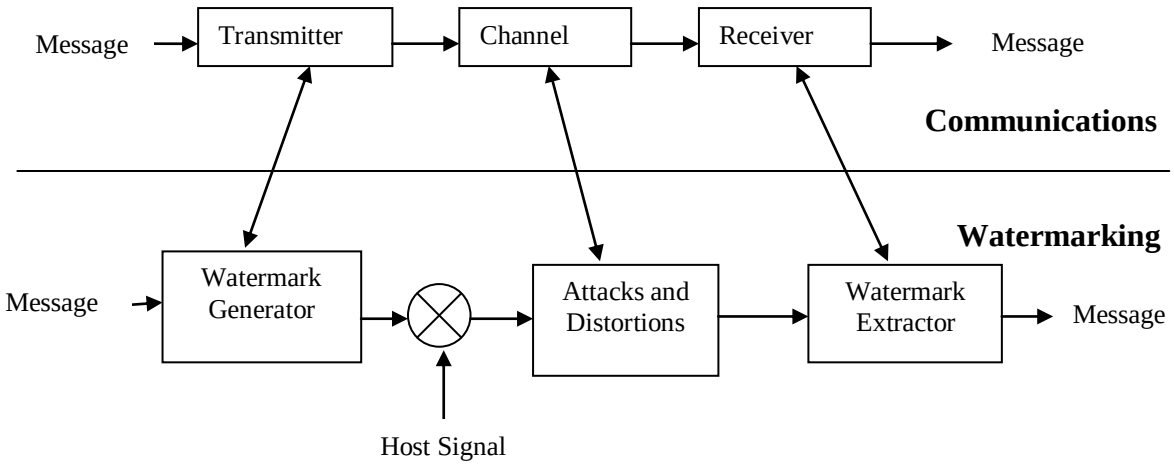


Figure 1.1 Similarity between watermarking and communication (Adopted from Arnold *et al.* 2003).

The channel model depends on the watermarking scenario and the amount of information available in the watermark extraction process.. If a copy of the non-watermarked host signal is available, then we have a channel with the additional information that can be used to improve the extraction process.

In a practical application of a watermarking scheme, the watermarked signal may suffer additional alterations caused by signal processing manipulations during distribution and storage (e.g. compression) or other distortions due to digital to analog or analog to digital

conversions. All these sources of distortions can be included in our communications model as part of the channel.

1.4 CLASSIFICATION OF WATERMARKING TECHNIQUES

Classification of watermark techniques is done based on their application areas and purposes. Lee and Jung (2001) have mentioned that watermarking techniques can be classified according to the watermark robustness, data required for extraction, perceptivity of watermark, processing method, host media type and inserting watermark type.

Classification According to the Watermark Robustness

i). **Robust Watermarking:** In this watermarking, owner's logo or copyright information is embedded as watermark in the host media. Embedded watermarks must be robust to protect the owner's identity from various attacks.

ii). **Semi-Fragile Watermarking:** Semi-fragile watermarks are capable of bearing the non malicious attacks i.e. common signal processing operations like Joint Photographic Expert Group (JPEG) compression, low pass filtering etc. but are fragile against the malicious or intentional attacks.

iii). **Fragile Watermarking:** Fragile watermarks are designed to be easily destroyed if a watermarked image is manipulated in the slightest manner. This type of watermarking is used for the authentication of the original content.

Classification According to Data Required For Watermark Extraction

i). **Non-blind watermarking:** This type of watermarking is also called private watermarking. In this watermarking host image is required at the time of extraction of watermark.

ii). **Semi-blind watermarking:** This watermarking is also called semi-private watermarking. In this watermarking host image is not required at the time of extraction but some side information is required to extract the watermark. Side information contains data related to the watermark embedding.

iii). **Blind watermarking:** This watermarking is also called public watermarking. It does not require the host image at the time of extraction.

Classification According to Processing Method

i). **Spatial Domain Watermarking:** In spatial domain watermarking direct modifications are made into the image pixels.

ii). **Frequency Domain Watermarking:** In frequency domain watermarking modifications are made into the transform coefficients.

Classification According to Perceptivity of Watermark

i). **Visible Watermarking:** This watermarking is mainly used for inserting a visible logo and trademark. Here watermark is overwritten on the covering medium.

ii). **Invisible Watermarking:** Invisible watermark is embedded into the host image by using the limitations of human visual system (HVS) and attributes of the host image.

Classification According to Host Media Type

i). **Text Watermarking:** In this watermarking, watermark is inserted in the font shape and the space between characters and line spaces.

ii). **Image Watermarking:** It embeds special information to an image and detects or extracts it later for ownership confirmation.

iii). **Video Watermarking:** It is an extension of image watermarking. This method requires real time extraction and robustness for compression.

iv). **Audio Watermarking:** In this watermarking host media is audio. It needs the watermark to be inaudible and robust.

.

Classification According to Inserting Watermark Type

i). **Noise Type Watermarking:** In this category embedded watermark is the sequence of pseudo noise, Gaussian random noise etc.

ii). **Image Type Watermarking:** Binary image, logo or label etc. is embedded as a watermark in this category. Advantage of this watermarking is that extracted watermark is visually distinguishable.

1.5 APPLICATIONS OF WATERMARKING

A few most common applications mentioned by Furht *et.al.* (2005) are as following:

- Owner Identification
- Data Authentication
- Copy and Playback Control
- Fingerprinting
- Broadcast Monitoring
- Medical applications

1.6 CHARACTERISTICS OF WATERMARK

The main characteristics of a watermark summed up by Zhang (2009) are as following:

i). **Robustness:** .Watermark should be able to resist signal processing operations such as image enhancement, lossy compression, D/A and A/D conversion, resampling, quantizaiton, etc.

ii). **Imperceptibility:** Watermark should neither be discernible to human eyes nor hearable by the human ears.

iii). **Capacity:** Capacity is the maximum number of bits that can be embedded in an image under the limiting conditions of detection probability, false alarm probability and fidelity between the original image and the watermarked image.

iv). **Fidelity:** Fidelity is the measure of similarity between the host image and the watermarked image.

1.7 IMAGE-ADAPTIVE WATERMARKING AND STRENGTH FACTOR

Watermarking in the frequency domain is more preferred over the spatial domain watermarking because in spatial domain watermarking direct modifications are made into the image pixels while in the frequency domain watermarking, modifications are made into the transform coefficients. Also some transforms have properties like energy compaction which are very useful in the watermarking. In section 1.3, it has been shown that watermarking process is analogous to the communication system and the watermarked image is equivalent to the channel in the communication system. Similar to channel, which has the maximum

probability of noise occurrence, a lot of distortion or error could affect the watermarked image. The cause of this distortion could be lossy compression, geometric operations like scaling or cropping, image enhancement operations like increasing of contrast and histogram equalization, resampling, requantization, A/D and D/A conversions etc.

According to Cox *et al.* (1997) to avoid the effects of these distortions, the watermark should be embedded in the visually significant parts of the image. Using any type of image property or characteristic for embedding of the watermark is called image-adaptive or image dependent watermarking. Spread spectrum watermarking is done in the transform domain by which the watermark is spread across a large number of transform coefficients. Therefore in any one frequency component the watermarking content is very negligible and could not be determined. But as the location and content of the watermark is known to the watermarking process, it is possible to extract the complete watermark at the receiving end. Perceptual models or masks designed by using the limitations of the Human Visual System (HVS) are also used in image-adaptive watermarking. By using the perceptual models or masks those regions in the visually significant parts of the image are known that can bear some additional data without being perceptible. The watermark is then embedded in those regions.

Also as asserted by Cox *et al.* (1997) each coefficient in the frequency domain has an ability to carry some extra information. This information carrying ability varies from one coefficient to another. Strength factor in the watermarking process determines how much a frequency coefficient can be modified in accordance with its information carrying ability so that it does not affect the perceptual fidelity of the data. Assuming H is a group of transform coefficients of the image, W is a group of watermark bits and H' is a group of watermarked transform coefficients, given as following-

$$H \in \{h_1, h_2, h_3, \ldots\ldots\ldots h_n\}$$
$$W \in \{w_1, w_2, w_3, \ldots\ldots\ldots w_n\}$$
$$H' \in \{h'_1, h'_2, h'_3, \ldots\ldots\ldots h'_n\}$$

Watermark embedding using additive strength factor SF is done as following-

$$h'_i = h_i + SF.w_i \qquad (1.1)$$

Watermark embedding using multiplicative strength SF is done as following-

$$h'_i = h_i (1 + SF.w_i) \qquad (1.2)$$

And watermark embedding using exponential strength factor *SF* is as following-

$$h'_i = h_i (e^{SF \cdot w_i}) \quad (1.3)$$

Equation (1.1) is used when h_i values do not have very large variations among them. But if h_i values have very wide variations then use of equations (1.2) and (1.3) would be more appropriate. Experiments with a large number of images, watermarks and transforms help to find the correct relationship for the watermark embedding.

1.8 MOTIVATION

Main use of watermarking is in the copyright/ownership protection of the digital content. Robust watermarking is used in this application. Most of the research work in robust watermarking is being done in frequency domain as watermarking in the frequency domain is more robust and secure than spatial domain watermarking.. In the frequency domain, watermarking could be done using spread spectrum method or Quantization Index Modulation (QIM). But the watermarking using QIM is found to be very sensitive to the scaling of signal and hence very feebly resistant against the probable malicious attacks. On the other hand, spread spectrum based watermarking poses much stronger resistance against the malicious and non-malicious attacks. Also spread spectrum based watermarking has lesser complexity level and multiple watermarks could be embedded using it. Therefore robust watermarking using spread spectrum method is more preferred over the QIM method. As the internet has now become accessible to a large population of the world, necessity of robust watermarking to protect the copyrights of the content owners is increasing day by day. So, there is still a wide scope of research in this area.

A lot of image-adaptive watermarking techniques are being proposed by the researchers as they are more robust than the non-image-adaptive techniques. There is a need to thoroughly study these techniques. There is a scope to find out more watermarking techniques where many image-adaptive measures could be applied simultaneously to obtain better robustness of the extracted watermark against a large number of watermarking attacks.

In most of the watermarking techniques, image is segmented into the into the smaller, non-overlapping image pixel blocks for the purpose of watermark embedding. There has not

been any study which attempts to find out the block segmentation size that causes least error in the extracted watermark.

Most of the robust watermarking techniques use optimized strength factor which has a constant value for all the blocks of the image. There is a scope to find out a strength factor which may have a unique value for every block of the image. Also there is a scope to find out a property of the image, the use of which in the strength factor formation causes least error in the extracted watermark.

1.9 CONTRIBUTION OF WORK

- In this work a dynamic strength factor has been introduced which can be customized according to the PSNR requirements of the watermarked image for an acceptable level of error in the extracted watermark.
- Robustness and imperceptibility are considered opposing requirements. But there are hardly any proofs of this fact in the literature in the form of graphical plots linking Peak Signal to Noise Ratio (PSNR) (dB) of watermarked image with Bit Error Rate (BER) (%) of extracted watermark. In the presented work this inverse relationship has been shown between robustness and imperceptibility in the form of graphical plots.
- In this work three block segmentation sizes (8×8, 16×16 and 32×32) have been used with a proposed Discrete Wavelet Transform (DWT) based watermarking technique and their robustness results are compared by applying the common watermarking attacks. From the results it is concluded that use of 8×8 block segmentation size produces best robustness results.
- The presented watermarking techniques in the work are semi-blind. Very reliable security arrangements have been made for the side information. An encoding technique for sending the side information has also been provided which enhances its security even more.
- A hybrid technique using DWT, Singular Value Decomposition (SVD) and Discrete Cosine Transform (DCT) is proposed in this work. This technique shows better performance than the earlier DWT based technique against the common watermarking attacks.

- Another hybrid technique using DWT, SVD and Walsh Hadamard Transform (WHT) is presented in this work. One version of this technique, which uses dynamic strength factor derived from entropies of the watermark embedding blocks, has been found experimentally as be the best robust watermarking technique of this work.

1.10 THESIS ORGANIZATION

Chapter 1 presents the introduction, classification of watermarking techniques, image-adaptive watermarking, motivation, contribution of work and organization of the thesis.

Chapter 2 presents the literature review of the image-adaptive watermarking, HVS models and various transforms used in the watermarking. Watermarking attacks, quality metrics, objectives of research and research methodology are also described in the chapter.

Chapter 3 explores the relation between robustness of the watermarking scheme and block segmentation size by using DWT based semi-blind watermarking technique. Concept of dynamic strength factor is introduced. Here three block segmentation sizes (8×8, 16×16 and 32×32) are compared by applying them in same host images and embedding the same watermarks.

In **Chapter 4** detailed analysis of dynamic strength factor is presented. Performance of the presented watermarking scheme is observed by embedding small, medium and large sized watermarks in various host images. Comparisons with established techniques of watermarking are also made by applying common watermarking attacks. Provisions to secure side-information have also been made.

Chapter 5 presents a hybrid watermarking scheme using DWT, SVD and DCT. Use of dynamic strength factor is done in the presented hybrid scheme too. Proposed scheme is compared with three well known watermarking techniques present in the literature.

In **Chapter 6** another hybrid watermarking scheme using DWT, SVD and WHT is introduced. Here three types of dynamic strength factors derived from three local properties of the image are used. Presented hybrid scheme is compared with established watermarking techniques of literature and the watermarking techniques proposed in the previous chapters.

In the **Chapter 7** conclusions are drawn. The results and inferences are summarized and future scope of the presented work is discussed.

CHAPTER 2

LITERATURE REVIEW

IN this chapter, the transforms used in the proposed robust image-adaptive watermarking schemes, HVS models, block segmentations in watermarking and methods to make the watermarking techniques image-adaptive are discussed. Hybrid techniques used in the robust image-adaptive watermarking have also been discussed. Common watermarking attacks and quality metrics used for the performance evaluation of the watermarking techniques are talked about next. Research gaps based on the literature review, research objectives and research methodology are taken up in the end.

2.1 INTRODUCTION

Transform domain techniques are best suited for robust image-adaptive watermarking. Firstly because no changes are made into to the image-pixels and secondly because a lot of image characteristics elicit themselves in the transform domain only. Many HVS models have been proposed by the researchers, which are used in various image processing applications including watermarking (Watson, 1993; Barni *et al.* 2001). Study of the HVS helps us to know about that part of the frequency spectrum and chromatic components towards which HVS is less sensitive. The watermark could be embedded in these frequency regions or chromatic components of the image to make it imperceptible to the human eyes.

In most of the watermarking techniques, the first step towards watermark embedding is segmentation of the host image into the squared blocks. Many properties related to these blocks can be used for watermarking. Adapting any watermarking system in accordance with the characteristics or properties of the image helps it to become more robust and transparent (Podilchuk and Zeng, 1998). Many methods have been used over the years to make the watermarking schemes image-adaptive. In recent times, hybrid watermarking techniques using more than one transform are also being used increasingly. These techniques benefit from the advantages of all the transforms being employed in the watermarking.

2.2 TRANSFORMS EMPLOYED IN WATERMARKING

In this section DWT, DCT, SVD and WHT transforms are discussed briefly along with their histories of development.

2.2.1 Wavelet Transform

The wavelet transform gives a time-frequency illustration of the signal. The genesis of wavelet transform is found in the pioneering research work done by Alfred Haar on the orthogonal function systems more than hundred years ago (Haar, 1910). His research work initiated the development of a set of rectangular basis functions. From the basis (or father) function mother's, daughters', sons', granddaughters' and grandsons' functions were achieved by successive scaling and translation. Haar explained that a signal can be represented at different levels of details by using these functions.

After the Haar's work not much of the research work was reported in the field of wavelets for the next nearly twenty five years. In the decade of 1930s a physicist Paul Levy applied the Haar's basis function in the study of the Brownian motion. He found out that scale changing Haar's basis function was more useful than the Fourier basis functions in the research of the Brownian motion. For the next forty years, the works of some notable scientists like John Littlewood, Richard Paley (Littlewood and Paley, 1931), Elias M. Stein (Jaffard *et al.*, 2001) and Norman H. Ricker (Ricker, 1953) carried forward the research into the field of wavelet transforms. A very remarkable breakthrough in the research of wavelet transforms came from Jean Morlet who invented and put into use the method of scaling and shifting of the analysis window functions (Mackenzie, 2001). The theory of development of the wavelets was first reported in the paper (Grossmann and Morlet, 1984). This paper explained that any signal can be transformed into a wavelet. Afterwards it can be retransformed into the original signal with no harm of information. Along with this impactful paper many other research papers were published which contributed significantly into the development of wavelet transform theory (Stromberg, 1983; Grossmann et al., 1985, 1986; Newland, 1983).

The concept of multiresolution analysis in the wavelet transform that made it hugely popular was proposed in a research paper on orthogonal wavelets (Meyer, 1989). Some other research papers centered on the multiresolution analysis were also published in the close succession (Mallat, 1989 a, b) and (Meyer, 1993). Around the same time, Ingrid Daubechies

employed multiresolution analysis to create her own family of wavelets. She introduced a family of compactly supported orthogonal wavelet systems with arbitrarily high, but fixed regularity using construction methods related to filter banks (Daubechies, 1988). Properties such as compact support, orthogonality, regularity, and continuity were offered by these wavelets and made them very useful in signal and image analysis. As a result, the Daubechies wavelets are now some of the most commonly used wavelets.

Wavelets have been used for different signal and image processing applications (Vetterli and Kovacevic, 1995; Stollnitz *et al.*, 1996).

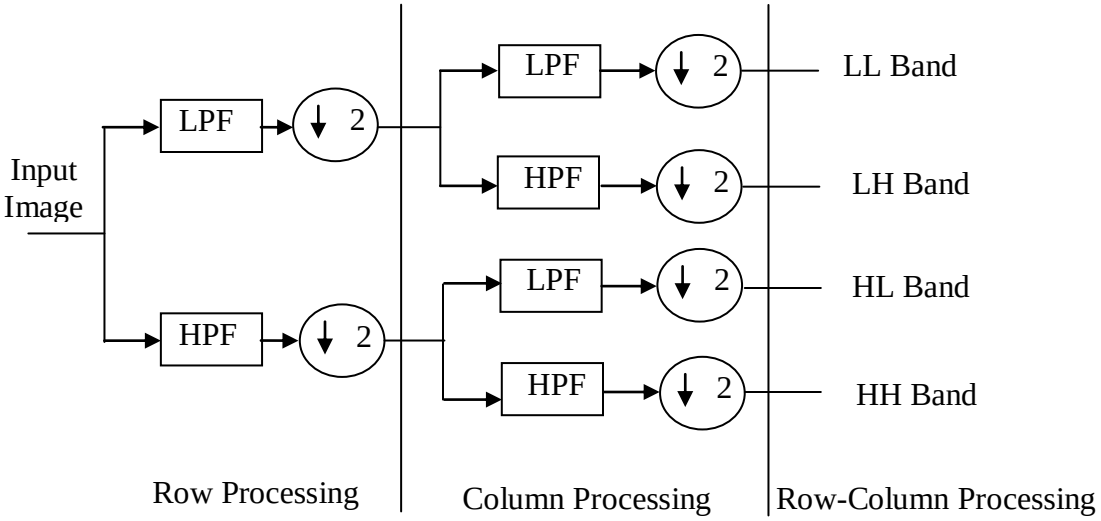


Figure 2.1 The decomposition of an input image into four subbands (Adopted from Gonzalez and Woods, 2009)

An image can be analyzed in the DWT by exposing it first to an analysis filter bank and then later on applying a down-sampling operation on it. At every decomposition stage the analysis filter bank has a low pass and high pass filter. The signal which goes from these filters gets divided into two bands. The low pass filter associated with mean operation, brings out the most important information of the signal. The high pass filter associated with a subtraction operation, brings out the complete details of the signal information. The resultant signal after the filtering operation is then down-sampled by two. A two-dimensional transform is obtained by applying two different one-dimensional transforms. In the beginning, image is filtered along the row and down-sampled by two. Obtained sub-image is then filtered along the column and down-

sampled by two. In this process the image gets divided into four bands called as HH, HL, LH and LL, as shown in Figure 2.1.

Here LL represents the least resolution approximation component while HL represents the horizontal, LH represents the vertical and HH represents the diagonal component respectively. The LL subband can subsequently be decomposed to achieve one more decomposition level. This decomposition process goes on in this manner till the required levels for a particular application are attained. The 2-level decomposition of *Lena* image is shown in Figure 2.2.

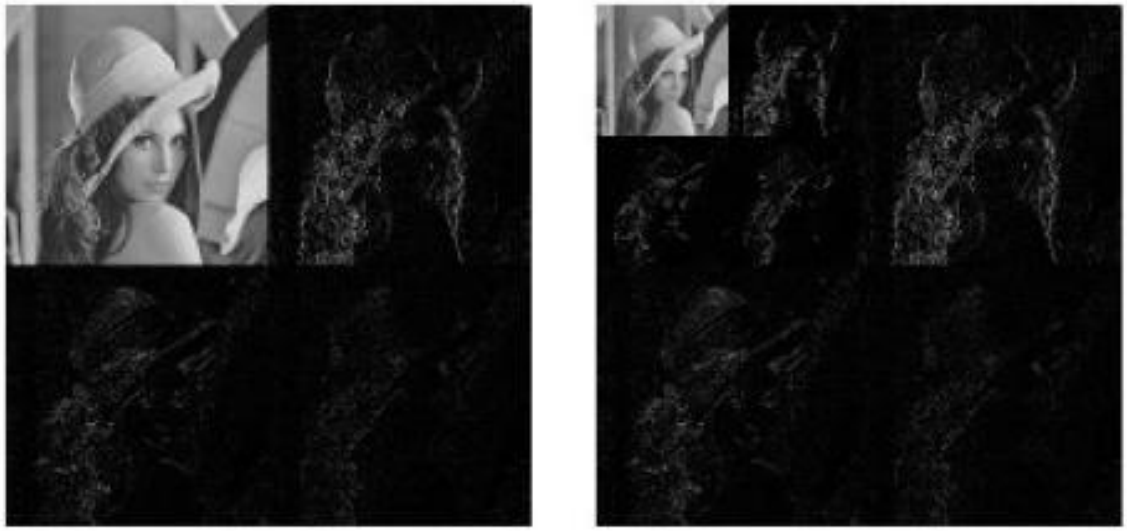


Figure 2.2 The 2-level decomposition of Lena image

The 2D-DWT of an image $f(x, y)$ of size $N_1 \times N_2$ can be expressed as:

$$W_{\varphi}(j_0, k_1, k_2) = \frac{1}{\sqrt{N_1, N_2}} \sum_{x=0}^{N_1-1} \sum_{y=0}^{N_2-1} f(x, y) \varphi_{j_0, k_1, k_2}(x, y) \tag{2.1}$$

$$W_{\psi}^{i}(j, k_1, k_2) = \frac{1}{\sqrt{N_1, N_2}} \sum_{x=0}^{N_1-1} \sum_{y=0}^{N_2-1} f(x, y) \psi_{j, k_1, k_2}^{i}(x, y) \tag{2.2}$$

where, $f(x, y)$- Original image

N_1, N_2 - Dimensions of image

$\varphi_{j_0,k_1,k_2}(x,y)$ - Two dimensional scaling function

$\psi^i_{j,k_1,k_2}(x,y)$ - Two dimensional wavelet function

i – Directional index of wavelet function

$W_\varphi(j_0,k_1,k_2)$ - Approximation coefficient matrix of 2D-DWT

$W^i_\psi(j,k_1,k_2)$ - Detailed coefficients matrix of 2D-DWT

j_0 – Any arbitrary starting scale which may be treated as j_0=0

j – A number such that $j \geq j_0$

k_1, k_2 - Coefficients of 2D-DWT

The inverse 2D-DWT is obtained as following to get back the original image $f(x, y)$.

$$f(x,y) = \frac{1}{\sqrt{N_1 N_2}} \sum_{k_1} \sum_{k_2} W_\varphi(j_0,k_1,k_2)\varphi_{j_0,k_1,k_2}(x,y)$$
$$+ \frac{1}{\sqrt{N_1 N_2}} \sum_{i=H,V,D} \sum_{j=0}^{\infty} \sum_{k_1} \sum_{k_2} W^i_\psi(j,k_1,k_2)\psi^i_{j,k_1,k_2}(x,y) \qquad (2.3)$$

2.2.2 Discrete Cosine Transform

In the late sixties and early seventies, Karhunen-Loeve transform (KLT) was considered an optimal transform for the comparison of images by the research fraternity. But at that time no efficient algorithm was available to compute it. Dr. Nasir Ahmed worked on this problem and a path breaking paper (Ahmed *et al.*, 1974) was published. This paper acquainted the scientific world with Discrete Cosine Transform or DCT. Later on Dr. Ahmed also gave an interesting firsthand account about the discovery of DCT (Ahmed, 1991).

The DCTs belong to a group of discrete sinusoidal unitary transforms having real values. Strang (1999) has shown that the family of DCT is a natural result of various combinations of homogeneous boundary conditions, which are applied to the discrete solution of a simple harmonic equation. Discretized cosine function which is the rudimentary function of the family of DCT, is the eigen function (or eigen vector) in the matrix version of the homogeneous harmonic oscillator system.

The two dimensional (2D) DCT of an image signal $f(x,y)$ of size N×N is given by

$$F(k,l) = \alpha(k)\alpha(l)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{2x+1\ \pi k}{2N}\right]\cos\left[\frac{2y+1\ \pi l}{2N}\right] \qquad (2.4)$$

where, $\alpha(k) = \sqrt{\frac{1}{N}}$ *if* $k = 0$ and $\alpha(k) = \sqrt{\frac{2}{N}}$ *if* $k \neq 0$

Also $\alpha(l) = \sqrt{\frac{1}{N}}$ *if* $l = 0$ and $\alpha(l) = \sqrt{\frac{2}{N}}$ *if* $l \neq 0$

$f(x,y)$ - Input image $F(k,l)$ - DCT transform

N - Dimension of input image x, y - Image co-ordinates

k,l - Coefficients of 2D-DCT

The 2D inverse DCT is given by

$$f(x,y) = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1}\alpha(k)\alpha(l)F(k,l)\cos\left[\frac{(2x+1)\pi k}{2N}\right]\cos\left[\frac{(2y+1)\pi l}{2N}\right] \qquad (2.5)$$

The development of many fast algorithms for the efficient implementation of the DCT has greatly helped to make this transform very popular. The main advantage of DCT is that it eliminates the redundancy between neighboring pixels of an image. As a result uncorrelated transform coefficients are obtained which can be encoded independently. Energy is bundled by DCT in the low frequency coefficients keeping the total energy of the image conserved. Therefore some high frequency coefficients could be abandoned without any appreciable loss of quality. That's the reason for a very prominent use of DCT is in the compression of images.

2.2.3 Singular Value Decomposition

History of singular value decomposition (SVD) finds its roots in the work of Gauss (Gauss, 1823). In this paper he proposed an algorithm to decompose the matrix. Gauss was also successful in obtaining the inverse of the matrix. Properties of the eigen values and eigen vectors of the symmetric system were established by Cauchy (1829). Some other research papers could be termed as stepping stones towards the development of SVD (Jacobi, 1846; Weierstrass, 1868). A remarkable survey paper traces the early history of the development of SVD (Stewart, 1993). SVD was independently developed by two mathematicians (Beltrami, 1873 and Jordan, 1874 a, b). Beltrami's algorithm had some limitations. This algorithm did not consider the degenerate matrices while reducing from bilinear form to linear form. Jordan (1874 a, b) used a lesser

known technique called deflation to overcome the limitations of Beltrami (1873). J. J. Sylvester (1889) also achieved the SVD of real square matrices. Sylvester referred to the singular values as canonical multiplier of the matrix. Autonne (1915) obtained the SVD by polar decomposition. Two other significant papers were published around the same time (Schmidt, 1907; Pickard, 1909). Proof of the SVD for rectangular and complex matrices was presented by Eckart and Young (1936). Practical methods for computing SVD was finally presented in the decade of 1950 (Kogbetliantz, 1955). Golub and Kahan (1965) provided a better method of computing SVD by using Householder transformations. A different version of this work was published after five years (Golub and Reinsch, 1970), which has now become the most popular method for computing the SVD.

The singular value decomposition of a rectangular matrix *A* could be shown as below

$$A = U\,S\,V^T \tag{2.6}$$

where, A - Any $m \times n$ matrix.

U and V - Orthonormal matrices.

S - Diagonal matrix which contains singular values of A.

The singular values appear in descending order along the main diagonal of *S.* For example,

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 \ldots\ldots\ldots \sigma_n \geq 0$$

The equation (2.6) can be written as

$$A = u_1, u_2 \ldots . u_n \begin{bmatrix} \sigma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_n \end{bmatrix} \begin{bmatrix} v_1^T \\ . \\ . \\ v_n^T \end{bmatrix} \tag{2.7}$$

The values of U and V are computed as eigen vectors of AA^T and A^TA (Strang, 1998). The singular values along the diagonal of S are achieved by taking the square root of the eigen values of AA^T and A^TA. As the singular values appear in descending order, the first singular value carries a large amount of image information. Second value also carries significant image information but less than the first one and so on.

This indicates that few singular values could be used to represent the image with little difference from the original image. It means that most of the energy of the image gets converged

into a few singular values. Now these values carrying most of the image information could be used in an image-adaptive watermarking. A very important benefit of using SVD in watermarking is that there is very little effect of any attack on the singular values obtained in SVD decomposition. SVD can be used in image compression, face recognition and texture classification also (Stewart, 1993).

2.2.4 Walsh-Hadamard Transform

The Walsh-Hadamard transform that is WHT, simply called as Hadamard transform is very closely linked with the Walsh transform, the only change being that rows of the transform matrix are re-ordered. About 150 years ago Sylvester (1867) discussed about the matrices for all orders that were powers of two. Hadamard (1893) found square matrices of orders 12 and 20 with entries ±1 which had their rows and columns, pair wise orthogonal.

These matrices, $X = (x_{ij})$, satisfied the following inequality,

$$\left|\det X\right|^2 \leq \prod_{i=1}^{n} \sum_{j=1}^{n} \left| x_{i,\,j} \right|^2$$

and so had the largest determinant value among matrices with ±1. Hadamard (1893) gave examples of Hadamard matrices for a few small orders and postulated that they exist for every order divisible by 4. Two noteworthy papers were published in the later years which contributed significantly in the development of Walsh-Hadamard transforms (Walsh, 1923; Paley, 1933). Williamson (1944) in his paper coined the name Hadmard matrices and constructed another set of matrices which were called Williamson matrices. With a limited set of conditions they were called Williamson type matrices. These matrices are used to replace the variables of a formally orthogonal matrix.

The practical application of Hadamard transform was described in a very remarkable paper which spurred the interest of scientific community in Hadamard matrices (Baumert *et al.*, 1962). The authors used Hadamard matrices for obtaining the colored pictures of extraterrestrial objects and solar system from the black and white (gray scale) pictures taken by satellites or space mission rockets. Hadamard matrices were used because of two reasons. Firstly, because they have very high error correction capability and secondly, because the Hadamard matrices of power of two are equivalent to the Walsh functions and thus all the computer processing can be

accomplished using additions which are very fast and easy to implement in computer hardware. On the other hand, multiplications are much slower and relatively difficult to implement in hardware.

Complex Hadamard matrices with entries ±1, ±*i* and pair wise orthogonal rows and columns were studied by Turyn (1970). Fast algorithms for calculating WHT were proposed by many researchers (Kennett, 1971; Manz, 1972; Beer, 1981). Because of the simplicity and speed research fraternity took interest in these transforms and used them in various applications. Kak (1971) used Walsh transforms for measuring randomness of a finite sequence. Yuen (1972) used them for testing random number sequences. Shih and Haan (1978) applied them for solving first order partial differential equations. In the more recent times Fast Walsh-Hadmard Transform (FWHT) has been found useful in many areas of digital signal filtering, face identification, telecommunications and watermarking. Multicarrier Code Division Multiple Access (CDMA) and multiband Orthogonal Frequency Division Multiple Access (OFDM) are examples of it (Mohammad *et al.*, 2008; Nema *et al.*, 2010). WHT has its benefits in the fields of image and signal processing where real time implementation may also be required.

The fundamental components of the mutually orthogonal basis vectors of a Hadamard transform are either +1 or -1, which results in very low computational complexity in the calculation of the transform coefficients.

The Hadamard matrix is symmetrical and orthogonal. The Hadamard transform of an image *f* is given as

$$g = A \times f \times A \tag{2.8}$$

where, f - Input image

g - Hadamard transform

The matrix *A* is related to the Hadamard matrix as

$$A = \frac{1}{\sqrt{N}} H_{q,q} \tag{2.9}$$

where, N - dimension of the image.

The basic Hadamard matrix for *N=2* is given as

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.10}$$

The basic vectors of the Hadamard transform are created by sampling Walsh functions too. These functions receive only the binary values +1 or -1and make a fully orthonormal basis for square integrable functions. The Hadamard matrices of higher dimensions (Jain, 2009) can be represented as

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \tag{2.11}$$

The basic Hadamard transform for the matrix $H_{4,4}$ is given as

$$H_{4,4} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{matrix} \textit{Sequency} \\ 0 \\ 3 \\ 1 \\ 2 \end{matrix} \tag{2.12}$$

Sequency - number of zero crossings of a Walsh function or the number of transitions in a basic vector of the Hadamard transform.

In terms of Kronecker product (Beer, 1981) $H_{4,4}$ is represented as

$$H_{4,4} = H_{2,2} \Theta H_{2,2} \tag{2.13}$$

The inverse Hadamard transform is given as

$$f = A' g A' \tag{2.14}$$

The inverse Hadamard transform produces the exact original image matrix. The dynamic range and magnitudes of Hadamard transform coefficients can be predicted very easily. The zero sequency term is given by

$$H(0,0) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \tag{2.15}$$

H(0,0) gives the average brightness of the image. Assuming that *f(x, y)* is a positive real function then the highest probable value for the zero sequency term is N^2A where *A* is the highest value of

f(x, y). All Hadamard coefficients other than the zero sequency term range between $N^2A/2$ to N^2A. The value of the zero sequency term is a limiting factor for the value of all other Hadamard transform coefficients.

2.3 HUMAN VISUAL SYSTEM MODELS

During the study of the robust image-adaptive watermarking techniques in transform domain it was noticed that most of the techniques which employ HVS models as image-adaptive measure have used either Watson's model or Barni's pixel-wise model. As these two are the most popular HVS models being used, they have been discussed here chronologically in sufficient detail along with the inspiration behind them. Some other noteworthy models, used by image-adaptive techniques have also been discussed briefly.

2.3.1 Watson's DCT Based Perceptual Model

Ahumada and Peterson (1992) made a human visual model to mimic the perceptual thresholds for the DCT coefficient quantization error which later on became the base for Watson's research in the same field (Watson, 1993). The basic limitation of their model was that it calculated the visibility threshold matrix in complete isolation of the image.

Watson (1993) rectified the visibility threshold matrix by using the properties of image in its calculation. Average luminance value of the display influences the visibility threshold equation. The perceptual threshold amplifies with luminance in the background and variations in the average luminance in the image result in quite significant deviations in the DCT threshold. Therefore a DCT coefficient can be modified by a bigger value before it becomes noticeable after the mean intensity of the 8×8 block has become higher. The model of Watson amends the sensitivity table $T[i, j]$ for each block k in proportion to the block's DC term. Modified luminance based threshold (Watson, 1993) is shown as

$$T_L[i, j, k] = T[i, j]\left(\frac{C_0[0,0,k]}{C_{0,0}}\right)^{a_T} \tag{2.16}$$

where, a_T - 0.649

k - Count (number) of any 8×8 image pixel block

$C_0[0,0,k]$ - DC or non-altering coefficient of the kth block of the actual image

$C_{0,0}$ - Mean of all the DC coefficients of the image's DCT transform

$T[i, j]$ - Sensitivity table

$T_L[i, j, k]$ -Luminance based threshold

Contrast masking is the decrease in the perceptivity of one image element due to the existence of one more element in its vicinity. For a DCT coefficient $C_0[i, j, k]$ and threshold $T_L[i, j, k]$, the contrast masked threshold (Watson, 1993) $s[i, j, k]$ is given by

$$s[i, j, k] = \max\left\{T_L[i, j, k], |C_0[i, j, k]|^{w[i, j]}, T_L[i, j, k]^{1-w[i, j]}\right\} \qquad (2.17)$$

where, $w[i, j]$ - constant lying in the range 0-1.

$s[i, j, k]$ -Contrast based threshold

The threshold $s[i, j, k]$ predicts about the amount by which the individual coefficients of the blocks can be modified before causing a just noticeable distortion.

2.3.2 Watson's DWT Based Perceptual Model

DWT has become a very popular and indispensable tool for image and signal processing applications. It is the basic premise for the JPEG2000 image compression standard. In DWT based image compression there is a requirement to find out a good quantization matrix to obtain high compression ratio along with safeguarding the visibility of the image. For building this matrix the perceptual boundary values of DWT coefficients in subbands and levels of DWT decomposition are required to be known.

Watson *et al.* (1997b) found these perceptual boundary values in various subbands on many decomposition levels for 9/7 biorthogonal wavelets. These boundary values are described as following:

$$\log t_{\lambda,\theta} = \log a + k(\log f - \log g_\theta f_0)^2 \qquad (2.18)$$

where

$t_{\lambda,\theta}$ - Visibility threshold value

λ - Decomposition level

θ - Orientation value

a, k, f_0 -Constant values determined via psychological experiments

f - Spatial frequency of level λ

g_θ - Experimentally determined constant for each orientation θ

Visibility boundary values represented by $t_{\lambda,\theta}$ for different decomposition levels and orientations represent the frequency sensitivity of HVS. These are image independent, so there is a need for an even more accurate model that takes into account the additional properties of HVS also.

2.3.3 Watson's Entropy Model

Entropy determines the information stored in a signal. Watson *et al.* (1997a) observed that more complexity and uncertainty is found in high entropy areas of the image, because of the large concentration of information in these parts of the image. This higher complexity causes decline in perceptual capability that causes the rise of Just Noticeable Difference (JND) thresholds. This means that higher energy watermarks can be embedded in the regions of high entropy without being perceptible.

2.3.4 Barni, Bartolini and Pive's Pixel-wise Masking Model

Barni *et al.* (2001), modified the Lewis and Knowles (1992) HVS model. Their model considers a lot of aspects like frequency band, luminance, texture and nearness to a boundary etc. They developed a masking function on pixel by pixel basis for computing the weight factors to insert the pseudorandom binary sequences into high frequency subbands of the image. In this model, the image is decomposed by wavelet transform, maximum up to four levels. Every subband is denoted by $I_l^\theta(i,j)$ where $\theta \in \{1,2,3\}$ is the orientation and $l \in \{1,2,3\}$ gives resolution level of the image. Weighting function S_l^θ is calculated as following (Barni *et al.*, 2001)-

$$S_l^\theta(i,j) = \Theta(l,\theta) \,.\, \Lambda(l,i,j) \,.\, \Xi(l,i,j)^{0.2} \tag{2.19}$$

where, $\Theta(l,\theta)$ - Sensitivity to noise change in the frequency bands

$\Lambda(l,i,j)$ - Local brightness

$\Xi(l,i,j)$ - Local texture activity

And,

$$\Theta(l,\theta) = \begin{cases} \sqrt{2}, & if\ \theta = 1 \\ 1, & otherwise \end{cases} * \begin{cases} 1.00, & if\ l = 0 \\ 0.32 & if\ l = 1 \\ 0.16, & if\ l = 2 \\ 0.10, & if\ l = 3 \end{cases} \tag{2.20}$$

$$\Lambda(l,i,j) = 1 + \frac{1}{256} I_3^3\left(1 + \left\lfloor \frac{i}{2^{3-l}} \right\rfloor, 1 + \left\lfloor \frac{j}{2^{3-l}} \right\rfloor\right) \tag{2.21}$$

$$\Xi(l,i,j) = \sum_{k=0}^{3-l} \frac{1}{16^k} \sum_{\theta=0}^{2} \sum_{x=0}^{1} \sum_{y=0}^{1} \left\lfloor I_{k+l}^0\left(y + \frac{i}{2^k}, x + \frac{j}{2^k}\right)\right\rfloor^2 \cdot Var\left\{ I_3^3\left(1 + y + \frac{i}{2^{3-l}}, 1 + x + \frac{j}{2^{3-l}}\right)\right\}_{\substack{x=0,1 \\ y=0,1}} \tag{2.22}$$

2.3.5 Other HVS Models

Osberger and Maeder (1998) proposed a model for the recognition of the visually significant sections in an image based on the contrast, luminance, location, proximity to boundary and texture of the regions. Podilchuk and Zeng (1998) gave an HVS model based on the noise sensitivity coefficient *β (i, j)*. Using this model, in the image regions having less noise sensitivity, energy of the watermark is kept high and in the image regions having high noise sensitivity, energy of the watermark is kept small. Chou and Liu (2003) proposed a perceptual model to which they named as Non-Uniform Just Noticeable Color Difference (NUJNCD). Their model generates a JND value for each pixel of a color image. Until the embedded watermark is lower than this value, human eyes would not be able to perceive any difference.

2.4 BLOCK SEGMENTATION IN WATERMARKING

There are a large number of image-adaptive watermarking techniques being used nowadays which segment the host image in smaller non-overlapping image pixel blocks. In some of these techniques, a particular property of these blocks is used for selecting the suitable blocks for watermark embedding. Some watermarking techniques make use of the frequency transforms

that are applied to the host image and suitable blocks for embedding the watermark are chosen based upon the magnitude of transform coefficients related to the blocks. Podilchuk and Wenjun (1998) emphasized the use of block segmentations in image-adaptive techniques of robust watermarking. But even before the publication of (Podilchuk and Wenjun, 1998), the practice of segmenting the host image into smaller blocks or constituents was being carried out for some time. In the two watermarking techniques proposed around the same time, 8×8 segmentation is applied on the host image and all the blocks of image are subjected to DCT. Subsequently based upon a visual masking based approach, appropriate blocks for watermark embedding are chosen (Swanson *et al.,* 1996; Huang and Shi, 1998). More recently, Ghazy *et al.* (2007) in their watermarking technique based on SVD has used block segmentation of host image. The image-adaptive watermarking method described in (Yan *et al.,* 2009), segmented the host image into small blocks. DCT is applied on these non-overlapping blocks and watermark is embedded in the DCT coefficients belonging to the blocks.

Chang *et al.* (2009) in their work divided the host image in four small images. 8×8 block segmentation was used on these small images and DCT was used in the watermarking process. In the papers (Akhaee *et al.*,2009; Kalantari *et al.*,2010; Fami *et al.*, 2012; Akhaee *et al.*, 2010), small blocks from the host image were obtained. Entropies of all the blocks were computed and blocks having high value of entropy were selected to embed the watermark. Peng *et al.*, (2010), used 16×8 sized block segmentation in their watermarking scheme. Bhatnagar *et al.* (2012) obtained a reference image by using fractional wavelet packet transform which was further segmented to achieve smaller blocks for watermark embedding. Zhu *et al.* (2013), divided the remote sensing binary image into non-overlapping blocks. The watermark was embedded by changing parity of the white pixel in the image block.

From the above discussion it is clear that in a large number of watermarking techniques host image is segmented into smaller constituents or blocks. Properties of these blocks are used in the watermarking process.

2.5 ROBUST IMAGE-ADAPTIVE WATERMARKING TECHNIQUES

A lot of research work has been going on in the field of image-adaptive watermarking in the frequency domain (Cox *et al.*, 1997; Podilchuk and Zeng, 1998). Researchers have proposed a lot of watermarking schemes by applying different types of image-adaptive measures.

Categorization of these techniques can be done in the following manner depending on the applied image-adaptive measure:

- HVS models based
- Transform coefficients' properties based
- Entropy distribution based
- Feature points extraction based

2.5.1 HVS Models Based Watermarking Techniques

In this category of image-adaptive watermarking techniques, HVS models have been used for the purpose of making the techniques image dependent Watson's HVS models for DCT (Watson,1993) as well as DWT (Watson *et al.*, 1997b) have been used extensively along with Barni's pixel-wise model (Barni *et al.*, 2001).

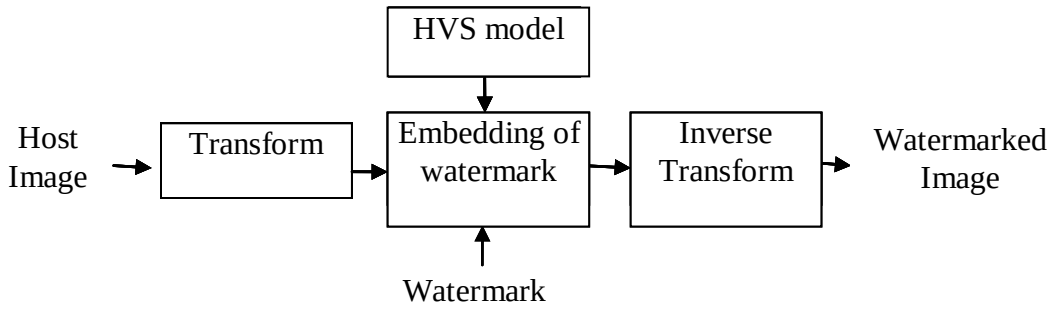


Figure 2.3 Use of HVS models in watermarking

2.5.1.1 Use of Watson's models

In the method proposed by Maity and Kundu (2011), Hadmard Transform is applied on host image and spatially dispersed watermark. Coefficients of watermark image and host image are sorted so that relatively large coefficients of watermark modulate the large coefficients of host image. Modulation function is determined by the Watson's visual model (Watson, 1993) and entropy masking model (Watson *et al.*, 1997a). Liu (2009) proposed a watermarking technique where JND profiles of all subbands of luminance and chrominance components of a color image are found in wavelet domain using Watson's model for DWT (Watson *et al.*, 1997b). Now these JND profiles are used in QIM based watermarking technique. In another QIM based

watermarking technique Li and Cox (2007), have used the modified version of Watson's DCT based perceptual model (Watson, 1993) to adaptively select the quantization step size. Podilchuk and Zeng (1998) have proposed two non-blind spread spectrum techniques which utilize Watson's DCT based visual model (Watson, 1993). Based on JND method, maximum power and maximum length of the watermark for a given image are known, subject to the transparency and imperceptibility condition. Shetty and Rodriguez (2006) also used Watson's model in their image-adaptive watermarking methods.

2.5.1.2 Use of Lewis and Knowles (1992) / Barni *et al.* (2001) models

In the watermarking technique proposed by Liu and She (2010), HVS model given by Lewis and Knowles (1992) is used. For embedding the watermark into the Dual Tree Complex Wavelet Transform (DTCWT) coefficients, JND values obtained from the HVS model are used. Al-Otum and Al-Taba'a (2009) proposed a selective pixel-wise algorithm where only high enough DWT coefficients of selected subband are used for insertion of watermark bits instead of using all the coefficients. They also proposed the extension of pixel wise and selective pixel wise methods of Barni *et al.* (2001) for color images. Zolghadrasli and Rezazadeh (2007) used the HVS models of Lewis and Knowles (1992) and Barni *et al*. (2001) to get the weighting functions for the coefficients of wavelet transform. These weighting functions along with a global watermark strength factor are used in the watermark embedding.

2.5.1.3 Use of other HVS models

Kutter and Winkler (2002) proposed their own HVS model for watermarking. In their technique local isotropic contrast measure and visibility thresholds given by the HVS model are used as means of getting image adaptivity.

Tsui *et al*. (2008) proposed two methods of watermarking the color images using Spatio Chromatic Discrete Fourier transform (SCDFT) and Quaternion Fourier transform (QFT). In the first method only chromatic component is used for watermarking while in second method using QFT, chromatic as well as luminance component is used for watermarking. HVS model given by Chou and Liu (2003) is used in both the methods. Xiao *et al.* (2005) suggested a visibility threshold model which provides JND profile for ridgelet transform coefficients. In the watermarking scheme proposed by Wu and Xiong (2010), HVS model given by Podilchuk and

Zeng (1998) has been used. In the watermarking scheme by Ghauti *et al.* (2006) a new perceptual model is proposed which is used for controlling the watermark strength. He *et al.* (2009) have also suggested a visual perception model which has been used for embedding the watermarks in the images. Two watermarks are embedded using different embedding techniques.

2.5.2 Transform Coefficients' Properties Based Watermarking Techniques

In this category of watermarking techniques inherent properties of various transforms' coefficients are used for making these techniques image adaptive. Different transforms namely DWT, DCT, contourlet transform, ridgelet transform, curvelet transform etc. are used in this category.

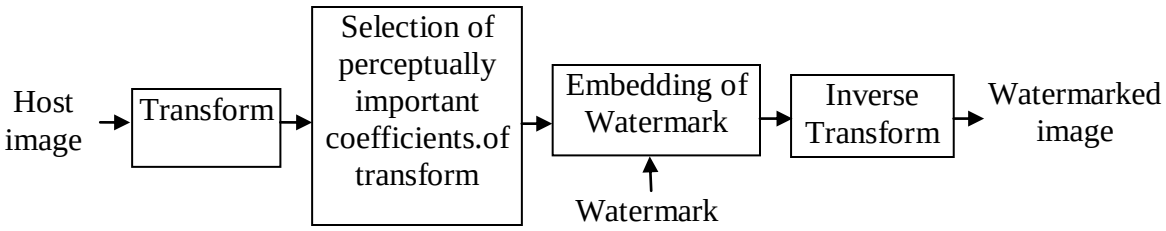


Figure 2.4 Use of the transform coefficients' properties in watermarking

2.5.2.1 Use of the properties of DWT coefficients

In the watermarking scheme of Shijie and Xin (2009), three level DWT of the host image is taken. Watermarking is done in the 2nd and 3rd level coefficients which are of low and middle frequency. Darazi *et al.* (2009) used the wavelet transform properties for watermarking. In their technique, spread transform dither modulation is used which is a variant of QIM. In this technique, a vector used in watermarking depends on the resolution, luminance, texture and edges of the image. Moon *et al.* (2007), Zaid *et al.* (2010), Kang (2010) and Feng *et al.* (2009) also used the properties of DWT coefficients in their image-adaptive watermarking schemes.

2.5.2.2 Use of the properties of DCT coefficients

When host image is subjected to DCT, the DC components of the transform have much larger perceptual capacity than any of the AC components. Huang *et al.* (2000) and Wang and Ji (2009), used this property of the DCT and embedded the watermark in the DC components of the

host image. Chen *et al.* (2000), proposed a method where 8×8 blocks of the image pixels are formed and for each block mean of the gradient magnitudes is taken which is a measure of the complexity of the block. Now the DCT is applied to the host image and blocks with sufficiently higher value of this parameter are chosen for embedding the watermark. Ejaz *et al.* (2014) proposed a method of adaptive blind digital image data hiding in DCT domain using minimum error least significant bit replacement method and genetic algorithm. Use of DCT compression in images may result in visible artifacts which can be removed by the signal adaptive approach (Singh *et al*., 2011).

2.5.2.3 Use of the properties of contourlet and curvelet transform coefficients

In their contourlet based image-adaptive watermarking scheme Song *et al.* (2008), embedded the watermark into the biggest subband (the high frequency subband) coefficients where it eventually spreads out in all subbands when the watermark image is reconstructed due to the special transform structure of Laplacian pyramid in contourlet transform. Bi *et al.* (2010), proposed a watermarking scheme where host image and low pass coefficients of contourlet transform are segmented into the blocks. These blocks are decomposed using SVD. As small changes in the singular values don't change the image greatly therefore watermark is embedded into the largest singular value. Zhang *et al.* (2008a) used the properties of curvelet transform coefficients in their watermarking method.

2.5.2.4 Use of the properties of other transforms' coefficients

Stankovic *et.al.* (2010) proposed a scheme which provided the estimation of local frequency content for each image pixel. The local frequency content is used to determine whether the image region is appropriate for watermarking or not. Kumsawat *et al.* (2005) have presented a watermarking technique which uses the Discrete Multiwavelet Transform (DMT). In this paper genetic algorithms have been used to improve robustness of the watermark and perceptual quality of the watermarked images. Distributed arithmetic has been used in Pal *et al.* (2012) and method of encryption for the security of the system is described in Milican *et al.* (2014). Bi *et al.* (2007) in their blind watermarking scheme used Multiband Wavelets Transformation (MWT). In this watermarking scheme the bits of watermark are inserted in the middle frequency subimages.

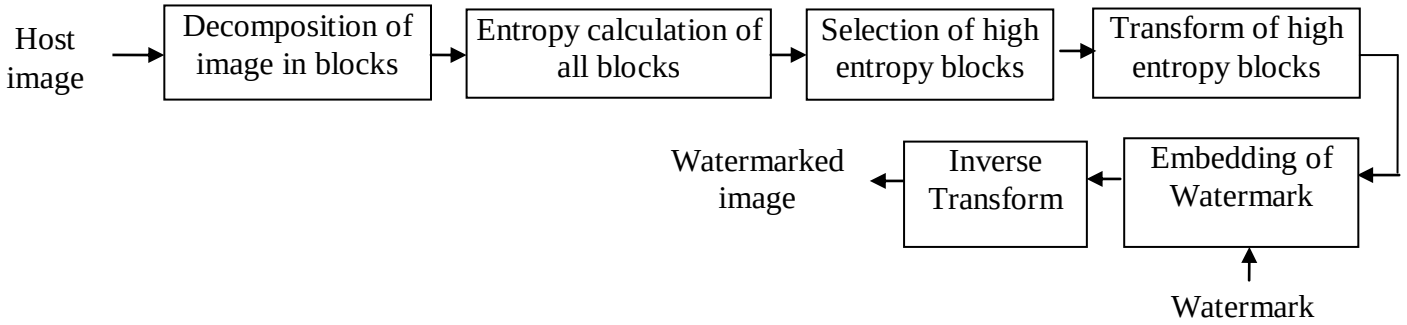


Figure 2.5 Using entropy distribution of image blocks in watermarking

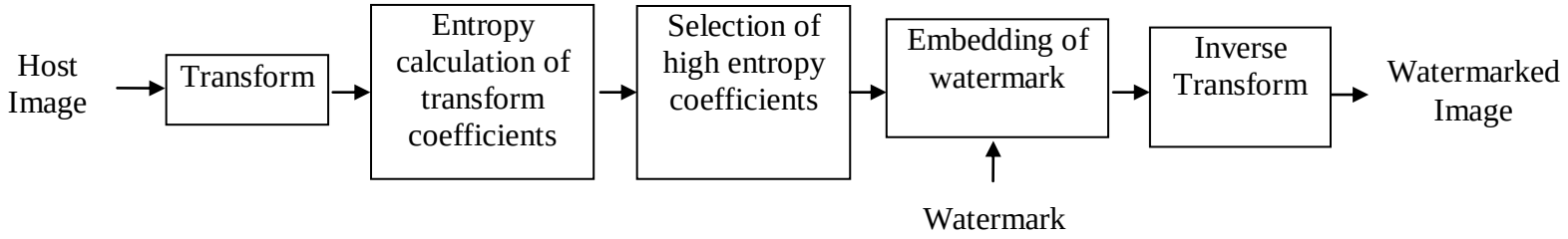


Figure 2.6 Using entropy distribution of transform coefficients in watermarking

Zhang *et al.* (2008b) used a statistical method based on Gaussian Mixture Model (GMM). Xiang *et al.* (2008) have used histogram and mean in their watermarking scheme. Fractional Fourier transform has been used by Kutay and Ozaktas (1998) for the optimal restoration of the image and Freitag method has been used by Jankowsky and Limiti (2010). A circular statistical method has been employed by Sarla and Jain (2000). Huang *et al.* (2008), Rashimi and Rabani (2010) and Han *et al.* (2009) also used the statistical properties of the image transforms for making the watermarking image dependent.

2.5.3 Entropy Distribution Based Watermarking Techniques

In this category of watermarking, image-adaptive character is given to the watermarking by using the entropies of the image pixel blocks or transform coefficients. The blocks with higher entropies can be modified by the higher values of watermark bits without being perceptible and hence resulting in more robustness for the watermark.

Akhaee *et al.* (2009) suggested a technique where high entropy blocks (16×16) of the host image are selected for watermark embedding and are subjected to 2D-DWT transform. For embedding the watermark, in each block low frequency coefficients are scaled upward or downward depending upon the value of watermark bit (1- up, 0- down) by a constant factor called strength factor. Sheng and Hui (2009), proposed a scheme where cover color image is segmented into several subbands after application of DWT and the subband having highest energy value is used to embed the composite watermark. Akhaee *et al.* (2010), applied the contourlet transform to the highest entropy blocks of the image. They chose the directional subbands with the highest energy for embedding purpose. Double Random Phase Encoding (DRPE) has been used by Liu *et al.* (2013). This watermarking scheme uses DRPE to scatter the energy of input information reversibly in the space as well as spatial frequency domains. Kalantri *et al.* (2010) have used the Finite Ridgelet Transform (FRIT) which has the least number of coefficients than any other transform. In this scheme blocks of the host image with most energetic direction are used for watermark embedding. Jadhav and Bhalchandra (2010) and Akhbari and Ghaemmaghami (2005) also used the entropy distribution properties of the image for making their watermarking algorithms image-adaptive.

2.5.4 Feature Points Extraction Based Watermarking Techniques

In this approach of image-adaptive watermarking techniques, perceptually most significant subimage or feature points of the covering image are extracted and are used for embedding the watermark, making the watermarking technique substantially robust.

Mohanty *et al.* (2006) proposed a method where perceptually most important subimage of the host image is segmented from the host image using Osberger and Maeder (1998) and its DCT is taken. Now the image statistics generator module calculates the required statistics from the segmented subimage and generates a synthetic image identical to the host subimage. DCT of the watermark is also taken and coefficients of the watermark are fused into a lesser sensitive area of the synthetic image to form an effective or compound watermark. This watermark is embedded in the host image coefficients.

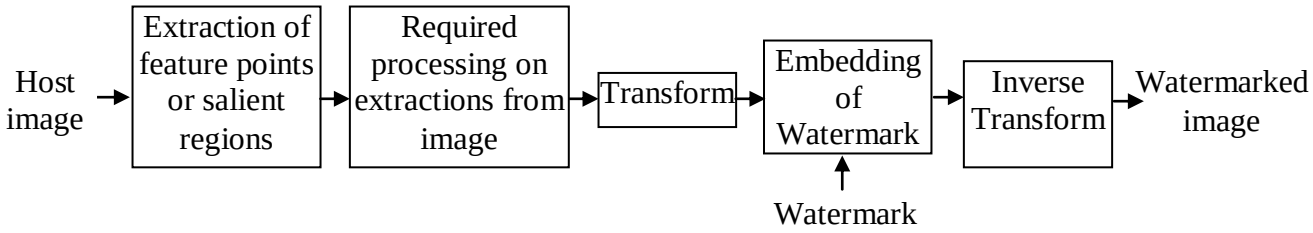


Figure 2.7 Use of the extractions from host image in watermarking

Niu *et al.* (2011) presented a watermarking technique where stable feature points are extracted from the host image by using Scale Invariant Feature Transform (SIFT). Local Feature Regions (LFRs) are constructed by taking some strong feature points at the center. Bandelet transform is applied on LFRs. Watermark is added in the LFR by making changes into the major Bandelet coefficients.

Qi and Qi (2007), proposed a scheme where feature points of image are extracted using Harris corner detector. Extracted feature points are used in the embedding of the watermark by employing DFT. Minghui and Jingbo (2009), Tian *et al.* (2011), Lu and Hsu (2007) and Zheng *et al.* (2009) have also used the extractions from host image for image-adaptive watermarking.

2.6 ROBUST HYBRID WATERMARKING TECHNIQUES

Watermarking techniques which use more than one transform in their watermarking operation are called hybrid watermarking techniques. In a hybrid watermarking method proposed by

Agarwal *et al.* (2013), HVS characteristics of the image in DCT domain are used to obtain a sequence of weighing factor from Genetic Algorithm-Back Paradigm Network (GA-BPN). This weighing factor is used to embed and extract the watermark from the image in DWT domain. Liu and She (2012) proposed a quantization based hybrid watermarking technique in DWT and DCT domains. In their scheme watermark is embedded in the high entropy area of the low frequency subband image. The quantization step size is controlled in an adaptive manner using Rational Dither Modulation (RDM). Relationship of fractional Fourier transform with chirp and wavelet transform is probed by Ozaktas *et al.* (1994) and reduced order model for multivariable system is described by Prasad *et al.* (2000). Lai and Tsai (2010) suggested a watermarking technique based on DWT and SVD. In their technique, the image is decomposed into four sub-bands by applying one level DWT transformation. Then SVD is applied on the intermediate frequency bands and watermark is embedded into the obtained singular values.

Falkowski (2008) proposed a phase watermarking algorithm which uses a modified, multi-resolution, multi polarity WHT and multi polarity Complex Hadamard transform (CHT). Watermark is embedded in the coefficients of forward CHT. Ganic and Eskicioglu, (2005) applied SVD on the DWT transformed host image as well on the watermark. The singular values of the watermark were embedded into the singular values of first level DWT subbands of the host image. Makbol and Khoo (2013) presented a watermarking scheme which used Redundant Discrete Wavelet Transform (RDWT) and SVD. Here, gray scale watermark is embedded directly into the singular values of the RDWT subbands of the host image. Pujara *et al.* (2007), proposed a hybrid scheme where DWT and Fractional Wavelet Transform (FWT) are used together in watermarking. Rastegar *et al.* (2011) presented a hybrid watermarking scheme in which radon transform is applied on the host image, followed by 2D-DWT and SVD. Singular values obtained from host image are used to embed the binary watermark's singular values. Ali and Ahn (2014) presented a DWT and SVD based hybrid image watermarking scheme using Self-adaptive Differential Evolution (SDE) algorithm. The scaling factors used in watermarking are optimized using SDE to gain the maximum achievable robustness and imperceptibility. Tsai *et al.* (2012) presented a blind watermarking scheme which used DWT, SVD and Support Vector Regression (SVR). In this scheme, one level DWT is applied on the host image's non-overlapping blocks. On the LL subband, SVD is applied and watermark is embedded by modifying the obtained U component of SVD decomposition. Blind watermark detection is

designed using trained SVR to estimate original coefficients. Also, the Particle Swarm Optimization (PSO) has been used to optimize the proposed scheme.

Run *et al.* (2012) proposed two watermarking schemes. In the first scheme, SVD was used with DCT and in the second scheme, SVD was used with DWT. They used a scaling factor which is not a scalar value but is in the matrix form. PSO is used to choose the correct value of the scaling factor. Santhi and Arulmozhivarman (2013), proposed a scheme in which color image in RGB domain is changed into YUV color space. Hadamard transform is applied on the luminance channel Y as well as on the watermark. In this method scaling factor is computed adaptively using sigmoid function in Hadamard transform domain. Rawat and Raman (2012a) presented a blind watermarking scheme which uses fractional Fourier transform, visual cryptography and SVD.

2.7 ATTACKS ON WATERMARKING SYSTEM

A watermarked image may be altered either intentionally or unintentionally. In both the cases the water-marking system should be able to extract the watermark. An intentional attack is also called malicious attack, while an unintentional attack is called non-malicious attack. Histogram equalization for image enhancement and compression of the images are some of the non-malicious attacks. Malicious attackers willfully want to destroy the watermark without causing excessive degradation of the watermarked image so that it remains commercially usable. Petitcolas *et al.* (1998) have mentioned various popular attacks; some of them may be malicious or non-malicious, depending on the application:

Filtering: Low-pass filtering is a non-malicious attack. It does not cause significant degradation in watermarked images. If the watermark has been added in the form of linear noise, then Wiener filtering is used as a malicious attack to remove the watermark. If the power spectrum of the embedded watermark is independent of the host image power spectrum then Gaussian filtering works as malicious attack.

Additive Noise: This may originate from the D/A and A/D conversions or from transmission errors in the form of non-malicious attack. However, an attacker can also introduce additive noise (AWGN etc.) of limited power which remains invisible. This will cause to increase the threshold of the correlation detector for extracting the watermark.

Compression: This is generally a non-malicious attack which mostly seen in multimedia applications. To lessen the effect of this attack, the watermark should be embedded in the same domain where the compression takes place.

Cropping: This is a very common malicious attack. Many times the attacker is interested in small portion of a particular image or frames of a video. To avoid the destruction of watermark after this attack, the watermark should be spread over the dimensions where this attack could possibly happen.

Statistical Averaging: This is also a malicious attack. By using this attack, an attacker first tries to estimate the watermark and then tries to remove it by doing subtraction from the watermarked image. Median attack is an example of it.

Rotation and Scaling: Both of these are malicious attacks. Correlation-based extraction fails after these attacks. This is because the inserted watermark and the locally generated version now have different spatial patterns and synchronization is lost. So, in case of scaling attack, to regain the synchronization, the scaled image can be converted back into its initial size

Multiple Watermarking: This too is a malicious attack. An attacker may watermark an already watermarked image and later make claims of ownership. The easiest solution to avoid the effect of this attack is to timestamp the embedded watermark.

Attacks at Other Levels: There are some other attacks which try to manipulate the embedded watermark. For example, data can be scrambled to avoid copy control mechanisms and the watermark gets lost.

2.8 QUALITY METRICS

Quality metrics are the parameters that are used for assessing the performance of the watermarking scheme by measuring the amount of error in the watermarked image and in the watermark extracted from it. PSNR and BER (%) are used in this thesis as quality metrics.

PSNR has been used to measure the quality of the watermarked image as compared to the original host image. More is the PSNR value (in dB), better is the watermarked image quality. Higher value of PSNR means that embedded watermark in the watermarked image remains imperceptible and the watermarked image looks similar to the host image. PSNR can be easily

defined via the Mean Square Error (MSE). Assuming a noise free host image $f(i, j)$ of size $m \times n$ and the watermarked image $g(i, j)$ of same size, MSE is defined as (Guo *et al.*, 2011):

$$MSE = \frac{1}{m.n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [f(i, j) - g(i, j)]^2 \quad (2.24)$$

The PSNR is defined as (Guo *et al.*, 2011; Nafornita, 2005; Wen *et al.*, 2009):

$$PSNR = 20.\log_{10}(\frac{Max_f}{\sqrt{MSE}}) \quad (2.25)$$

where, Max_f - Maximum pixel value in the host image

$f(i, j)$ - Noise free host image

$g(i, j)$ - Watermarked image

m - Number of rows

n - Number of columns

BER (%) is used to measure the percentage of error in the extracted watermark from the watermarked image. More the BER (%), lesser is the quality of the extracted watermark. BER (%) of the extracted watermark is given as (Dixit *et al.*, 2009):

$$BER(\%) = \frac{Number\ of\ errored\ bits}{Total\ number\ of\ bits\ in\ the\ watermark} \times 100 \quad (2.26)$$

A good watermarking scheme should have a high value of the watermarked image PSNR and low value of the BER (%) of the detected watermark. Error flow analysis can be done as shown by Dey and Badkoobehi (2011).

2.9 RESEARCH GAPS

Based on the literature review following gaps are identified:

Various transforms are being used in watermarking techniques. Most of these techniques use optimized strength factor having one value of strength factor for all the pixel blocks of the image. So, there is a scope to improve the robustness against common watermarking attacks if a more efficient strength factor could be used.

In the available literature no linkage has been reported between robustness of the watermarking scheme and block segmentation size. There is a scope to investigate whether any such relation exists between these two.

Almost all the watermarking techniques have used binary watermarks. Being able to embed a gray scale or color watermark in the image is still a big challenge to the researchers.

In the available literature there is no quantitative comparison among robustness results of strength factors derived from different local properties of the image for the same watermarking algorithm. The research needs to be done to find out a local property of the image best suited to design a strength factor.

In robust image-adaptive data hiding method using erasure and error correction, the detection of watermark is prune to errors, as there is no side information available about the locations where data is hidden.

2.10 RESEARCH OBJECTIVES

The following research objectives are formulated based on the literature review and research gaps:

1. To study the existing transform domain based image-adaptive techniques of robust watermarking for Human Visual System (HVS).

2. To propose a transform domain based new image-adaptive robust watermarking scheme using spread spectrum method for watermark embedding.

3. To analyze the watermark strength factor according to the local properties of the image.

4. To evaluate the robustness of the proposed technique against different types of malicious and non-malicious attacks.

2.11 RESEARCH METHODOLOGY

Main focus of the present research work is on the development of robust image-adaptive watermarking techniques using one or more transforms for protecting the ownership/intellectual property rights of the genuine owners. Sixteen host images and three sized watermarks (small, medium and large) have been used as shown in Appendix-I and Appendix-II respectively. Host

images are segmented into small sized image pixel blocks. Entropy values of all the blocks are calculated and blocks having high entropy values are selected for watermark embedding. Transform is applied on the selected high entropy blocks (In the hybrid watermarking three transforms have been applied one after another). Transform coefficients belonging to the selected blocks are used to embed the watermark bits. One block is used for embedding one watermark bit only. Watermarked images are subjected to a number of common watermarking attacks for the performance evaluation of the watermarking technique. Watermark is detected by comparing the pre-embedding statistical data related to the image blocks (contained in the side information) with the post embedding statistical data obtained from the watermarked image.

For the simulation of proposed techniques, MATLAB [version 7.10.0.499 (R2010a)] software is used on a system configuration Pentium 4, with an Intel® Core 2 Duo CPU T6400@2.00GHz, 800 MHz FSB, 2MB L2 cache processor along with 3 GB DDR3 RAM and Windows XP Professional (version 2002 service pack 3).

CHAPTER 3

DIFFERENT SIZED BLOCK SEGMENTATIONS IN WATERMARKING

IN this chapter the watermarking using three block segmentation sizes has been done and the concept of dynamic strength factor has been introduced. Robustness of the watermarking with these block segmentation sizes has been tested by subjecting the watermarked images to the many common watermarking attacks. Comparisons with other watermarking schemes have also been made. Block segmentation size which provides the best robustness results with and without applying the attacks on a number of host images has been determined.

3.1 INTRODUCTION

The practice of segmenting the image in smaller non-overlapping image pixel blocks prior to watermark embedding has been in existence for many years. Discussion on block segmentations in watermarking has been done in Section 2.4. From this discussion it can be stated that segmentation of image in the small squared groups of image pixels i.e. pixel blocks is a precursor to a large number of image-adaptive techniques in robust watermarking (Swanson *et al.*, 1996; Huang and Shi, 1998; Yan *et al.*, 2009; Kalantari *et al.*,2010; Fami *et al.*, 2012). But almost all the watermarking techniques in the available literature have used only one block segmentation size for the watermark embedding and detection. The effects of using multiple sized block segmentations on the extracted watermark's robustness are still needed to be evaluated. In this chapter a DWT based watermarking technique has been used with three block segmentation sizes (8×8, 16×16 and 32×32).

3.2 WATERMARKING SCHEME

In this section watermarking scheme is introduced. Watermark embedding and detection process has been described by using three sized block segmentations.

3.2.1 Watermark Embedding

Block diagram of watermark embedding in the presented scheme is shown in Figure 3.1. In the presented robust watermarking technique, the host image is segmented into N×N non-overlapping blocks (value of N could be 8, 16 or 32). Entropy values of all the blocks are calculated (Gonzalez et *al.*, 2009), and the mean entropy value of a block is obtained which is taken as a reference value. In the presented work, the blocks having their entropy values equal to or more than the reference value have been addressed as high entropy blocks and watermark is embedded in them. Binary watermarks with only '0' or '1' in their array or matrix are used. One bit of binary watermark is embedded in every selected high entropy block. So, the number of chosen high entropy blocks should be equal to or more than the watermark bits. If the number of high entropy blocks for an image is lesser than the number of bits in the watermark then the reference or benchmark value is minutely decreased to make the count of high entropy blocks same as that of the watermark bits.

The selected high entropy blocks are subjected to DWT. Daubechies wavelet with single level of decomposition has been used (Daubechies, 1988). As a result vertical, horizontal, diagonal and approximation DWT coefficient matrices, consisting of every high entropy block are attained. Approximation matrix having low frequency coefficients is chosen for watermark embedding, as low frequency coefficients carry the most vital information of an image. Approximation matrices consisting of all the high entropy blocks are slightly changed to embed a single '1' or '0' into them. If original and modified approximation coefficient matrices are represented by X and X' respectively, then any binary watermark can be embedded using spread spectrum method of watermarking (Cox *et al.*, 1997) as shown below:

$$X' = X.(1+DSF) \quad \text{For embedding element '1' of watermark} \tag{3.1}$$

$$X' = X.(1-DSF) \quad \text{For embedding element '0' of watermark} \tag{3.2}$$

where, *DSF* – Dynamic or Flexible Strength Factor derived from the standard deviations of the approximation coefficients belonging to the high entropy blocks.

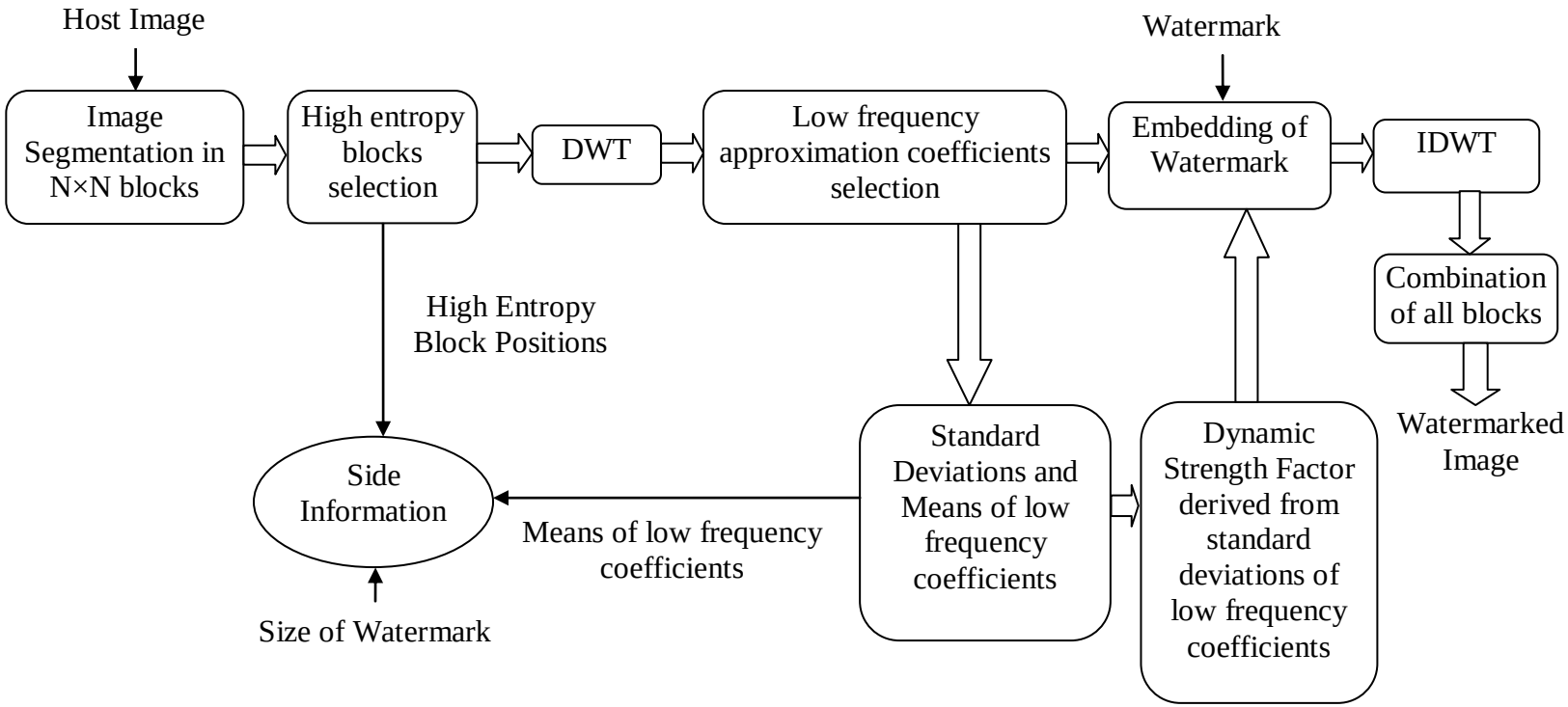


Figure 3.1 Embedding of watermark in the proposed watermarking scheme

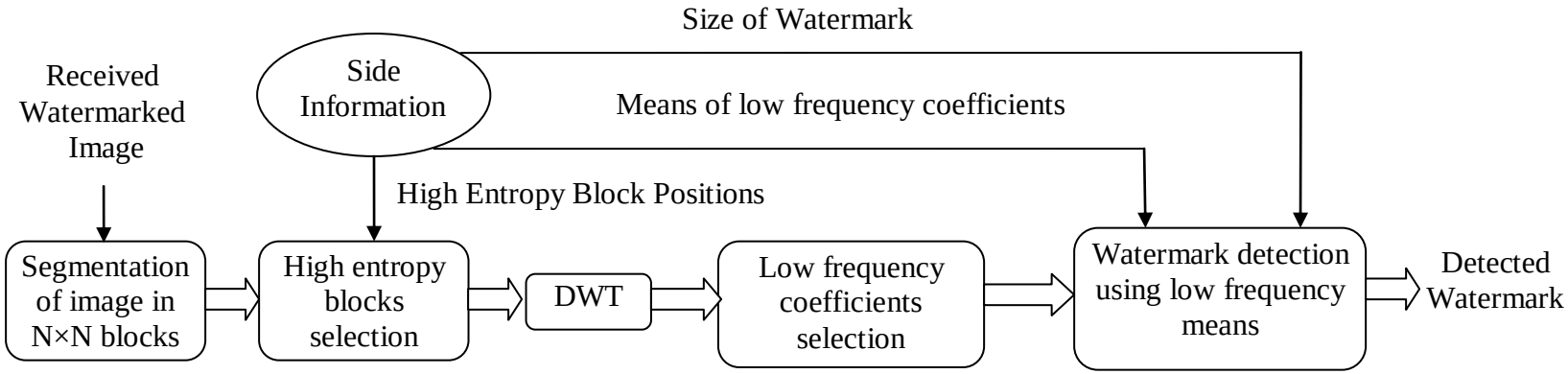


Figure 3.2 Detection of watermark in the proposed watermarking scheme

More discussion about *DSF* has been presented in the next subsection. Inverse discrete wavelet transform (IDWT) is applied to the high entropy blocks after embedding of the watermark in them. Then they are combined with other blocks to form a watermarked image. Side information required for the watermark detection is also generated during watermark embedding, which consists of high entropy block positions, means of the frequency coefficients and size of the watermark.

3.2.1.1 Concept of Dynamic Strength Factor

Most of the robust watermarking techniques use optimization techniques to achieve a strength factor for every host image. But in the proposed scheme an image block is considered as a complete entity by itself and a separate strength factor is found for every block. In the quest to find a dynamic or flexible strength factor having different values for every image block, standard deviation is considered an appropriate parameter. Standard deviation (σ) signifies the amount of deviation or diffusion from the expected or mean value in statistics and probability theory. High value of standard deviation denotes that data contains a large array of values while a low value of standard deviation points towards a small range of data clustered in the vicinity of mean. Standard deviation is defined as the square root of variance which for a specific set of values can be shown as:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2} \tag{3.3}$$

where, x_i is any value from the given set of data $\{x_1, x_2, x_3 \ldots\ldots\ldots\ldots x_N\}$

$\bar{x}$ is the mean value of these observations

N is the number of values in sample

In the proposed scheme of watermarking, DWT is applied on N×N high entropy blocks of image. Standard deviation of the approximation matrix (containing low frequency coefficients) belonging to every high entropy block is taken. Maximum value of standard deviation from approximation matrices is also noted. This maximum value is used for finding the individual strength factor for each block. Dynamic strength factor or *DSF* which has different values for all the blocks can be shown as:

$$DSF = \frac{\sigma_i}{(\sigma_{\max})^{\rho}} \tag{3.4}$$

where, σ_i - Standard deviation of DWT approximation coefficient matrix of a selected block.

$\sigma_{\max}$ - Maximum standard deviation among all the selected blocks.

ρ - Adjusting parameter of denominator.

By varying the value of adjusting parameter ρ the value of strength factor also varies. As adjusting parameter is the power of denominator, so when the value of adjusting parameter is increased, the value of strength factor decreases and vice-versa. The strength factor is used in the embedding of watermark. All the watermarked images used in the chapter are of PSNR value 45 dB because those values of ρ have been used for them which make the corresponding watermarked image PSNR as 45 dB. (An image with PSNR value of 45 dB is generally considered having very good visual quality.) Table 3.1 shows the values of adjusting parameter for some images for embedding two different sized watermarks using block sizes 8, 16 and 32.

Table 3.1 Variation of adjusting parameter ρ for watermarked image PSNR 45 dB with block size 8, 16 and 32.

Host Image	Value of adjusting Parameter (ρ) with watermark *TU* (12×9)			Value of adjusting Parameter (ρ) with watermark *T UNIV* (27×8)		
	Block Size 8	Block Size 16	Block Size 32	Block Size 8	Block Size 16	Block Size 32
Barbara	1.324	1.562	1.768	1.387	1.636	1.826
Boat	1.389	1.638	1.731	1.476	1.695	1.752
Peppers	1.426	1.526	1.716	1.475	1.589	1.727
Couple	1.472	1.604	1.800	1.530	1.650	1.756
Goldhill	1.610	1.667	1.735	1.646	1.710	1.765
Lake	1.406	1.536	1.663	1.460	1.598	1.724

3.2.2 Watermark Detection

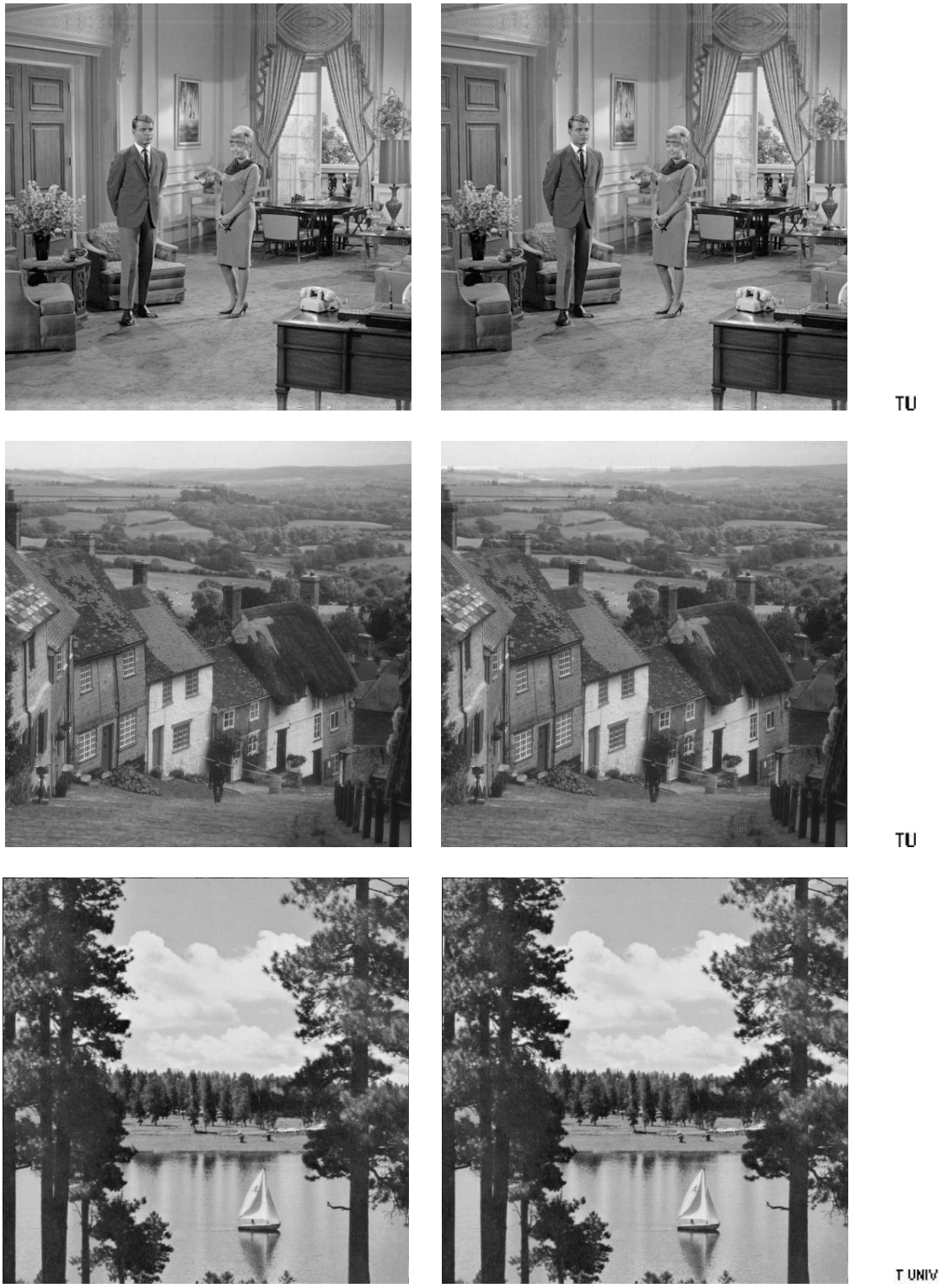
Block diagram of watermark detection is shown in Figure 3.2. In the detection of watermark, received watermarked image is segmented into respective N×N blocks. By using the side information sent along with the watermarked image, locations of watermark embedding high entropy blocks are known at the detection end and DWT is applied on them. As a result approximation coefficient matrices of all the high entropy blocks are achieved. Side information contains the means of low frequency approximation coefficient matrices before embedding of the

watermark in the host image. All the embedded bits of watermark are determined by comparing the means of approximation matrices of watermarked image with the means of corresponding approximation matrices of the unwatermarked host image. That is, if mean belonging to the watermarked image block is higher than the respective mean of the un-watermarked image block, existence of '1' is detected. Similarly for the opposite condition being true, existence of '0' is detected. In this way, the complete binary watermark gets extracted from the watermarked image. A very significant advantage of the proposed technique is that watermarked image is not harmed in any manner during the process of watermark extraction.

3.2.3 Use of Three Block Sizes

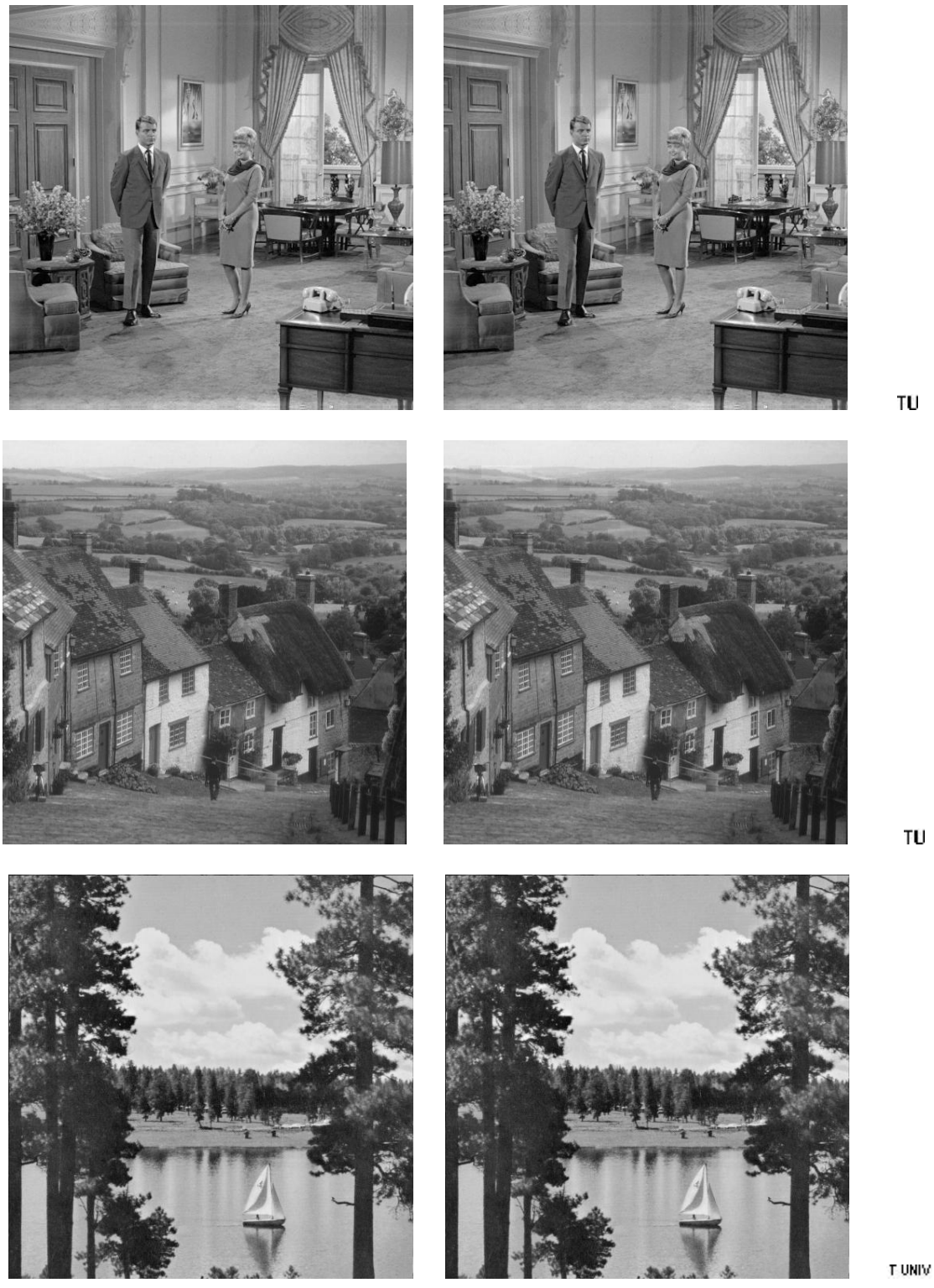
The proposed watermarking technique has three variants which make use of 8×8, 16×16 and 32×32 pixel block segmentations. All the sixteen host images which have been used in this work are of size 512×512, as shown in Appendix-I. As explained earlier in subsection 3.2.1, in every segmented block of the host image, only one watermark bit can be embedded. So, maximum number of watermark bits which can be embedded in a host image using block size 8 is 4096. Similarly maximum number of watermark bits which can be embedded in the host image using block size 16 is 1024 and using block size 32 is 256. Performance comparison of three block sizes in the proposed technique can only be done if a watermark of such a length is used which is suitable to all three block sizes. In other words the watermark to be used in this watermarking scheme should be of length 256 or less. Two small sized binary watermarks as shown in Appendix-II have been used to fulfil this requirement: *TU* (12×9) and *T UNIV* (27×8). As both of these watermarks have their lengths less than 256, they can be easily embedded in any host image by using block sizes 8, 16 and 32.

Figures 3.3 to 3.5 show the original host images *Couple*, *Goldhill* and *Lake*, their watermarked images of PSNR 45 dB and recovered watermarks for image segmentation block sizes 8, 16 and 32 respectively. All the host images and watermarked images have been shown at nearly half of their actual sizes while all the recovered watermarks have been shown without any reduction to their actual sizes. From these figures it is observed that all the watermarked images do not have any perceptible difference from their original images. All the recovered watermarks also look similar to the original watermarks



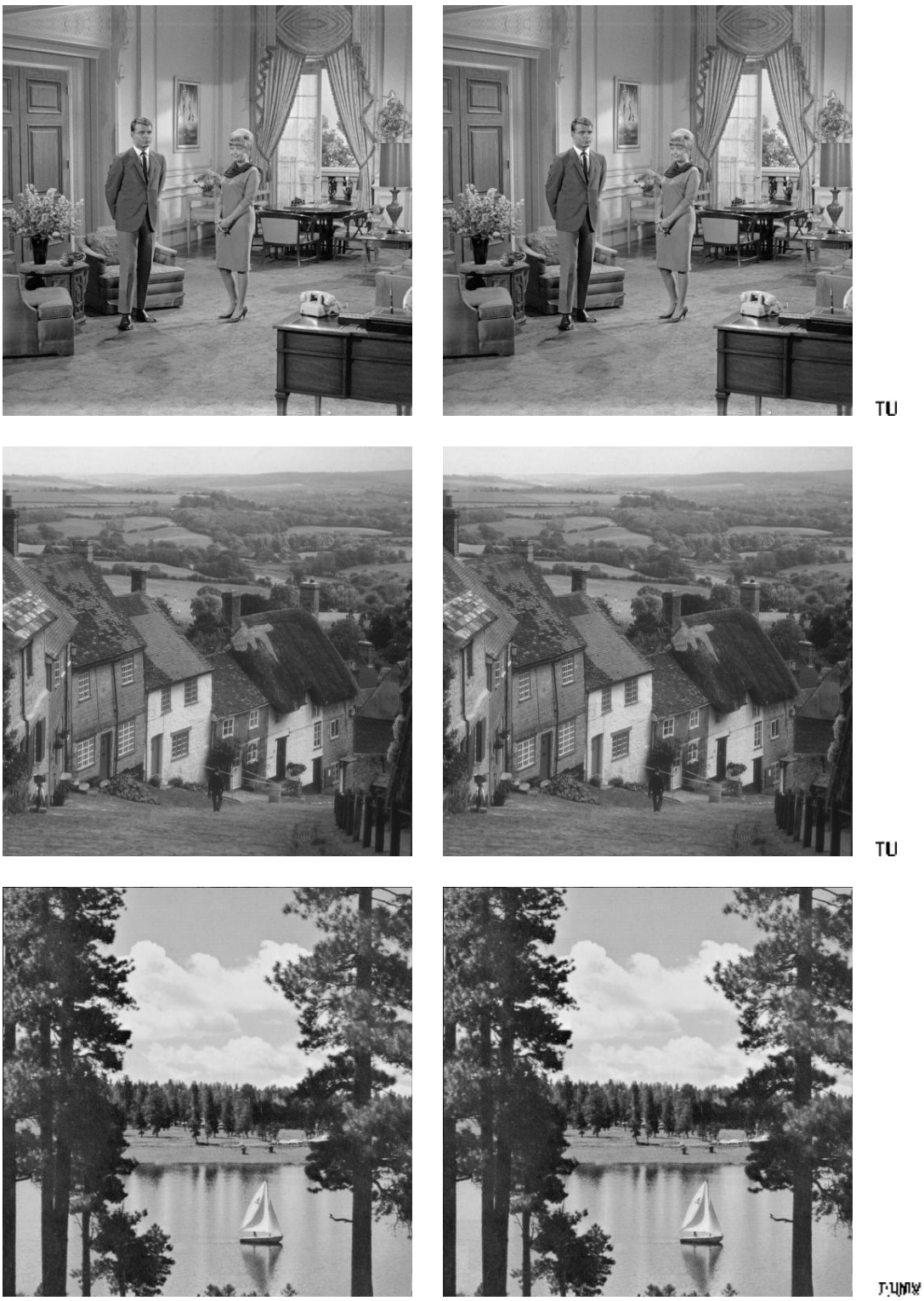
Column 1 Column 2 Column 3

Figure 3.3 Original host image (column 1), watermarked image with PSNR as 45 dB (column 2) and recovered watermark (column 3) using block size 8



Column 1 Column 2 Column 3

Figure 3.4 Original host image (column 1), watermarked image with PSNR as 45 dB (column 2) and recovered watermark using (column 3) block size 16



Column 1 Column 2 Column 3

Figure 3.5 Original host image (column 1), watermarked image with PSNR as 45 dB (column 2) and recovered watermark (column 3) using block size 32

3.3 EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section performance comparison of three block sizes in the presented watermarking technique has been done without applying attacks as well as under the application of attacks. Comparison with well known techniques of literature has been done next.

3.3.1 Performance analysis without applying attacks

Figure 3.6 shows the BER (%) plots of recovered watermark *T UNIV* from sixteen unattacked watermarked images (having PSNR as 45 dB) for three block sizes 8, 16 and 32 in the presented watermarking scheme.BER (%) has been used as a robustness parameter. High BER (%) of the recovered watermark indicates the low robustness and low BER (%) of the recovered watermark indicates the high robustness. More error is observed in the high intensity images for bigger block sizes 16 and 32. In this plot the BER (%) value for watermarked images using block segmentation size 8 is least. Therefore it can be said that the robustness of the proposed watermarking scheme using block size 8 is best when no watermarking attacks are applied.

3.3.2 Performance analysis under common attacks

Results of common attacks have been shown using three host images *Couple*, *Goldhill* and *Lake* and watermarks *TU* and *T UNIV* for block segmentation sizes 8, 16 and 32. Tables 3.2 and 3.3 show BER (%) of recovered watermark for a limited set of attacks. All three variants of the presented watermarking scheme using block segmentation sizes 8, 16 and 32, show excellent performance against Gaussian filter, Wiener filter and scaling attacks, producing zero or very negligible BER (%) for them. For the AWGN noise attack of variance 20, BER (%) of the recovered watermark is zero or slightly more for block size 8 with all three images. For the same attack BER (%) of recovered watermark is marginally higher for block size 16. For the JPEG compression attack of very low quality factor 10%, the proposed scheme shows very strong resistance for block sizes 8 and 16. Similarly for the median filter (3×3) and sharpening attacks, block size 8 and 16 show reasonably good performance.

Tables 3.4 - 3.6 and Figures 3.7 - 3.8 show performance of the proposed scheme more descriptively against the attacks. Table 3.4 shows the performance of three block sizes in the proposed scheme against scaling attacks of various levels. BER (%) of recovered watermark for

all block sizes is zero against almost all scaling attacks with watermark *TU*. Performance of the block sizes 8 and 16 with watermark *T UNIV* is also extremely good against all scaling attacks.

Figure 3.7 shows the plots of JPEG compression attacks for various quality factors and Figure 3.8 shows the plots of AWGN attacks for different variances with watermark *TU*. In Tables 3.5 and 3.6, performance of the three block sizes in the proposed scheme has been shown against some other attacks. From these plots and tables it is observed that proposed watermarking scheme with block size 8 gives lesser BER (%) for a larger number of attacks in comparison to the block sizes 16 and 32. The superiority of the block size 8 over block sizes 16 and 32 can be more clearly observed in the plots of Figures 3.9 to 3.12.

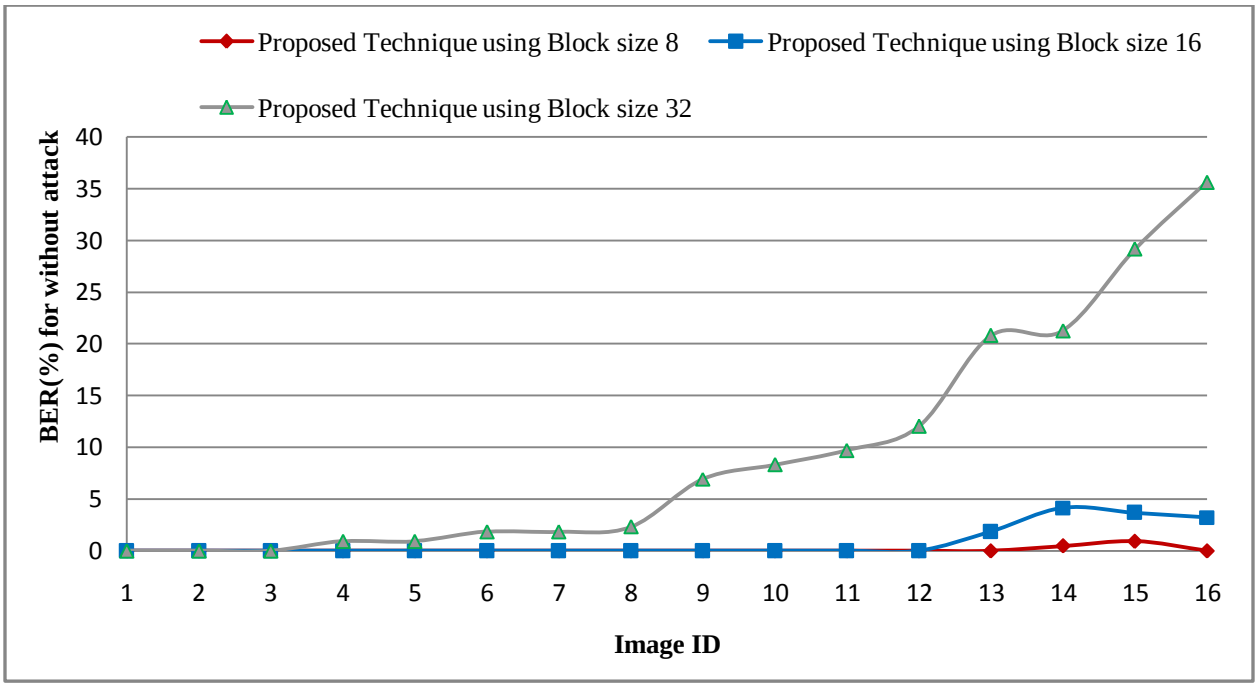
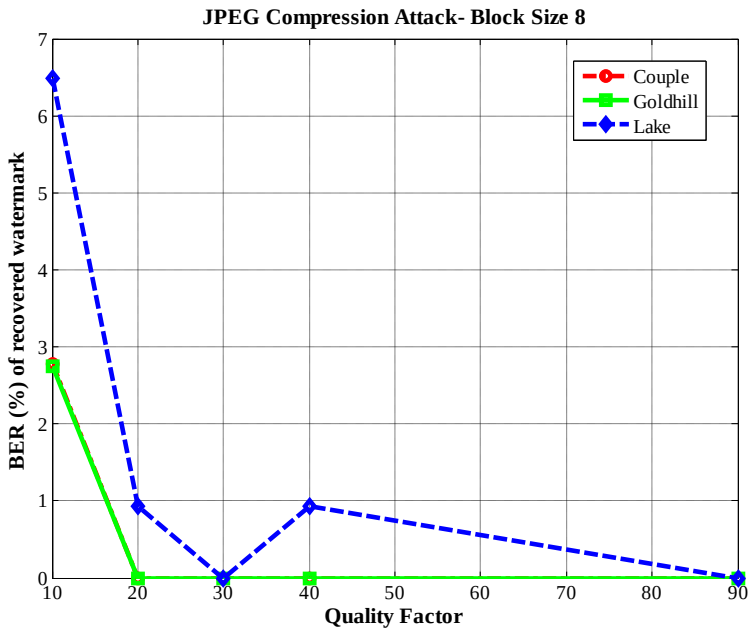
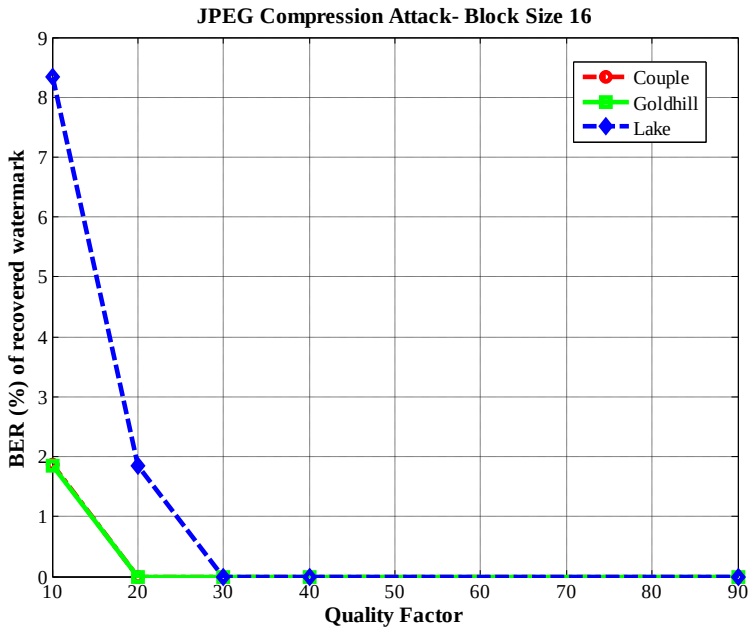


Figure 3.6 BER (%) plot of recovered watermark *T UNIV* without applying any attack using block sizes 8, 16 and 32 with sixteen watermarked images having PSNR as 45 dB

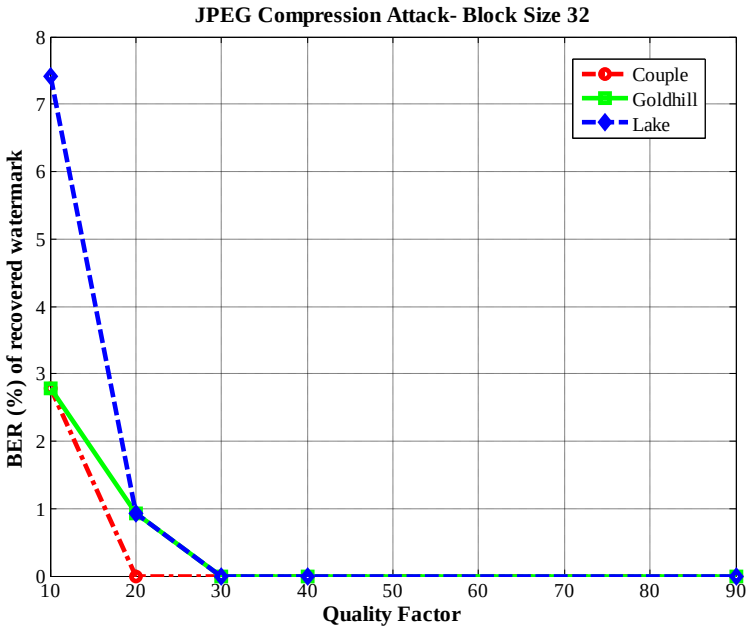


(a)



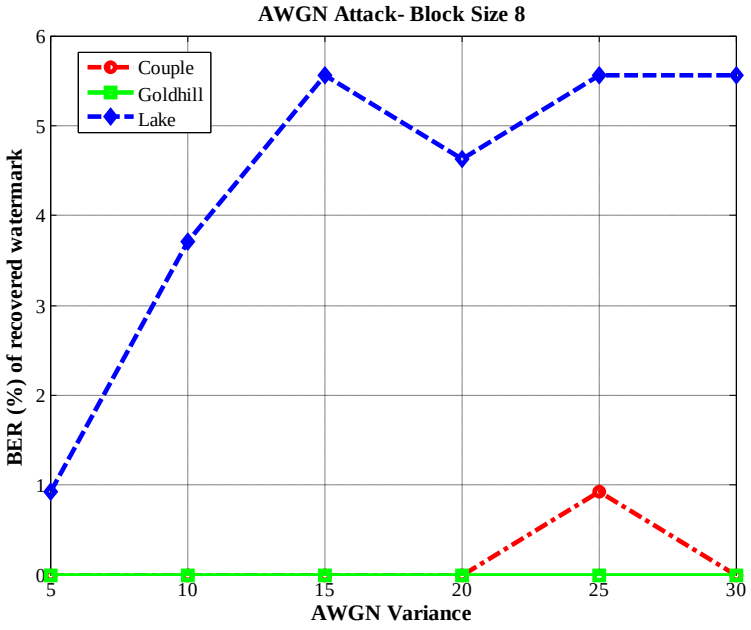
(b)

Figure 3.7 JPEG compression attack with watermark *TU* using (a) Block size 8 (b) Block size 16 and (c) Block size 32 by keeping watermarked image PSNR as 45 dB



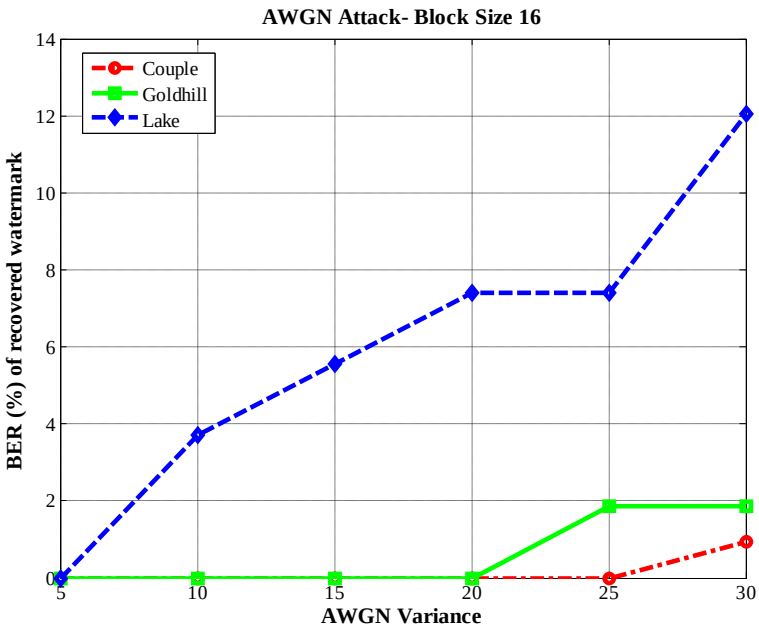
(c)

Figure 3.7 JPEG compression attack with watermark *TU* using (a) Block size 8 (b) Block size 16 and (c) Block size 32 by keeping watermarked image PSNR as 45 dB

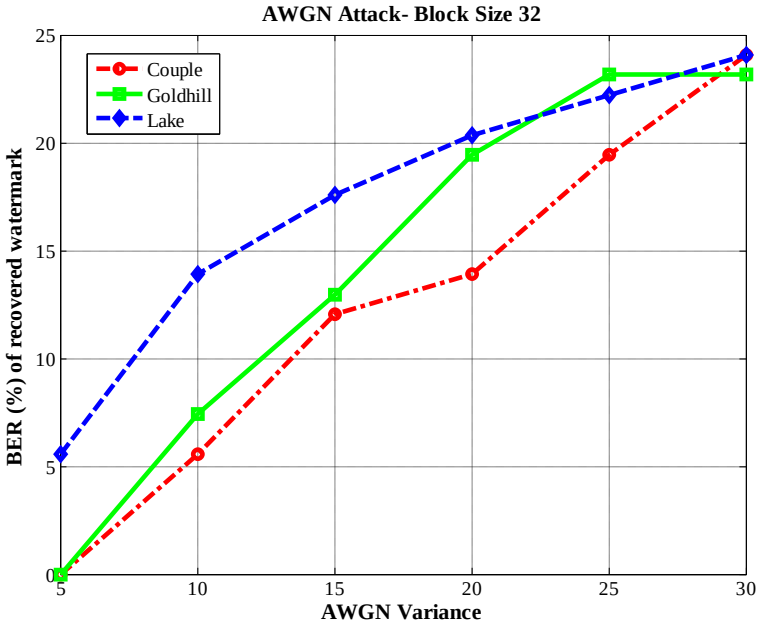


(a)

Figure 3.8 AWGN noise attack with watermark *TU* using (a) Block size 8 (b) Block size 16 and (c) Block size 32 by keeping watermarked image PSNR as 45 dB



(b)



(c)

Figure 3.8 AWGN noise attack with watermark *TU* using (a) Block size 8 (b) Block size 16 and (c) Block size 32 by keeping watermarked image PSNR as 45 dB

Table 3.2 BER (%) of recovered watermark under JPEG, AWGN and Median filter attacks for three block sizes

Watermark	Couple			Goldhill			Lake		
	JPEG Q=10%	AWGN σ^2=20	Median 3×3	JPEG Q=10%	AWGN σ^2=20	Median 3×3	JPEG Q=10%	AWGN σ^2=20	Median 3×3
Block Size 8									
TU (12 × 9)	2.78	0.00	0.00	2.78	0.00	0.00	6.48	4.63	8.33
T UNIV(27 × 8)	8.80	0.92	0.92	9.26	0.00	0.00	13.42	2.31	9.26
Block Size 16									
TU (12 × 9)	1.85	0.00	0.00	1.85	0.00	0.00	8.33	7.41	6.48
T UNIV(27 × 8)	7.41	4.63	2.31	6.02	6.02	0.00	7.87	8.33	19.91
Block Size 32									
TU (12 × 9)	2.78	13.89	3.70	2.78	19.44	0.00	7.41	20.37	14.81
T UNIV(27 × 8)	4.63	18.98	4.63	11.57	19.91	6.02	14.35	19.44	30.09

Table 3.3 BER (%) of recovered watermark under scaling, sharpening, Wiener and Gaussian filter attacks for three block sizes

Watermark	Couple				Goldhill				Lake			
	Scaling 1.5	Sharpening	Wiener 3×3	Gaussian 3×3	Scaling 1.5	Sharpening	Wiener 3×3	Gaussian 3×3	Scaling 1.5	Sharpening	Wiener 3×3	Gaussian 3×3
Block Size 8												
TU (12 × 9)	0.00	2.78	0.00	0.00	0.00	2.78	0.00	0.00	0.00	13.89	0.00	0.00
T UNIV(27 × 8)	0.00	3.24	0.00	0.00	0.00	0.92	0.00	0.00	0.46	11.57	0.00	0.92
Block Size 16												
TU (12 × 9)	0.00	1.85	0.00	0.00	0.00	0.93	0.00	0.00	0.00	2.78	0.00	0.00
T UNIV(27 × 8)	0.00	4.63	0.00	0.46	0.00	2.31	0.00	0.00	0.00	6.94	0.00	0.00
Block Size 32												
TU (12 × 9)	0.00	10.19	0.00	0.00	0.00	2.78	0.00	0.00	0.00	4.63	0.00	0.00
T UNIV(27 × 8)	1.39	12.04	3.70	2.31	0.46	3.24	2.31	2.78	5.56	11.57	6.02	5.09

Table 3.4 Comparison of BER (%) of recovered watermark under scaling attacks of different levels for watermarks *TU* and *T UNIV*

	Block Size 8					**Block Size 16**					**Block Size 32**				
	Scaling Level					Scaling Level					Scaling Level				
	0.75	*0.9*	*1.1*	*1.5*	*2*	*0.75*	*0.9*	*1.1*	*1.5*	*2*	*0.75*	*0.9*	*1.1*	*1.5*	*2*
***TU* (12 × 9)**															
Couple	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Goldhill	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Lake	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.93	3.70	0.00	0.00
***T UNIV* (27 × 8)**															
Couple	0.00	0.00	0.46	0.00	0.00	0.00	0.00	0.93	0.00	0.00	1.39	1.85	5.56	1.39	2.31
Goldhill	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.46	2.31	6.02	0.46	0.93
Lake	0.00	0.00	0.46	0.46	0.00	0.00	0.00	3.70	0.00	0.00	4.63	9.26	17.59	5.56	5.56

Table 3.5 Comparison of BER (%) of recovered watermark under median filter and Wiener filter attacks for watermarks. *TU* and *T UNIV*

	Block Size 8				**Block Size 16**				**Block Size 32**			
	Median Filter		Wiener Filter		Median Filter		Wiener Filter		Median Filter		Wiener Filter	
	3 × 3	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*
***TU* (12 × 9)**												
Couple	0.00	0.93	0.00	0.00	0.00	4.63	0.00	0.00	3.70	9.26	0.00	0.00
Goldhill	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	5.56	0.00	0.00
Lake	8.33	17.59	0.00	2.78	6.48	27.78	0.00	0.00	14.81	33.33	0.00	0.93
***T UNIV* (27 × 8)**												
Couple	0.93	3.24	0.00	0.93	2.31	12.96	0.00	0.46	4.63	11.57	3.70	3.70
Goldhill	0.00	2.31	0.00	0.93	0.00	2.78	0.00	0.46	6.02	15.28	2.31	3.70
Lake	9.26	27.31	0.00	6.48	19.91	43.98	0.00	2.31	30.09	40.28	6.02	6.95

Table 3.6 Comparison of BER (%) of recovered watermark under Gaussian filter and sharpening filter attacks for watermarks *TU* and *T UNIV*.

	Block Size 8			**Block Size 16**			**Block Size 32**		
	Gaussian Filter		Sharpening	Gaussian Filter		Sharpening	Gaussian Filter		Sharpening
	3 × 3	*5 × 5*		*3 × 3*	*5 × 5*		*3 × 3*	*5 × 5*	
***TU* (12 × 9)**									
Couple	0.00	0.00	2.78	0.00	0.00	1.85	0.00	0.00	10.18
Goldhill	0.00	0.00	2.78	0.00	0.00	0.93	0.00	0.00	2.78
Lake	0.00	0.00	13.89	0.00	0.00	2.78	0.00	0.00	4.63
***T UNIV* (27 × 8)**									
Couple	0.00	0.00	3.24	0.46	0.46	4.63	2.31	2.78	12.04
Goldhill	0.00	0.00	0.93	0.00	0.00	2.31	2.78	2.78	3.24
Lake	0.93	0.93	5.71	0.00	0.00	6.94	5.09	5.09	11.57

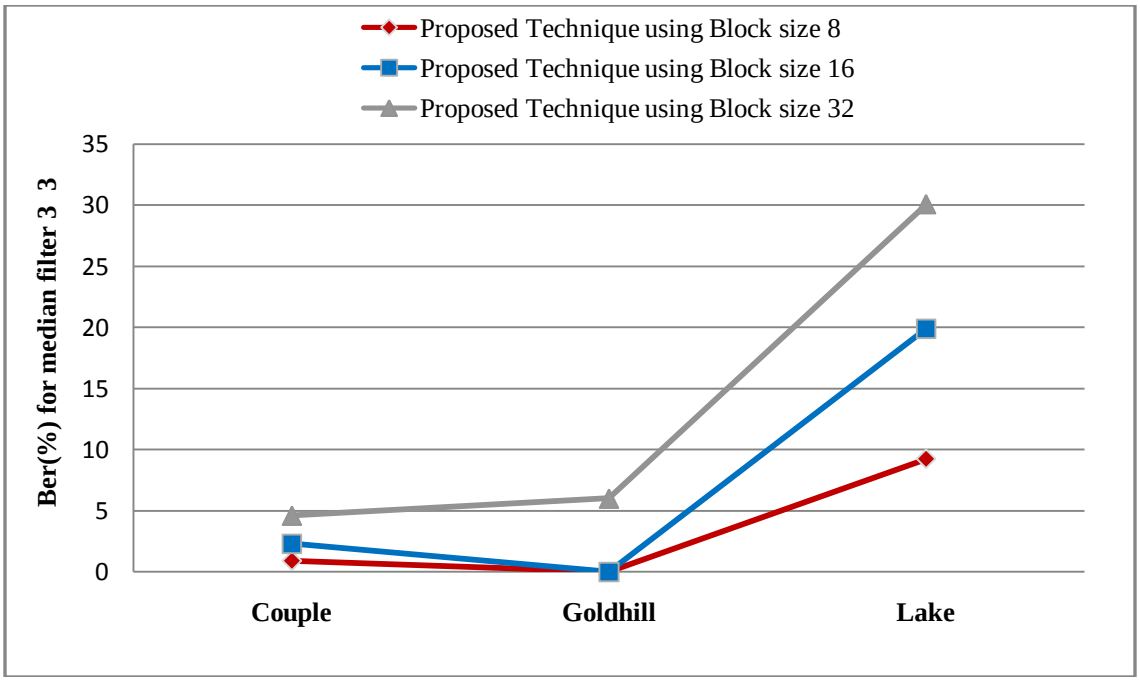


Figure 3.9 BER (%) plot of recovered watermark *T UNIV* under median filter attack of size 3×3 using block sizes 8, 16 and 32 with three host images *Couple*, *Goldhill* and *Lake*

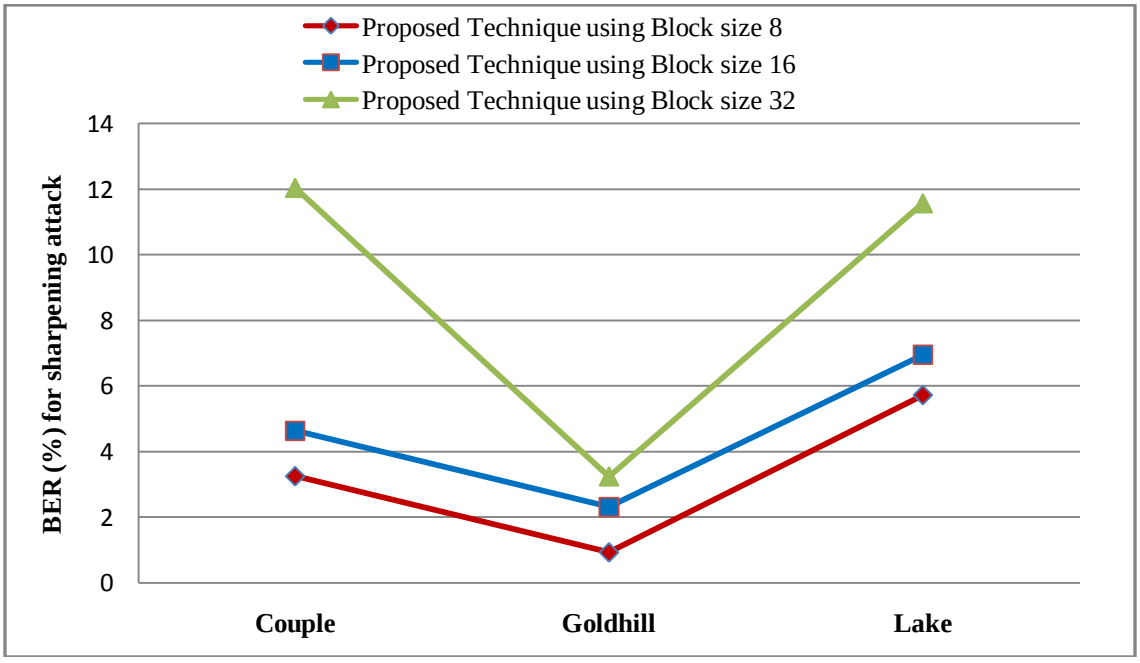


Figure 3.10 BER (%) plot of recovered watermark *T UNIV* under sharpening attack using block sizes 8, 16 and 32 with three host images *Couple*, *Goldhill* and *Lake*

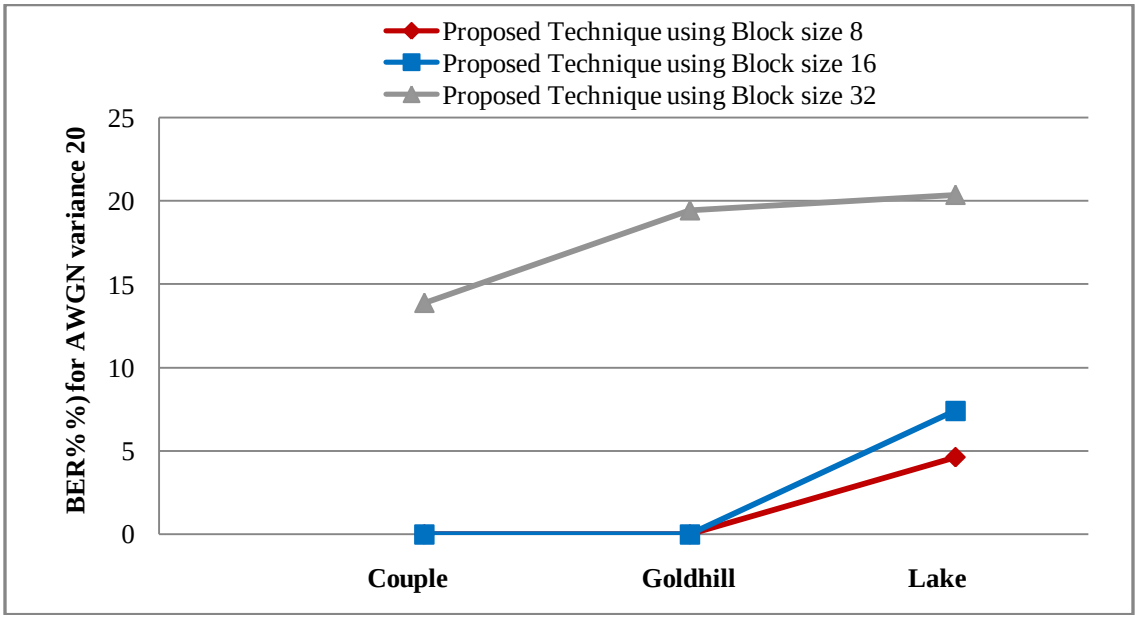


Figure 3.11 BER (%) plot of recovered watermark *TU* under AWGN attack of variance 20 using block sizes 8, 16 and 32 with three host images *Couple*, *Goldhill* and *Lake*

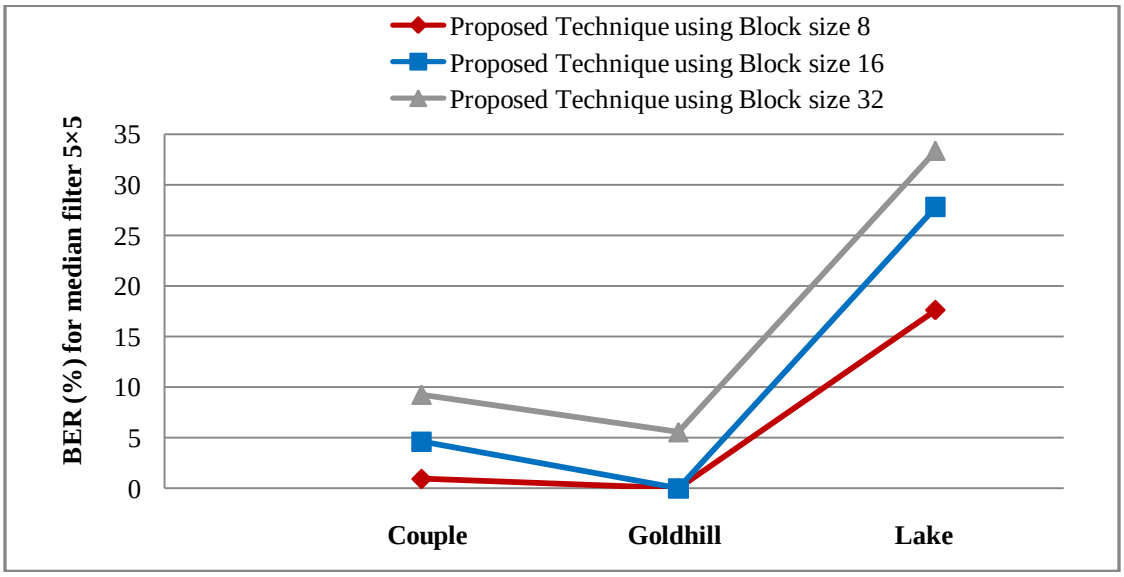


Figure 3.12 BER (%) plot of recovered watermark *TU* under median filter attack of size 5×5 using block sizes 8, 16 and 32 with three host images *Couple*, *Goldhill* and *Lake*

3.3.3 Comparison with other watermarking schemes

In this section comparison of the proposed scheme with three other watermarking schemes has been made which also use block segmentation as a part of their watermarking process. In the comparison tables wherever proposed scheme shows better performance than the compared scheme, the result is shown in the bold font for clear distinction.

3.3.3.1 Robustness Comparison with Akhaee *et al.* (2009)

Proposed watermarking scheme has been first compared with Akhaee *et al.* (2009). In this scheme image block segmentations of sizes 8, 16 and 32 have been used for the watermark embedding. In Table 3.7, BER (%) results of four attacks namely AWGN (variance 20), median filter (3×3), Gaussian filter (3×3) and JPEG compression (10%) have been compared for different watermark lengths and image block segmentations. Especially for the first three of these four attacks the proposed watermarking scheme shows exceptional results. For example for host image Barbara embedded with watermark length 128 bits and block size 8, the BER (%) results of AWGN (variance 20), median filter (3×3) and Gaussian filter (3×3) are 5.92, 7.90 and 3.33 for Akhaee *et al.* (2009). While the BER (%) results for the same attacks on the proposed scheme are zero in each case. It can be clearly observed from the Table 3.7 that the presented watermarking scheme gives better robustness results by producing lesser BER (%) more times than the competing scheme.

Although in Akhaee *et al.* (2009), the authors have used many combinations of watermark lengths and image segmentation block sizes, they have concluded that watermark length of 128 bits with block segmentation size 16 produces the best results. Therefore three variants of the presented scheme (using block size 8, 16 and 32) have been compared with the best version of their scheme in Tables 3.8 and 3.9 by keeping the same watermark length of 128 bits. As seen from these tables, proposed watermarking scheme with all three block sizes clearly outperforms the watermarking scheme of Akhaee *et al.* (2009) for the considered attacks. Figure 3.13 shows this fact graphically for the scaling attack of level 0.9 with five host images *Barbara*, *Boat*, *Baboon*, *Peppers* and *Goldhill*.

3.3.3.2 Robustness Comparison with Kalantari *et al.* (2010)

Kalantari *et al.* (2010) has used ridgelet transform in the watermarking scheme. But like the proposed scheme authors have also used block segmentation and have chosen high entropy blocks for watermarking. From the Table 3.10, it can be seen that the proposed scheme shows very good results with all three block segmentations. For example, using the host image *Baboon* embedded with a watermark of length 256 bits, the BER (%) results for JPEG compression (10%) and median filter attacks of 3×3, 5×5 and 7×7 are 7.03, 20.47, 36.71 and 41.41 for Kalantari *et al.* (2010). The results of same attacks for the proposed scheme using block size 8 are 4.30, 7.81, 24.22 and 37.89. Also the results of the proposed scheme using block sizes 16 and 32 are 4.69, 13.28, 29.69, 35.16 and 5.47, 17.97, 26.56, 31.25 respectively. Similarly Figure 3.14 shows the lesser BER (%) of the proposed scheme with all three block sizes than Kalantari *et al.* (2010) for median filter (5×5) attack. Hence it can be stated that proposed scheme is more robust than the compared scheme irrespective of the block size.

3.3.3.3 Robustness Comparison with contourlet based scheme Akhaee *et al.* (2010)

In Tables 3.11 and 3.12 the proposed scheme using block size 8, 16 and 32 has been compared with the watermarking scheme by Akhaee *et al.* (2010) for AWGN noise attack (variance 25 and 30), JPEG compression attack (quality factor 10%) and scaling attack of different levels. As is evident from the tables, proposed scheme produces much better results than the compared technique of Akhaee *et al.* (2010). Figure 3.15 shows that for an AWGN attack of variance 30, proposed technique using block size 8 and block size 16, produce lesser BER (%) than Akhaee *et al.* (2010) with four types of host images.

Plots in figures 3.13 to 3.15 once again show that proposed watermarking scheme with block size 8 produces least BER (%) results for the recovered watermark. Therefore it can be stated that robustness of the watermarking scheme using block segmentation size 8 is best as compared to other two block segmentation sizes.

Table 3.7 BER (%) comparison of recovered watermark between proposed watermarking scheme and Akhaee *et al.* (2009) (with block size 8 × 8, 16×16 and 32×32) for watermark lengths of 128, 256, 512, 1024 and 2048 bits

Block Size and Watermark Length	**Barbara**				**Boat**				**Peppers**			
	JPEG 10%	AWGN σ^2=20	Median 3×3	Gauss. 3×3	JPEG 10%	AWGN σ^2=20	Median 3×3	Gauss. 3×3	JPEG 10%	AWGN σ^2=20	Median 3×3	Gauss. 3×3
Block Size 8 and Watermark Length 128 bits												
Akhaee *et al.* (2009)	5.95	5.92	7.90	3.33	16.70	9.75	14.21	5.60	19.29	11.09	3.34	2.21
Proposed Scheme	**3.12**	**0.00**	**0.00**	**0.00**	**3.91**	**0.00**	**0.78**	**0.00**	**6.25**	**0.00**	**0.00**	**0.78**
Block Size 8 and Watermark Length 256 bits												
Akhaee *et al.* (2009)	7.80	6.33	7.06	3.16	16.39	9.54	11.11	5.46	17.25	11.23	2.78	3.26
Proposed Scheme	11.33	**0.00**	**0.00**	**0.39**	**9.37**	**2.34**	**1.95**	**1.17**	**10.94**	**3.12**	**0.39**	**1.95**
Block Size 8 and Watermark Length 512 bits												
Akhaee *et al.* (2009)	16.74	10.73	9.80	3.61	20.69	13.99	11.27	6.69	22.38	15.02	3.04	3.71
Proposed Scheme	**15.62**	**1.56**	**0,98**	**2.73**	**15.43**	**4.30**	**3.51**	**1.17**	**19.53**	**3.51**	**1.56**	**1.17**
Block Size 8 and Watermark Length 1024 bits												
Akhaee *et al.* (2009)	22.24	14.39	10.41	3.75	22.94	16.30	10.39	6.70	24.34	17.24	3.09	4.23
Proposed Scheme	25.78	**4.49**	**1.85**	**3.51**	23.92	**5.57**	**8.40**	**1.46**	26.85	**6.44**	4.10	**1.76**
Block Size 8 and Watermark Length 2048 bits												
Akhaee *et al.* (2009)	24.68	18.22	8.84	4.67	24.73	16.98	7.35	6.19	26.77	19.48	2.77	4.74
Proposed Scheme	33.84	19.63	**4.73**	**3.27**	34.03	21.04	15.62	**4.44**	34.42	24.17	13.13	9.76
Block Size 16 and Watermark Length 128 bits												
Akhaee *et al.* (2009)	2.34	1.82	3.98	1.01	1.57	1.67	4.38	0.00	3.23	2.02	0.34	0.00
Proposed Scheme	5.47	**0.78**	**0.00**	**0.00**	3.91	**0.78**	**0.00**	0.00	**3.12**	**0.78**	**0.00**	0.78
Block Size 16 and Watermark Length 256 bits												
Akhaee *et al.* (2009)	4.93	4.04	3.63	1.81	5.24	3.76	3.48	0.50	6.87	5.18	0.84	1.42
Proposed Scheme	10.16	4.69	**0.00**	**0.39**	8.59	**2.73**	**1.17**	**0.00**	8.20	5.47	**0.39**	**0.78**

Table 3.7 (*continued***)** BER (%) comparison of recovered watermark between proposed watermarking scheme and Akhaee *et al.* (2009) (with block size 8 × 8, 16×16 and 32×32) for watermark lengths of 128, 256, 512, 1024 and 2048 bits

Block Size and Watermark Length	**Barbara**				**Boat**				**Peppers**			
	JPEG 10%	AWGN σ^2=20	Median 3×3	Gauss. 3×3	JPEG 10%	AWGN σ^2=20	Median 3×3	Gauss. 3×3	JPEG 10%	AWGN σ^2=20	Median 3×3	Gauss. 3×3
Block Size 16 and Watermark Length 512 bits												
Akhaee *et al.* (2009)	10.58	7.02	3.72	4.08	6.50	4.50	3.96	1.24	8.33	7.13	0.82	1.40
Proposed Scheme	12.89	8.00	**0.98**	**2.34**	17.38	8.20	7.42	1.37	16.40	8.98	5.66	3.12
Block Size 32 and Watermark Length 128 bits												
Akhaee *et al.* (2009)	3.01	1.13	1.59	2.13	2.96	1.91	4.38	0.37	2.42	3.02	0.80	1.60
Proposed Scheme	4.68	5.47	**0.00**	**0.00**	**1.56**	6.25	**1.56**	**0.00**	5.47	6.25	1.56	0.78
Block Size 32 and Watermark Length 256 bits												
Akhaee *et al.* (2009)	19.04	14.98	7.17	10.55	15.00	10.74	5.91	10.56	22.99	17.41	2.92	7.90
Proposed Scheme	**13.28**	**12.11**	10.16	**5.08**	23.05	13.28	15.62	15.62	**17.97**	**11.72**	15.23	10.55

Table 3.8 BER (%) comparison of recovered watermark of length 128 bits between Akhaee *et al*. (2009) with block size 16 and proposed scheme with block sizes 8, 16 and 32 under scaling attack of different levels.

Akhaee *et al.* (2009) Watermarking Scheme (with block size 16)				**Proposed Watermarking Scheme (with block size 8)**			**Proposed Watermarking Scheme (with block size 16)**			**Proposed Watermarking Scheme (with block size 32)**		
Image	Scaling Level			Scaling Level			Scaling Level			Scaling Level		
	0.75	*0.9*	*1.1*	*0.75*	*0.9*	*1.1*	*0.75*	*0.9*	*1.1*	*0.75*	*0.9*	*1.1*
Barbara	9.13	2.79	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	0.78	**0.00**	**0.00**	4.69
Boat	9.12	4.46	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	2.34	**0.00**	**1.56**	11.72
Baboon	5.70	1.63	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	0.00	**0.00**	**0.00**	0.00
Peppers	5.73	1.27	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	1.56	**0.00**	**0.78**	5.47
Goldhill	6.75	2.14	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	0.00	**0.00**	**0.00**	0.00

Table 3.9 BER (%) comparison of recovered watermark of length 128 bits between Akhaee *et al.* (2009) with block size 16 and proposed scheme with block sizes 8, 16 and 32 for median filter and Gaussian filter attacks.

Akhaee *et al.* (2009) Watermarking Scheme (with block size 16)					**Proposed Watermarking Scheme (with block size 8)**				**Proposed Watermarking Scheme (with block size 16)**				**Proposed Watermarking Scheme (with block size 32)**			
Image	Median Filter		Gaussian Filter		Median Filter		Gaussian Filter		Median Filter		Gaussian Filter		Median Filter		Gaussian Filter	
	3 × 3	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*	*3 × 3*	*5 × 5*
Barbara	3.98	16.37	1.01	3.84	**0.00**	**5.47**	**0.00**	**0.00**	**0.00**	**1.56**	**0.00**	**0.00**	**0.00**	**4.69**	**0.00**	**0.00**
Boat	4.38	15.35	0.00	0.00	**0.78**	**3.91**	**0.00**	**0.00**	**0.00**	**2.34**	**0.00**	**0.00**	1.56	11.72	**0.00**	**0.00**
Baboon	3.20	17.91	0.38	0.38	**3.12**	21.87	**0.00**	**0.00**	9.37	29.69	**0.00**	**0.00**	24.22	34.37	**0.00**	**0.00**
Peppers	0.34	3.00	0.00	0.74	**0.00**	6.25	0.78	0.78	**0.00**	**0.78**	0.78	0.78	**1.56**	**2.34**	**0.78**	**0.78**
Goldhill	0.00	8.47	0.00	0.00	**0.00**	**1.56**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	10.94	**0.00**	**0.00**

Table 3.10 BER (%) comparison of recovered watermark of length 256 bits between Kalantari *et al.* (2010) and proposed scheme with block sizes 8, 16 and 32 for JPEG compression and median filter attack of different types.

Image	**Kalantari *et al.* (2010)**				**Proposed Scheme (Block Size 8)**				**Proposed Scheme (Block Size 16)**				**Proposed Scheme (Block Size 32)**			
	JPEG	Median Filtering			JPEG	Median Filtering			JPEG	Median Filtering			JPEG	Median Filtering		
	10%	*3 × 3*	*5 × 5*	*7 × 7*	*10%*	*3 × 3*	*5 × 5*	*7 × 7*	*10%*	*3 × 3*	*5 × 5*	*7 × 7*	*10%*	*3 × 3*	*5 × 5*	*7 × 7*
Boat	9.64	14.38	26.10	37.89	**9.37**	**1.95**	**9.37**	**17.97**	**8.59**	**1.17**	**8.20**	**17.97**	23.05	15.62	**25.39**	**31.25**
Baboon	7.03	20.47	36.71	41.41	**4.30**	**7.81**	**24.22**	**37.89**	**4.69**	**13.28**	**29.69**	**35.16**	**5.47**	**17.97**	**26.56**	**31.25**
Peppers	8.07	3.44	14.45	25.07	10.94	**0.78**	**5.86**	**13.28**	8.20	**0.39**	**3.12**	**10.16**	17.97	15.23	18.75	**19.92**
Lena	9.24	10.16	21.48	28.52	18.75	**0.39**	**1.95**	**6.64**	9.37	**2.34**	**7.81**	**12.89**	16.41	16.41	**19.92**	**23.44**

Table 3.11 BER (%) comparison of recovered watermark of length 128 bits between Akhaee *et al.* (2010) with block size 16 and proposed scheme with block sizes 8, 16 and 32 for AWGN noise attack and JPEG compression attack of quality factor 10

Akhaee *et al.* (2010) Watermarking Scheme (with block size 16)				**Proposed Watermarking Scheme (with block size 8)**			**Proposed Watermarking Scheme (with block size 16)**			**Proposed Watermarking Scheme (with block size 32)**		
Host Image	AWGN attack		JPEG comp.	AWGN attack		JPEG comp.	AWGN attack		JPEG comp.	AWGN attack		JPEG comp.
	σ^2=25	σ^2=30	10%	σ^2=25	σ^2=30	10%	σ^2=25	σ^2=30	10%	σ^2=25	σ^2=30	10%
Baboon	0.5	1.5	7.3	**0.00**	**0.00**	**0.00**	0.78	**0.78**	**0.78**	7.03	7.03	**1.56**
Barbara	0.5	0.95	3.7	**0.00**	**0.00**	3.12	1.56	2.34	5.47	6.25	7.81	4.69
Bridge	2.3	5	8.1	**0.00**	**0.00**	**2.34**	**1.56**	**2.34**	**3.91**	7.03	7.81	3.12
Couple	2.3	6	7	**0.00**	**0.00**	3.91	**0**	**0.78**	**3.12**	**7.81**	7.81	3.12

Table 3.12 BER (%) comparison of recovered watermark of length 128 bits between Akhaee *et al.* (2010) with block size 16 and proposed scheme with block sizes 8, 16 and 32 under scaling attack of different levels.

Akhaee *et al.* (2010) Watermarking Scheme (with block size 16)						**Proposed Watermarking Scheme (with block size 8)**					**Proposed Watermarking Scheme (with block size 16)**					**Proposed Watermarking Scheme (with block size 32)**				
Host Image	Scaling Factor					Scaling Factor					Scaling Factor					Scaling Factor				
	0.75	0.9	1.1	1.5	2	0.75	0.9	1.1	1.5	2	0.75	0.9	1.1	1.5	2	0.75	0.9	1.1	1.5	2
Baboon	10.39	1.17	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00
Barbara	31.02	0.31	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	0.78	0.00	0.00	**0**.00	**0**.00	4.68	0.00	0.00
Bridge	7.85	3.13	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	3.12	0.00	0.00
Couple	13.28	5.47	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	0.00	0.00	0.00	**0**.00	**0**.00	0.78	0.00	0.00

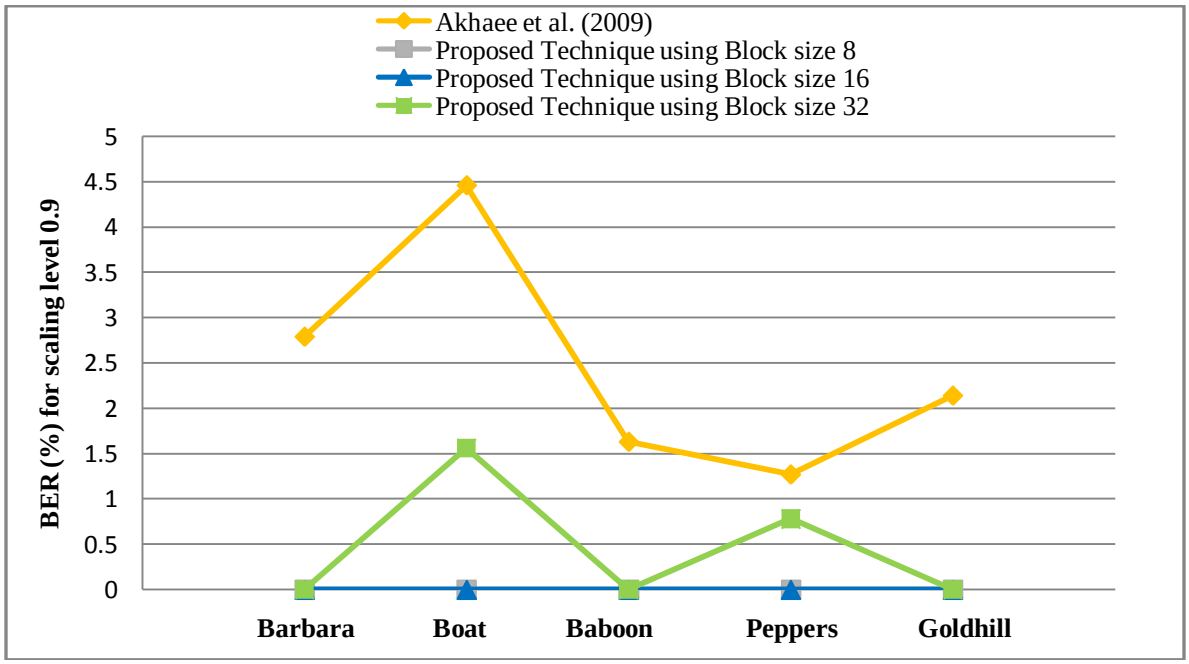


Figure 3.13 Plot of BER (%) of recovered watermark of length 128 bits under scaling attack of level 0.9 for Akhaee *et al.* (2009) and proposed technique using block size 8, 16 and 32 with five host images

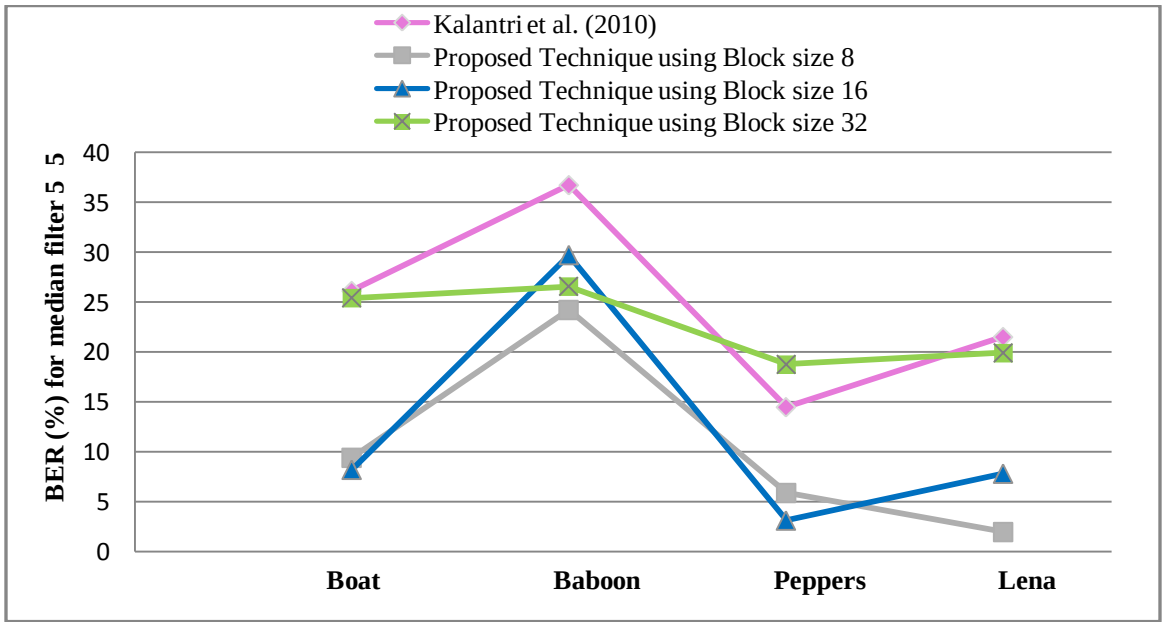


Figure 3.14 Plot of BER (%) of recovered watermark of length 256 bits under median filter attack (5×5) for Kalantri *et al.* (2010) and proposed technique using block size 8, 16 and 32 with four host images

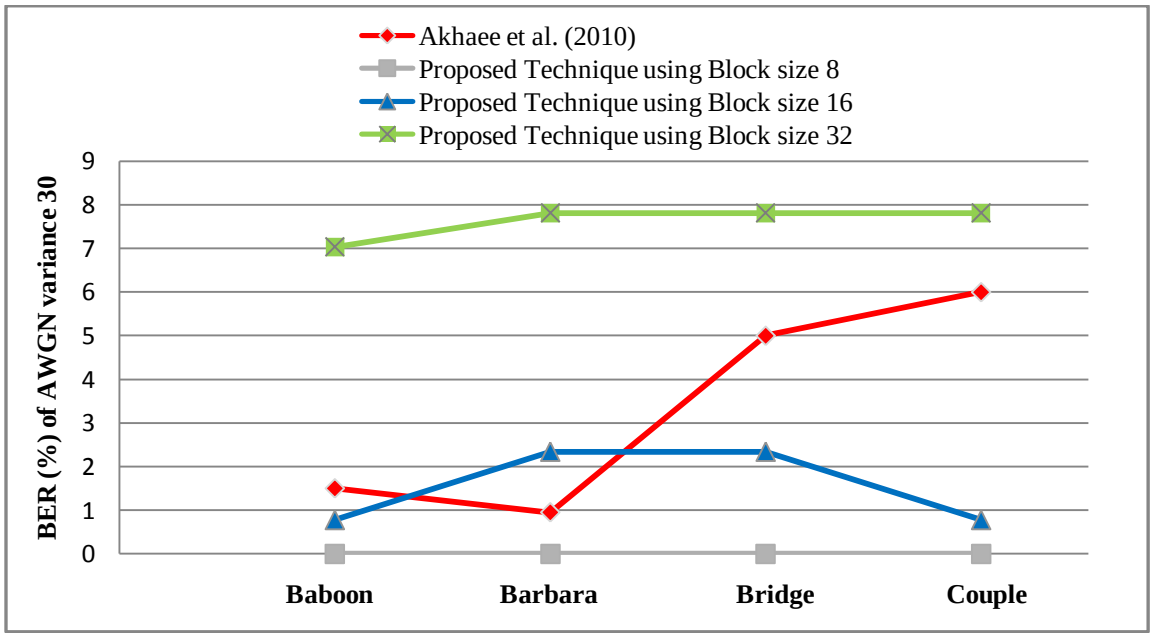


Figure 3.15 Plot of BER (%) of recovered watermark of length 128 bits under AWGN attack of variance 30 for Akhaee *et al.* (2010) and proposed technique using block size 8, 16 and 32 with four host images

3.4 CHAPTER SUMMARY

In this chapter 8×8, 16×16 and 32×32 image pixel block segmentations have been used with a DWT based semi-blind robust watermarking scheme. For comparing the performance of three different sized block segmentations, two small binary watermarks have been used. Length of both the watermarks is less than the total number of blocks in the 32×32 block segmentation. Presented watermarking scheme with all three block sizes, shows commendable resistance against a lot of common watermarking attacks. In this experimental study it has been observed that BER (%) of recovered watermark from both the attacked and unattacked watermarked images is least for the 8×8 block segmentation. So it is inferred that use of 8×8 block segmentation makes the watermarking more robust as compared to the other block segmentations. Also a much bigger watermark of length 4096 bits could be embedded by using 8×8 block segmentation as compared to 16×16 and 32×32 block segmentations which allow the maximum watermark length of 1024 and 256 respectively for a 512×512 sized host image.

Therefore it is concluded that 8×8 image pixel block segmentation is best for embedding the watermark in an image and so it has been used in the next chapters for the watermarking purpose.

Fourth chapter analyzes the dynamic strength factor by varying its adjusting parameter from minimum to maximum possible values. Security of the sideband information of the presented semi-blind technique has also been discussed.

CHAPTER 4

DYNAMIC STRENGTH FACTOR ANALYSIS IN ROBUST IMAGE-ADAPTIVE WATERMARKING

THIS chapter carries outs the detailed analysis of the dynamic strength factor, introduced in the last chapter. Robustness of the watermarking scheme is determined by embedding three different sized watermarks in many host images and by applying common watermarking attacks. A novel method to ensure effective security of the side information has been presented. An encoding technique to further boost the side information security has also been discussed.

4.1 INTRODUCTION

Robust watermarking is mainly used to protect the legitimate owner's intellectual property rights over his digital content. Therefore a watermark embedded in a host image using a robust watermarking scheme should be able to resist the malicious as well as non-malicious watermarking attacks. The best way to make a watermark robust is to make it adapt to the local image characteristics and viewing conditions (Podilchuk and Zeng, 1998).

DWT transform based watermarking technique presented in the last chapter is a robust image-adaptive watermarking technique. Image-adaptive nature of the scheme is manifested in the use of high entropy blocks of the host image for watermark embedding as shown in Section 3.2.1. Use of standard deviations of the DWT coefficients of these high entropy blocks in deriving the strength factor of the watermarking also indicates towards the image adaptivity of the scheme (Section 3.3). As concluded in third chapter 8×8 block segmentation is best for the watermarking purpose, so only this segmentation has been used in the present chapter with watermarking technique described in the previous chapter. Main focus in this chapter is on the detailed analysis of dynamic strength factor and security of the side information. Three watermarks, small (*TU* of size 25 × 18), medium (*Copyright* of size 50 × 20) and large (*Thapar_Univ* of size 80 × 20) as shown in Appendix –II have been used.

4.2 SIGNIFICANCE AND ANALYSIS OF DYNAMIC STRENGTH FACTOR

The dynamic strength factor i.e. *DSF* has been defined in the section 3.2.1.1. In the expression of *DSF* in (3.4) numerator is σ_i, the standard deviation of approximation coefficient matrix of any high entropy block. Denominator is σ_{max}, the maximum standard deviation in all the selected high entropy blocks and ρ the adjusting parameter of *DSF* is the power of denominator. Its value varies between 1 and 2.

The concept of dynamic strength factor is in complete contrast with many watermarking techniques in the literature like Akhaee *et al.* (2009) which have used a static or single valued strength factor. These techniques have put in a lot of computational effort to get an optimized value of strength factor for one image. But the dynamic strength factor introduced in the last chapter is more image-adaptive in nature and hence is more efficient. Its value gets changed according to the values of low frequency approximation coefficients of the selected high entropy blocks. Therefore dynamic strength factor has a different value for every high entropy block. Adjusting parameter of denominator, ρ plays an important role in determining the value of strength factor. For a particular host image as the value of adjusting parameter ρ is increased from 1 to 2, an almost a linear increase in the PSNR of watermarked image and a nearly exponential rise in the BER (%) of extracted watermark is obtained, which is shown in Figure 4.1 In this figure watermarked *Lena* image's PSNR and recovered watermark *TU*'s BER (%) have been plotted against adjusting parameter ρ of strength factor. The value of ρ needs to be kept between 1 and 2. If the value of ρ is made less than 1, the watermarked image's PSNR becomes very low and watermark starts getting visible. If the value of ρ is made higher than 2, the BER (%) of recovered watermark becomes very high indicating a very high distortion in the extracted watermark.

Six host images, their watermarked versions and recovered watermarks have been shown in the Figure 4.2 keeping watermarked image PSNR as 45 dB. Figure 4.3 shows the plots of watermarked image PSNR and recovered watermark BER (%) with the variation of adjusting parameter ρ from 1 to 2 for seven host images along with three types of watermarks. From the plots it is observed that by increasing the value of adjusting parameter ρ, the watermark becomes

progressively weaker and weaker which results in the increase of PSNR of the watermarked image. But it is also associated with the progressive reduction in the robustness as BER (%) of recovered watermark goes on increasing. Thus it can be said that the increase in PSNR of the watermarked image is proportional to the increase in the BER (%) of the extracted watermark. But PSNR of the watermarked image is linked with the imperceptibility of the watermark in a watermarked image; higher the PSNR better is the imperceptibility. Also BER (%) is linked with the robustness of the watermark; lesser the BER (%) higher is the robustness. Therefore it is established experimentally from the plots in Figure 4.3 that imperceptibility and robustness in the watermarking are in direct conflict with each other. If one is increased, the other one is bound to decrease and vice-versa.

Adjusting parameter ρ of strength factor, which is plotted on X-axis in the plots of Figure 4.1 and 4.3, is a tool by which the PSNR of the watermarked image can be kept to a desired level while knowing the resultant BER (%) of the extracted watermark. Presented method is much easier and efficient as compared to the optimization of strength factor in dark.

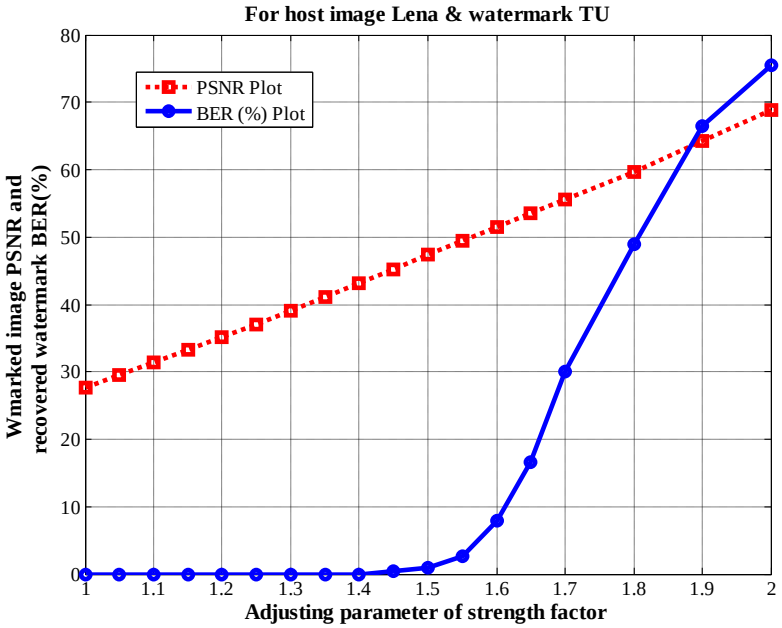


Figure 4.1 Plot of watermarked image PSNR(dB) and recovered watermark BER(%) with adjusting parameter ρ of strength factor for host image *Lena* and watermark *TU*

Figure 4.2 Original image (Column 1), watermarked image with PSNR as 45 dB (Column 2) and recovered watermark (Column 3)

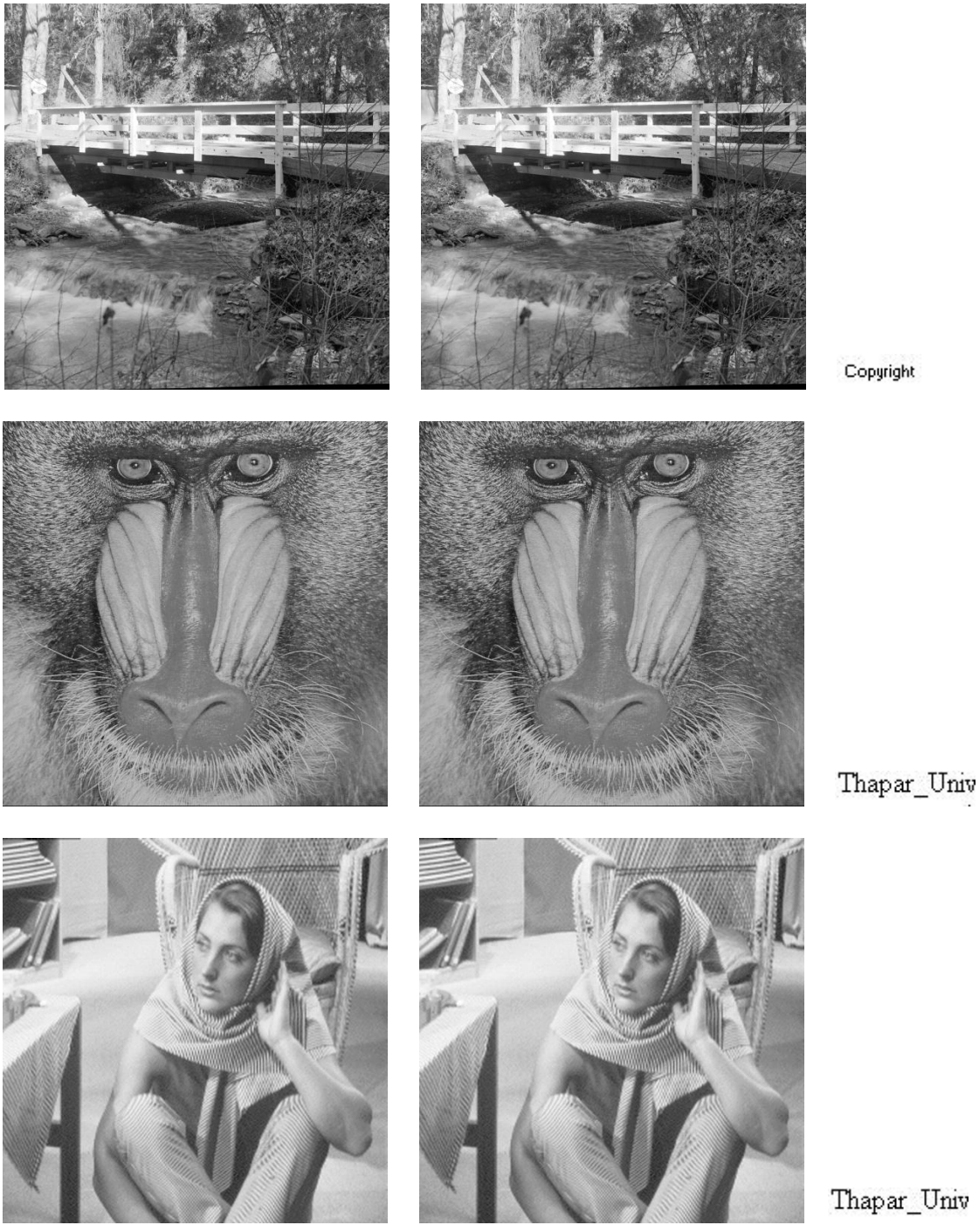
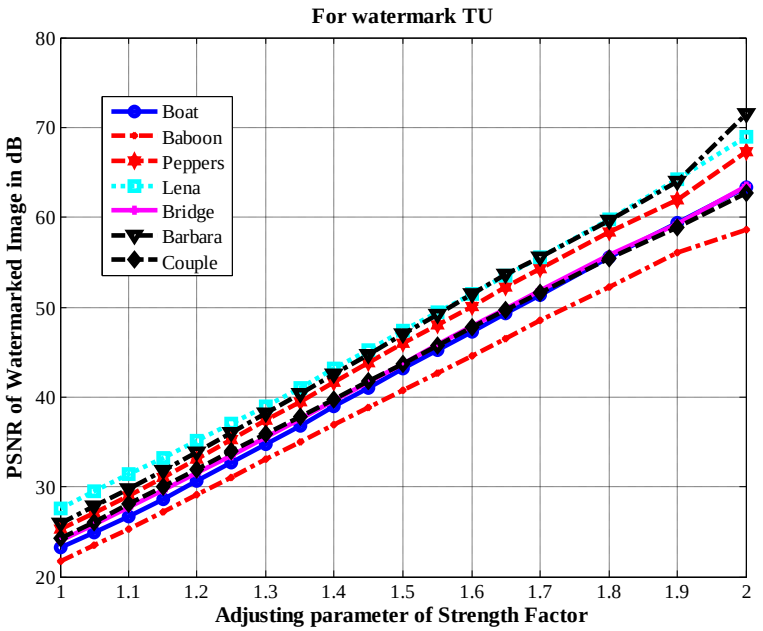
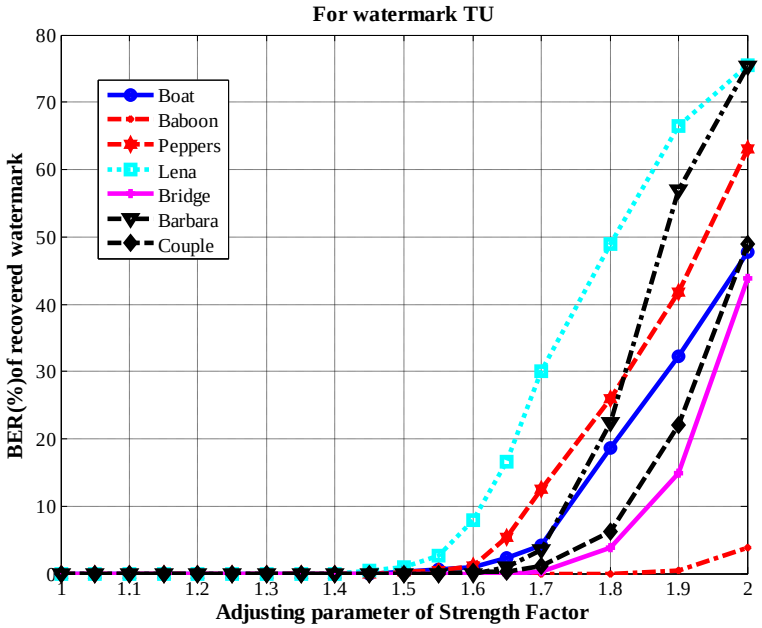


Figure 4.2 Original image (Column 1), watermarked image with PSNR as 45 dB (Column 2) and recovered watermark (Column 3)

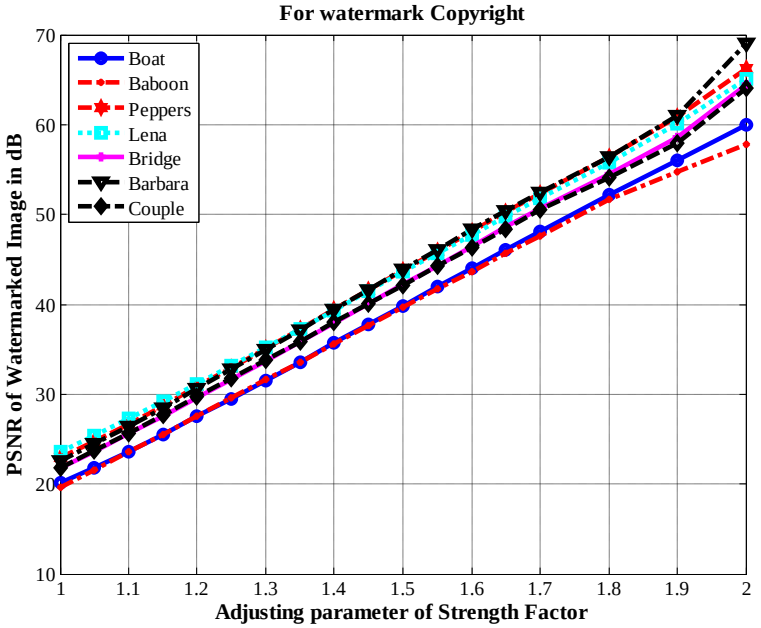


(a)

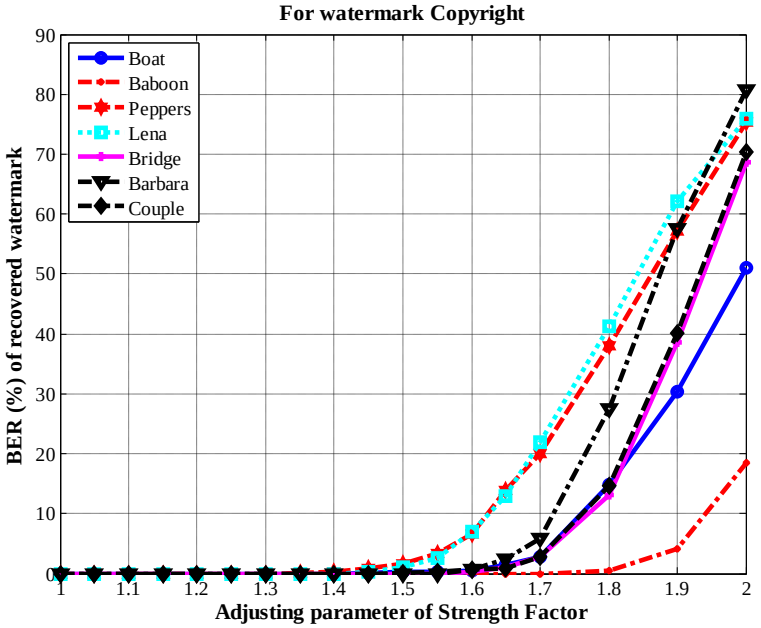


(b)

Figure 4.3 Plots of watermarked image PSNR (dB) and recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively using seven different images; (a - b) for small watermark *TU*, (c - d) for medium watermark *copyright* and (e - f) for large watermark Thapar_*Univ*

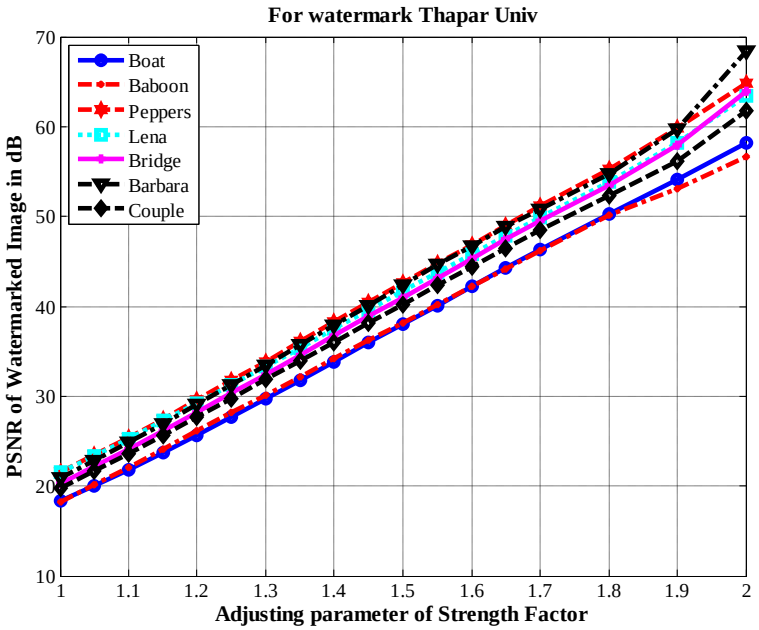


(c)

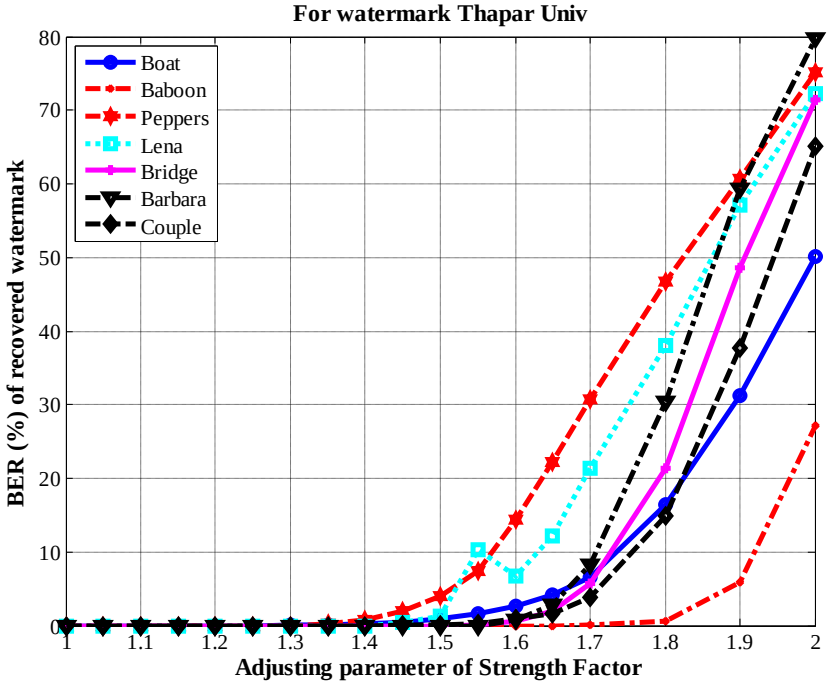


(d)

Figure 4.3 Plots of watermarked image PSNR (dB) and recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively using seven different images; (a - b) for small watermark *TU*, (c - d) for medium watermark *copyright* and (e - f) for large watermark Thapar_*Univ*



(e)



(f)

Figure 4.3 Plots of watermarked image PSNR (dB) and recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively using seven different images; (a - b) for small watermark *TU*, (c - d) for medium watermark *copyright* and (e - f) for large watermark Thapar_*Univ*

4.3 SECURITY OF SIDE INFORMATION

High entropy block positions, means of low frequency coefficients of these blocks and size of the watermark are sent as side information in the watermark embedding process, which is later on used during extraction of watermark from the watermarked image. A person with malicious intentions could try to intercept the side information to know about high entropy positions so that he can remove the watermark. But the high entropy block positions which are sent in the side information, are not related directly to the host image. These positions are of a cell array in which the 8×8 blocks of the image are stored. There are at least 16 ways by which the 8×8 blocks from the image can be picked and there are 13 ways by which these blocks can be placed in a cell array. So, it is very difficult for a malicious interceptor to correlate these cell array positions of blocks with their actual positions in the watermarked image as he does not know in which way the blocks have been picked from the image and how the blocks have been placed in a cell array.

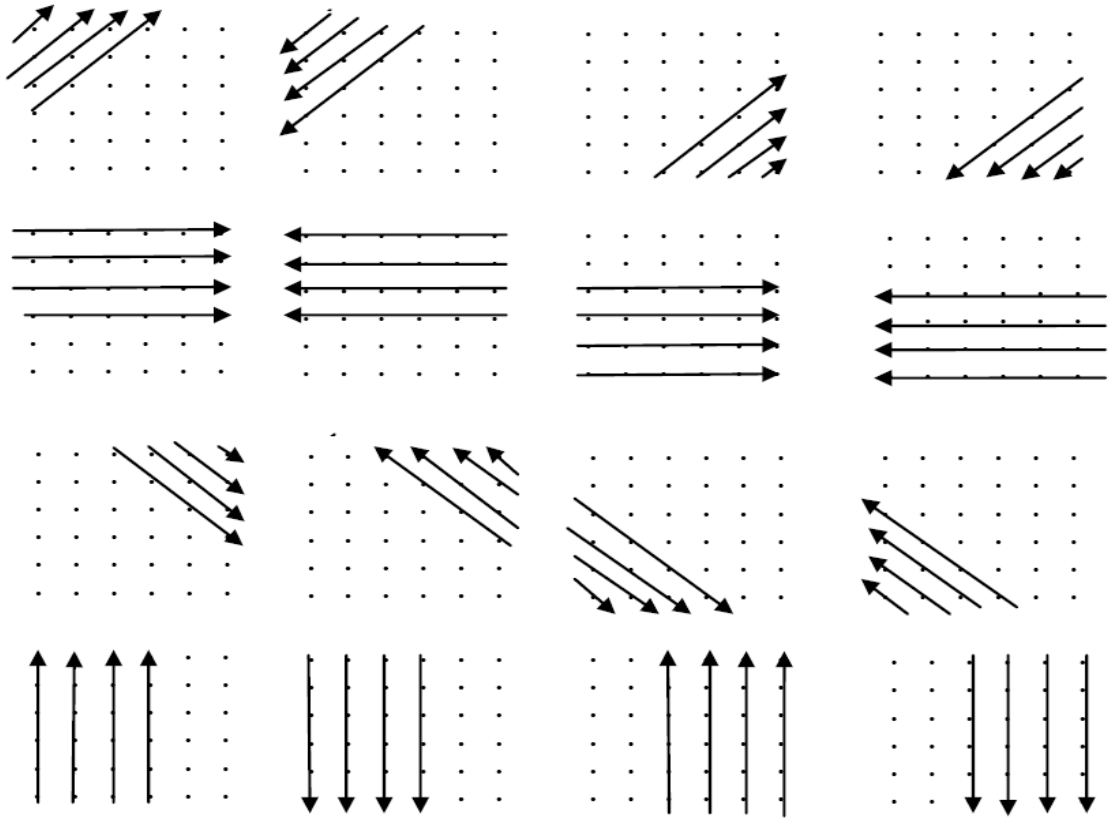


Figure 4.4 Sixteen ways in which 8×8 blocks of the image are picked up by moving along both diagonals and rows and columns for storing in a cell array

Picking 8×8 blocks from image

For illustration an 8×8 block of the image has been represented by a single dot. Blocks can be picked up by moving along both the diagonals, rows and columns respectively for storing in cell array. Figure 4.4 shows the 16 ways in which blocks can be picked up along the two diagonals and along the rows and columns.

Storing 8×8 blocks in cell array

There are 4096, 8×8 blocks in a 512×512 image. These blocks can be stored in a cell array in the following 13 ways-

1×4096	2×2048	4×1024	8×512	16×256
32×128	64×64	128×32	256×16	512×8
1024×4	2048×2	4096×1		

Probability p with which a malicious user can correctly estimate the high entropy block positions in the watermarked image from the intercepted side information can be calculated as shown below-

$$p = (\textit{No. of ways of picking the } 8\times8 \textit{ blocks from image})^{-1} \times (\textit{No. of ways of arranging the } 8\times8 \textit{ blocks in cell array})^{-1}$$

$$p = \frac{1}{16} \times \frac{1}{13}$$

$$p = \frac{1}{208} = 0.48\,\%$$

Therefore as has been calculated the success rate is less than half percent. An ill-intentioned interceptor will have to put in a lot of effort and time before he is able to remove the watermark bits by knowing the exact location of high entropy blocks. But he would have probably damaged the watermarked image quite severely till that time and hence won't be able to make any commercial gains from the image.

For even greater security of proposed watermarking system the side information data can be sent in an encoded form. One way of encoding, which could be applied is as follows:

Encoding at watermark embedding end

Step 1. Original number to be encoded is first multiplied by 2.

Step 2. Obtained doubled number is subtracted from another number which has 1 at its most significant place (that is at the leftmost place) while the other digits in the number are

zeros which are one more in count than the number of digits in the integral part of the doubled data number.

The difference result obtained from Step 2 is the Encoded number, which is sent in the side information.

Decoding at watermark extraction end,

Step 1. Received number is subtracted from a number which has 1 at its most significant place and the other digits in the number are zeros which are one more in count than the number of digits in the integral part of the received number.

Step 2. In the difference obtained, the two most significant digits are dropped, which are 9 and 0 always.

Step 3. The remaining number is divided by two.

The number obtained as quotient is the Decoded number which is equal to the Original number.

Table 4.1 Examples of encoding and decoding at watermark embedding and extraction ends respectively

Encoding				**Decoding**			
Original Number	Step 1	Step 2	Encoded Number	Step 1	Step 2	Step 3	Decoded Number
1	1×2 = 2	100 – 2 = 98	98. Sent in the side information	1000 – 98 = 902	90 is dropped. Remaining number is 2.	2 ÷ 2 = 1	1
893.756	893.756×2 = 1787.512	100,000 - 1787.512 = 98212.488	98212.488. Sent in the side information	1000, 000 - 98212.488 = 901787.512	90 is dropped. Remaining number is1787.512	1787.512 ÷ 2 = 893.756	893.756
4096	4096 × 2 = 8192	100,000 – 8192 = 91808	91808. Sent in the side information	1000,000 – 91808 = 908192	90 is dropped. Remaining number is 8192	8192 ÷ 2 = 4096	4096

The biggest number required to be encoded is 4096, comprising of total 8×8 blocks in a 512×512 sized host image. Therefore the encoding method is explained below by taking three numbers; one very small, one of middle value and one of maximum value.

In this thesis, the above discussed side information security will be provided in the forthcoming proposed techniques as well.

4.4 EXPERIMENTAL RESULTS AND DISCUSSIONS

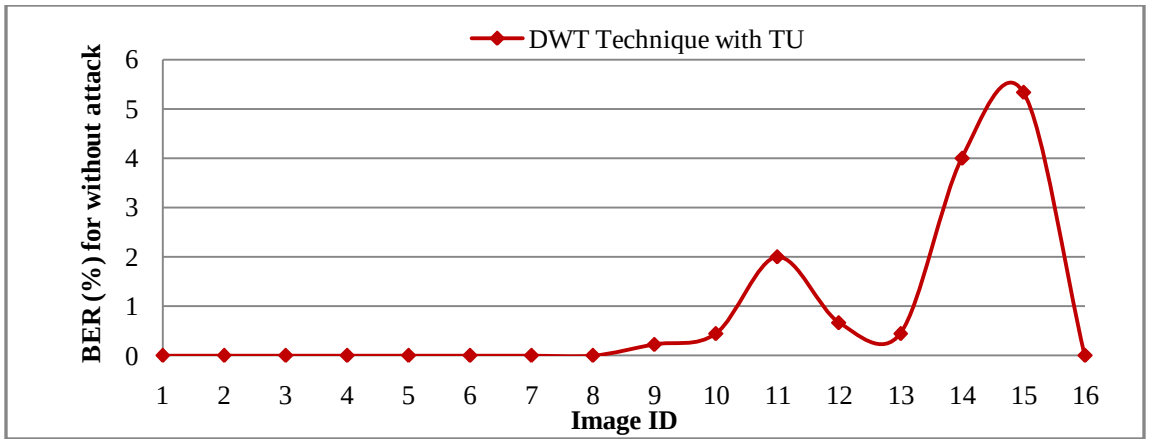
In this section performance of the DWT based watermarking technique is evaluated firstly without applying any attack and then by applying common watermarking attacks. Afterwards presented scheme has been compared with established watermarking techniques of literature.

4.4.1 Performance analysis without applying attacks

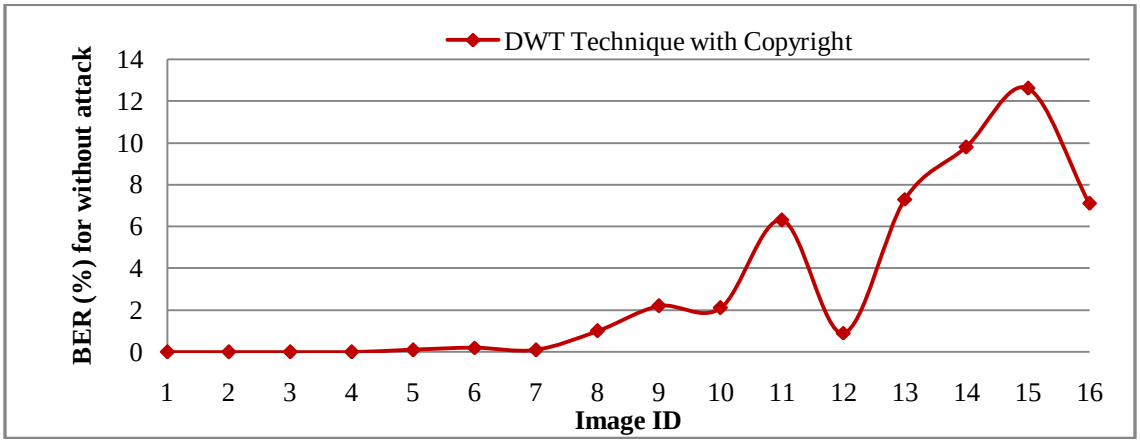
The DWT based technique (with 8×8 block segmentation) has been used to embed three different sized watermarks in sixteen host images shown in Appendix-I. The BER (%) of recovered watermarks from the unattacked watermarked images have been plotted against their corresponding host images in Figure 4.5 for the three watermarks. As is predictable BER (%) of recovered *TU* watermark is least for all the sixteen images while BER (%) of recovered *Thapar_Univ* watermark is maximum for all these images. Also there are two images *Barbara* and *Aerial* which have their BER (%) values as zero for all three watermarks as observed from Figure 4.5.

4.4.2 Performance Analysis under common attacks

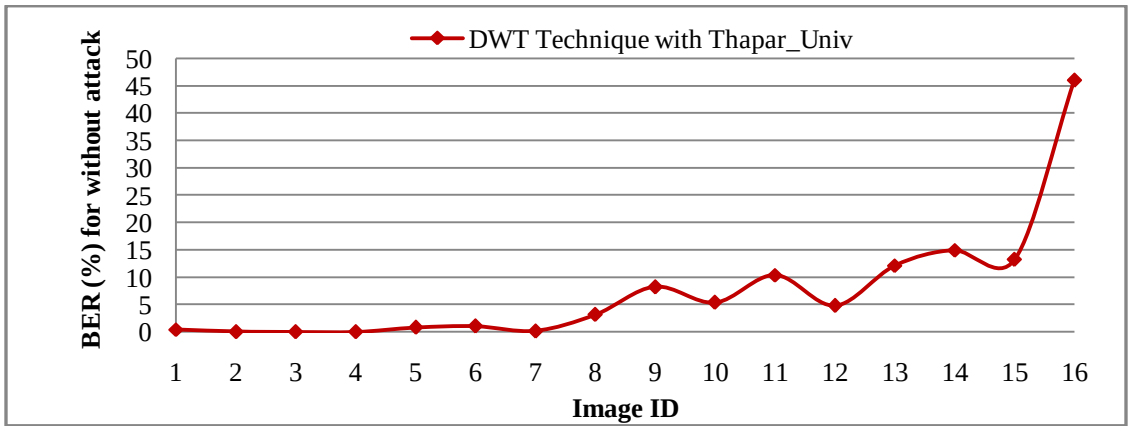
Results of common watermarking attacks have been shown after embedding three different sized watermarks in host images *Boat*, *Barbara* and *Peppers*. All the attacks have been applied on the watermarked images having PSNR value 45 dB. As discussed earlier, by using the appropriate value of adjusting parameter (ρ) of strength factor any desired PSNR value of the watermarked image can be obtained. Table 4.2 shows the BER (%) values of the recovered watermark on applying JPEG compression, AWGN noise, salt and pepper noise, scaling, sharpening and median, wiener and Gaussian filter attacks with *Boat* image. Similarly Table 4.3 and Table 4.4 show the BER (%) results for these attacks with *Barbara* and *Peppers* images respectively. As observed from the tables, JPEG compression attack with quality factor 10% causes highest BER (%) values and scaling attack of level 1.5 causes minimum BER (%) values with all three watermarks.



(a)



(b)



(c)

Figure 4.5 BER (%) plot of recovered watermark without applying any attack on sixteen watermarked images having PSNR as 45 dB with watermark (a) *TU* (b) *Copyright* (c) *Thapar_Univ*

Table 4.2 Performance of presented DWT technique in terms of BER (%) of recovered watermark under various attacks with three different sized watermarks and host image *Boat*, for watermarked image PSNR as 45 dB

Technique / Attack	Proposed DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	15.33	24.4	30.44
AWGN (σ^2=20)	3.78	3.70	8.06
Median Filter (3×3)	3.78	7.10	14.19
Salt and Pepper (p=0.01)	10.22	12.50	16.56
Scaling (1.5)	0.22	0.70	2.94
Sharpening	12.00	21.20	24.00
Wiener Filter (3×3)	0.67	1.80	5.44
Gaussian Filter (3×3)	1.56	1.50	3.88

Table 4.3 Performance of presented DWT technique in terms of BER (%) of recovered watermark under various attacks with three different sized watermarks and host image *Barbara* for watermarked image PSNR as 45 dB

Technique / Attack	Proposed DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	14.89	25.60	31.50
AWGN (σ^2=20)	1.78	4.40	7.31
Median Filter (3×3)	0.89	1.80	4.19
Salt and Pepper (p=0.01)	8.67	13.70	15.75
Scaling (1.5)	0.00	0.00	0.06
Sharpening	9.11	18.1	24.19
Wiener Filter (3×3)	0.67	0.90	1.06
Gaussian Filter (3×3)	2.00	3.30	3.38

Table 4.4 Performance of presented DWT technique in terms of BER (%) of recovered watermark under various attacks with three different sized watermarks and host image *Peppers* for watermarked image PSNR as 45 dB

Technique / Attack	Proposed DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	18.67	26.80	32.75
AWGN (σ^2=20)	4.22	5.80	8.63
Median Filter (3×3)	0.67	3.30	8.44
Salt and Pepper (p=0.01)	7.11	14.20	19.12
Scaling (1.5)	0.00	0.90	3.69
Sharpening	7.78	13.90	17.88
Wiener Filter (3×3)	0.89	1.60	6.50
Gaussian Filter (3×3)	1.56	1.70	5.56

Table 4.5 BER comparison of recovered watermark for various attacks between proposed watermarking method and Tsougenis *et al.* (2013) with watermark length of 100 bits, host image size 256×256 and watermarked image PSNR 45 dB.

Attack / Technique	JPEG Compression				Median Filter		Random Noise (%)					Scaling					
	20	40	60	80	6×6	8×8	1	2	3	4	5	0.5	0.7	0.9	1.1	1.3	1.5
Host Image Lena																	
Tsougenis *et al.* (2013) PCET	0.01	0.00	0.00	0.00	0.46	0.54	0.00	0.01	0.04	0.22	0.38	0.05	0.03	0.04	0.08	0.08	0.12
Proposed DWT Technique	0.13	0.02	0.01	0.02	**0.33**	**0.37**	0.01	**0.01**	**0.01**	**0.01**	**0.01**	**0.01**	0.20	0.10	**0.06**	**0**.00	**0**.00
Host Image Peppers																	
Tsougenis *et al.* (2013) PCET	0.02	0.00	0.00	0.00	0.31	0.45	0.00	0.03	0.17	0.28	0.48	0.13	0.05	0.08	0.17	0.17	0.20
Proposed DWT Technique	0.05	**0**.00	0.01	**0**.00	**0.31**	**0.34**	**0**.00	**0**.00	**0**.00	**0**.00	**0**.00	**0**.00	0.13	**0.06**	**0.01**	**0**.00	**0**.00

Table 4.6 BER (%) comparison of recovered watermark for various attacks between proposed watermarking method and Nezhadarya *et al.* (2011) with watermark length of 256 bits, host image size 512×512 and watermarked image PSNR 42 dB.

Attack / Technique	JPEG Compression					Median Filter		Gaussian Filter		Scaling
	20	30	40	50	60	3×3	5×5	3×3	5×5	2
Host Image Peppers										
Nezhadarya *et al.* (2011) GDWM	1.41	0.18	0.04	0.00	0.00	1.17	6.64	0.00	0.58	0.00
Proposed DWT Technique	**0.39**	**0**.00	0.39	0.39	**0.00**	**0.00**	**4.30**	0.78	0.78	**0.00**
Host Image Baboon										
Nezhadarya *et al.* (2011) GDWM	1.41	0.62	0.19	0.07	0.00	5.03	19.75	0.00	0.96	0.00
Proposed DWT Technique	**0.00**	**0**.00	**0.00**	**0.00**	**0**.00	**2.73**	**14.06**	**0.00**	**0.00**	**0.00**
Host Image Barbara										
Nezhadarya *et al.* (2011) GDWM	1.69	0.16	0.05	0.00	0.00	1.10	8.14	0.00	0.13	0.00
Proposed DWT Technique	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**2.73**	**0**.00	**0**.00	**0**.00
Host Image Lena										
Nezhadarya *et al.* (2011) GDWM	1.65	0.41	0.22	0.10	0.00	0.00	7.10	0.00	0.17	0.00
Proposed DWT Technique	3.51	0.78	**0.00**	**0.00**	**0.00**	0.39	**0.78**	**0.00**	**0.00**	**0.00**

4.4.3 Comparison with Other Watermarking Schemes

In Table 4.4, proposed technique has been compared with a very latest technique presented by Tsougenis *et al.* (2013). This technique shows very good results against JPEG compression attack. But proposed technique shows better results against median filter, random noise and scaling attacks. In Table 4.5, proposed technique has been compared with a QIM based technique presented by Nezhadarya *et al.* (2011). In this comparison too, the proposed watermarking scheme better robustness results by producing lesser BER(%) of the extracted watermark for the applied attacks..

4.5 CHAPTER SUMMARY

In this chapter a thorough analysis of the dynamic strength factor has been presented in context of a DWT based watermarking technique by taking different adjusting parameter values of the dynamic strength factor. The watermarked image of any desired PSNR level can be obtained by taking an appropriate value of this adjusting parameter. It has been shown that by having a high PSNR of watermarked image (associated with high imperceptibility of watermark), the BER (%) of recovered watermark increases (associated with decreasing robustness of watermark). Very high security of the side information has been ensured against the probable unauthentic interception. Encoding method of the side information has also been explained. Proposed DWT based technique using 8×8 block segmentation has also been compared with well known watermarking techniques of literature and has shown better performance.

In the next chapter a hybrid watermarking technique using DWT, SVD and DCT has been presented.

CHAPTER 5

DWT-SVD-DCT BASED HYBRID WATERMARKING TECHNIQUE

IN the present chapter a novel hybrid watermarking technique based on DWT, SVD and DCT has been presented. Like the earlier DWT based technique this is also a semi-blind technique in which side information generated during watermark embedding is used in the extraction of watermark. Dynamic strength factor has also been used in this technique. This technique has been compared with earlier proposed DWT based watermarking technique and other well accepted watermarking techniques from literature.

5.1 INTRODUCTION

Hybrid watermarking techniques use more than one transforms in the watermarking process. These techniques have been discussed in section 2.6 (Falkowski, 2008; Run *et al.*, 2012; Agarwal *et al.*, 2013 etc.). The proposed scheme is a hybrid image-adaptive robust watermarking scheme which uses DWT, SVD and DCT together. The advantage of using DWT is that it has very good re-construction and multi-resolution property. The benefit of using the SVD is that singular values obtained after applying SVD are hardly affected by any kind of watermarking attack. DCT has been used along with DWT and SVD, which is real and orthogonal and has got very good energy compaction efficiency. Detailed discussion about these transforms has been provided in Section 2.2.

5.2 PROPOSED WATERMARKING SCHEME

In this section watermark embedding and detection of the presented hybrid watermarking technique has been discussed.

5.2.1 Watermark Embedding

The host image is segmented into 8×8 blocks of image pixels as shown in the embedding block diagram in Figure. 5.1. Entropies of all the blocks are calculated as shown by Gonzaelez *et al.*

(2009). High entropy blocks are selected for watermark embedding as they carry the most crucial information about the host image. DWT is applied on these selected high entropy blocks. Daubechies wavelet with single level of decomposition is used here. Low frequency approximation coefficients, got after application of DWT are subjected to SVD. On the obtained singular values DCT is applied. So, for every high entropy block, there is a corresponding matrix of DCT coefficients. The number of blocks used for watermark embedding is equal to the number of bits in the watermark. The matrix of DCT coefficients is modified by using the spread spectrum method (Cox *et al.*, 1997), for embedding a single bit '0' or '1' of the watermark.

For embedding '1':

$$C_{emb} = C(1 + DSF) \tag{5.1}$$

For embedding '0':

$$C_{emb} = C(1 - DSF) \tag{5.2}$$

where, C- DCT coefficients matrix before embedding the watermark bit.

C_{emb}- DCT coefficients matrix after embedding the watermark bit.

DSF- Dynamic or varying strength factor derived from standard deviations of the DCT coefficients.

The discussion about *DSF* is provided in section 5.2.3. After embedding the watermark in DCT coefficients matrix, inverse DCT is applied. As a result the modified singular values matrix 'S' is obtained (as in Section 2.2.3). The modified singular values matrix 'S' is multiplied by the original unitary matrices 'U' and 'V' and the modified approximation coefficients matrix of DWT is attained. Now the inverse-DWT is applied and as a result the modified high entropy block is obtained. This process is repeated until all watermark bits are embedded in the selected high entropy blocks. Now these all modified high entropy blocks are combined with other blocks of the image and the resultant watermarked image is achieved.

As the presented watermarking scheme is a semi-blind scheme, therefore some additional side information is sent along with the watermarked image which helps in the extraction of watermark at the receiving end. The side information which is sent in this scheme consists of

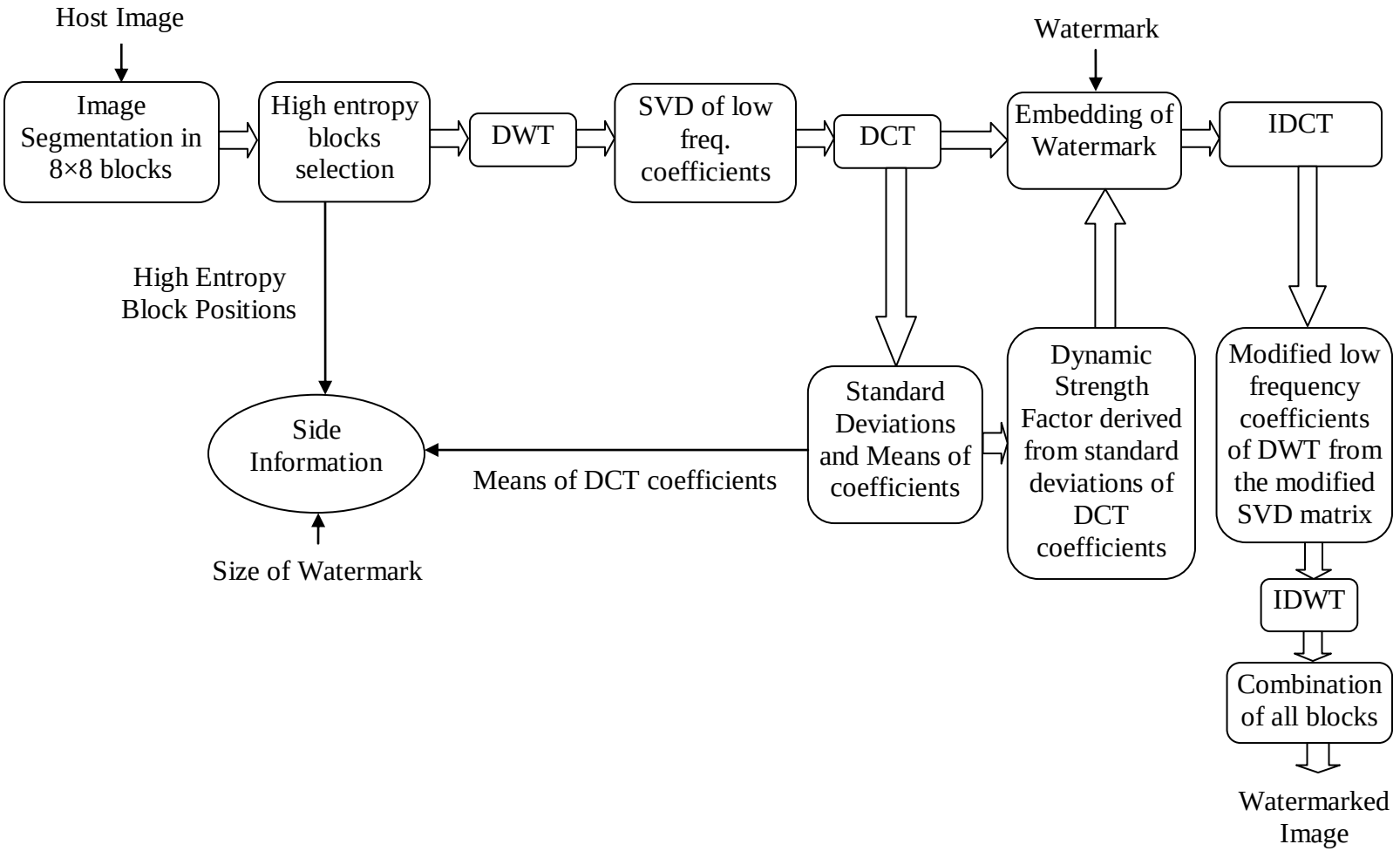


Figure 5.1 Embedding of watermark in the proposed watermarking scheme

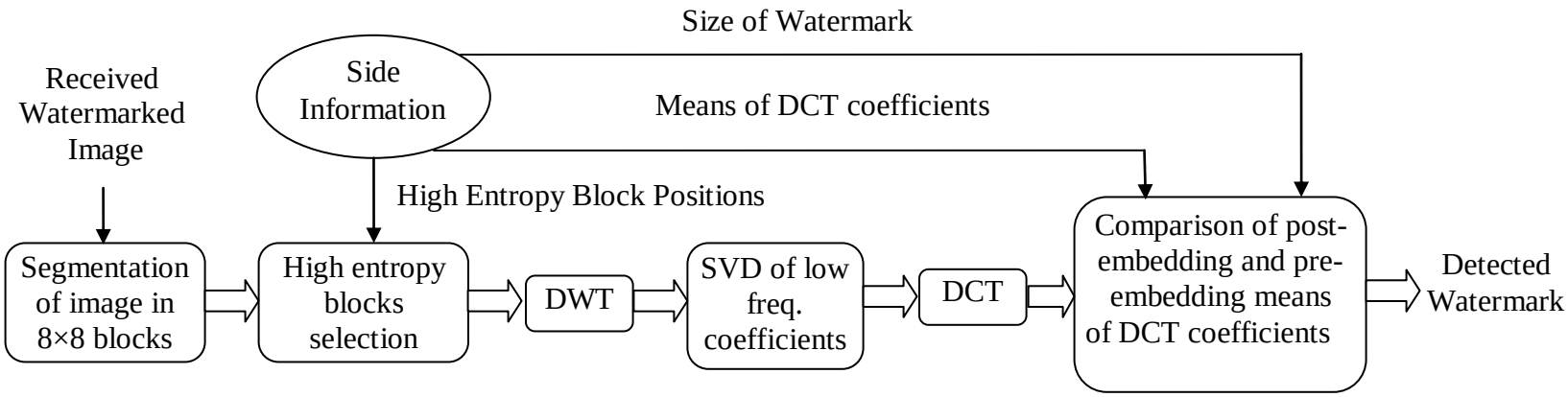


Figure 5.2 Extraction of watermark in the proposed watermarking scheme

high entropy block positions, means of the DCT coefficients' matrices and size of the watermark. Security to the side information is provided in the manner as explained in the section 4.3.

5.2.2 Watermark Extraction

Block diagram of watermark extraction is shown in Figure 5.2. In the extraction process, the received watermarked image is segmented into 8×8 non-overlapping blocks. Then using the side information the high entropy blocks of the watermarked image are recognized. After that DWT is applied on these blocks and the low frequency approximation coefficients' matrices are obtained. Then by applying SVD on approximation coefficients of DWT, singular values' matrices are attained. DCT is applied on the singular values and the corresponding DCT coefficients' matrices are got. The means of these DCT coefficients matrices are compared by the corresponding means of the un-watermarked DCT coefficients matrices present in the side information. By making this comparison, the presence of bit '1' or '0' of the binary watermark can be easily identified.

Assuming that C_mean_{curr} and C_mean_{prev} represent the current and previous means of DCT coefficients.

If,

$C\_mean_{curr} > C\_mean_{prev}$ - Bit '1' is detected.

and if

$C\_mean_{curr} < C\_mean_{prev}$ - Bit '0' is detected.

In this manner all the embedded watermark bits are obtained. By arranging these watermark bits according to the size of the watermark, present in the side information, watermark is retrieved back. Figure 5.3 shows six host images, their watermarked images with PSNR 45 dB and extracted watermarks.

5.2.3 Image-Adaptive Watermarking Using Dynamic Strength Factor

Strength factor determines the amount of variation which is made into the transform coefficient's value when a bit '1' or '0' of the binary watermark is embedded. A dynamic strength factor has been used in the presented technique. Standard deviations of the DCT coefficient matrices

obtained from the selected 8×8 blocks are used in the formation of strength factor. The expression of the heuristically derived strength factor is given as below:

$$DSF = \frac{Standard\ deviation\ of\ any\ DCT\ coefficient\ matrix}{(Maximum\ standard\ deviation\ among\ all\ the\ DCT\ coefficient\ matrices)^{\rho}} \quad (5.3)$$

where, ρ - Adjusting parameter of the strength factor

Robustness of the scheme can be expressed in terms of the BER (%). This is the percentage of error which gets into the extracted watermark as compared to the original watermark after a particular watermarking attack. A good watermarking scheme should have the imperceptibility and robustness both. But these two properties are opposing in nature to each other. When one is increased, other tends to decrease and vice-versa.

Adjusting parameter (ρ) is the power of the denominator part of strength factor expression in (5.3). By changing this parameter different values of the strength factors are obtained. Lower value of the adjusting parameter makes the strength factor higher and watermarking scheme more robust (less BER (%)), but visual quality of the watermarked image (represented by PSNR) becomes very less. Similarly a very high value of the adjusting parameter makes the strength factor lower. As a result, PSNR of the watermarked image becomes high but BER (%) of the extracted watermark becomes high also which is indicative of low robustness of the scheme. Figure 5.4 shows the plots of watermarked image PSNR and recovered watermark BER (%) with the variation of adjusting parameter ρ from for six host images along with watermark *TU*. By using the adjusting parameter quality of the watermarked image can be easily controlled. Table 5.1 shows the adjusting parameter values to make the watermarked image PSNR 45 dB for six host images embedded with three different sized watermarks.

Column 1 Column 2 Column 3

Figure 5.3 Original images (column 1), watermarked Images with PSNR 45 dB (column 2) and recovered watermarks (column 3)

Figure 5.3 Original images (column 1), watermarked Images with PSNR 45 dB (column 2) and recovered watermarks (column 3)

5.3 EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section the proposed DWT-SVD-DCT technique has been first evaluated without applying attacks and then by applying common watermarking attacks.

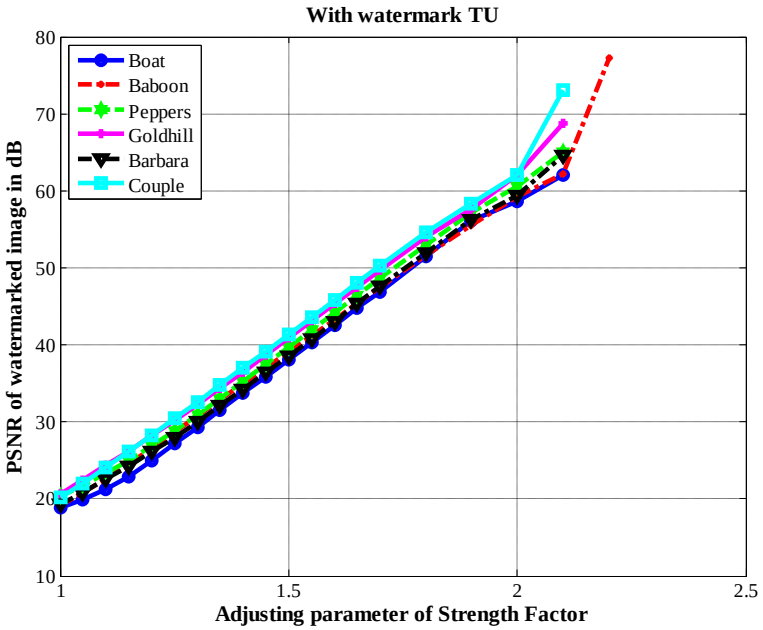
5.3.1 Performance analysis without applying attacks

For evaluating the performance of the proposed watermarking technique, sixteen host images as shown in Appendix-I have been used with three watermarks. In the Figure 5.5 BER (%) of the recovered watermark from these sixteen unattacked watermarked images has been plotted against their corresponding images using proposed DWT-SVD-DCT based hybrid technique and DWT technique of previous chapter. As is clearly evident from the three plots (corresponding to the three watermarks) in the Figure 5.5, that presented hybrid technique produces quite lesser BER (%) for almost all images as compared to the DWT technique. It means that DWT-SVD-DCT technique presented in this chapter is more robust when no attacks are applied on the watermarked image.

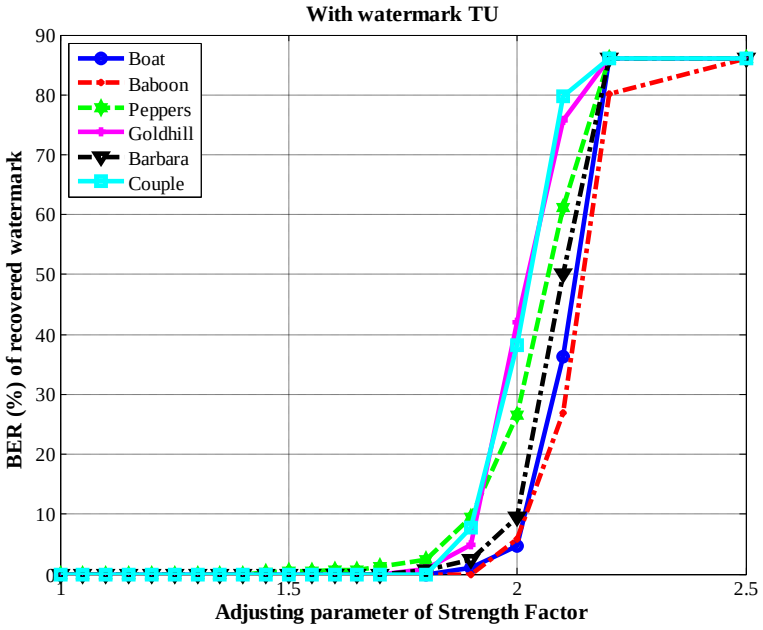
5.3.2 Performance analysis under common attacks

In the Table 5.2 and 5.3 the detailed BER (%) results of scaling, median filter, wiener filter, Gaussian filter, salt and pepper noise and sharpening attacks are shown. These results are for six host images *Boat, Barbara, Peppers, Baboon, Couple* and *Godhill* embedded with *TU* watermark. Figure 5.6 shows the plots of recovered watermark BER (%) from AWGN attacked images and JPEG compression attacked images with various values of AWGN variance and quality factor respectively. In the JPEG compression attack plot, lesser the quality factor higher is the JPEG compression. All the watermarked images used in the attacks are of PSNR value 45 dB.

Tables 5.4 to 5.6 show the comparison between DWT-SVD-DCT technique and DWT technique using the same set of attacks, for the three host images *Boat, Barbara* and *Peppers*. From these two tables it is observed that BER (%) of recovered watermark is lesser for the presented DWT-SVD-DCT based hybrid technique with all three watermarks. Therefore it can be stated that proposed hybrid technique using DWT, SVD and DCT together, is superior to DWT technique of last chapter.

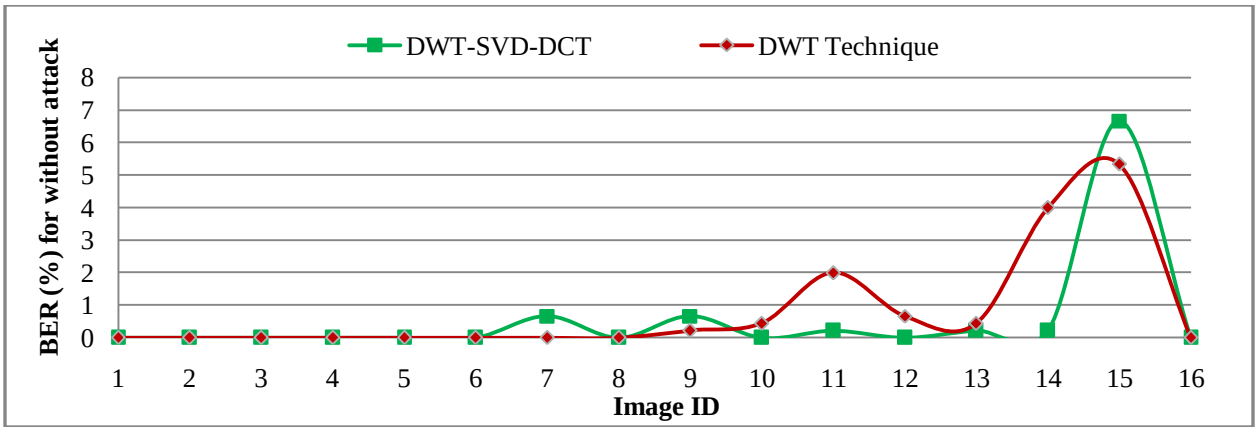


(a)

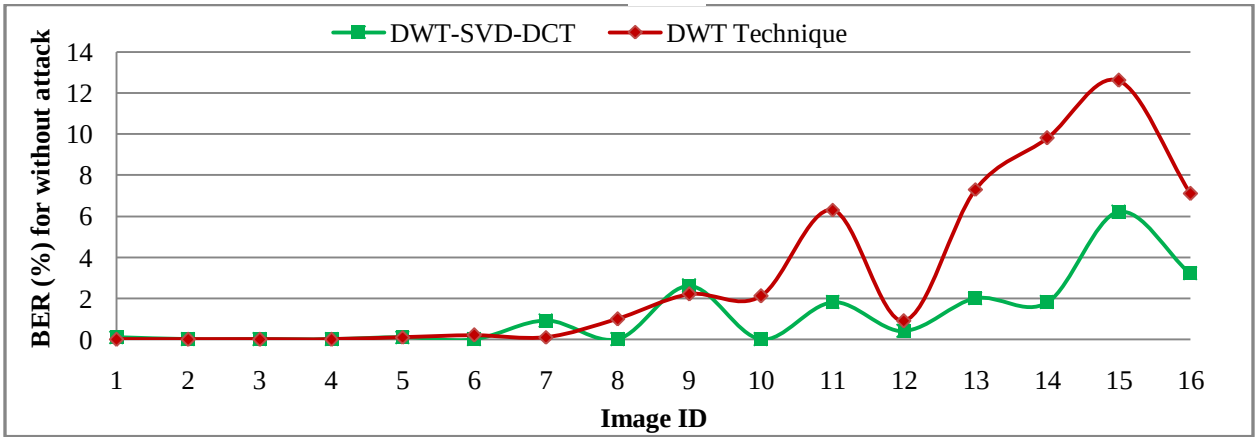


(b)

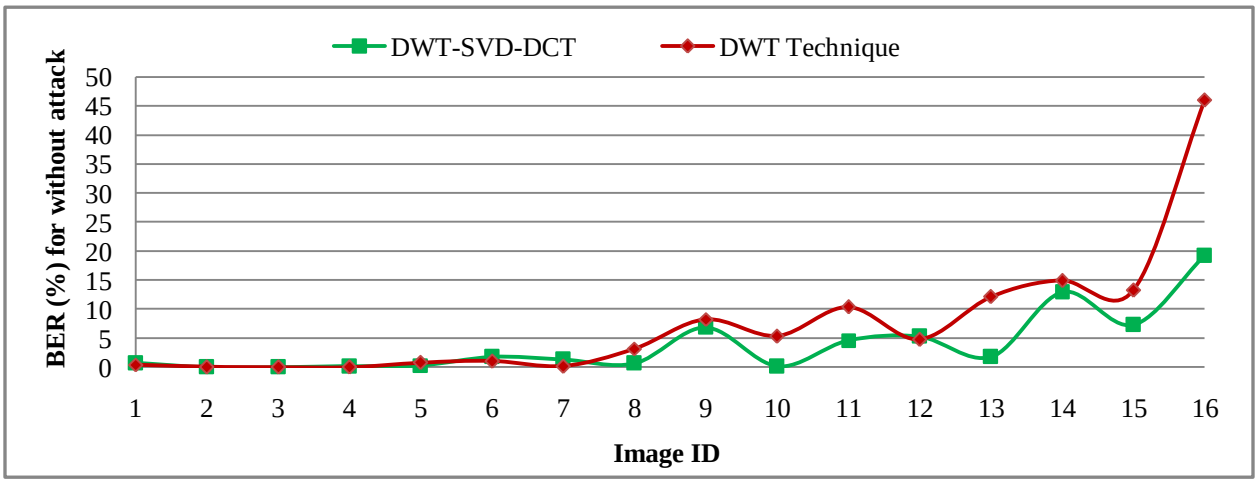
Figure 5.4 Plots of (a) Watermarked image PSNR (dB), (b) Recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively for six different images with watermark *TU*



(a)



(b)



(c)

Figure 5.5 BER (%) plot of recovered watermark without applying any attack on sixteen watermarked images having PSNR as 45 dB using DWT-SVD-DCT hybrid technique and DWT techniques with watermark (a) *TU* (b) *Copyright* (c) *Thapar_Univ*

Table 5.1 Variation of adjusting parameter ρ for making watermarked image PSNR 45 dB with three different watermarks

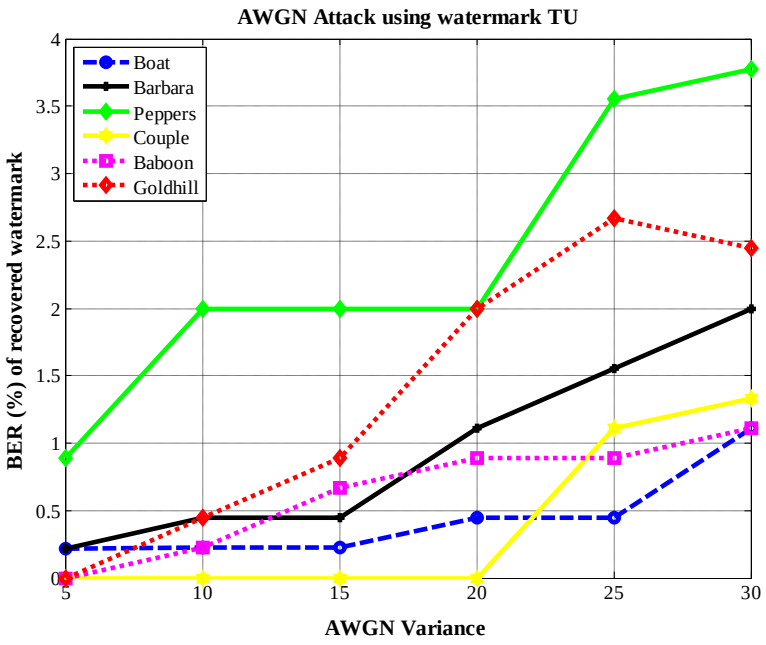
Host Image	Value of adjusting Parameter (ρ) with watermark *TU*	Value of adjusting Parameter (ρ) with watermark *copyright*	Value of adjusting Parameter (ρ) with watermark *Thapar_Univ*
Boat	1.657	1.709	1.740
Barbara	1.643	1.721	1.770
Peppers	1.620	1.693	1.724
Baboon	1.640	1.717	1.746
Couple	1.581	1.683	1.705
Goldhill	1.593	1.633	1.673

Table 5.2 BER (%) of recovered watermark under scaling, median and wiener filter attacks of different types for watermark *TU* and watermarked image PSNR as 45 dB

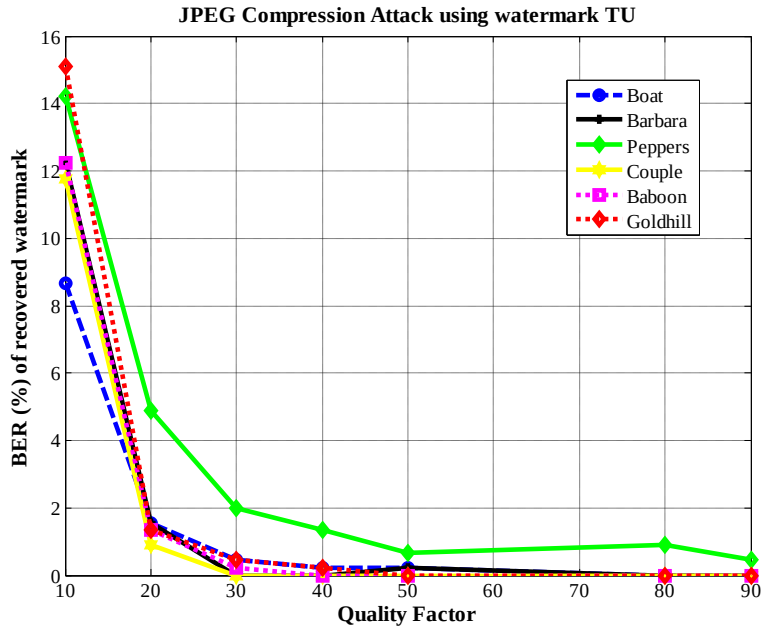
Image	Scaling Level					Median Filter		Wiener Filter	
	0.75	***0.9***	***1.1***	***1.5***	***2***	***3 × 3***	***5 × 5***	***3 × 3***	***5 × 5***
Boat	0.22	1.33	12.00	0.00	0.00	2.44	10.22	0.22	0.89
Barbara	0.00	0.22	4.44	0.00	0.00	1.33	15.56	0.22	3.11
Peppers	1.33	3.33	9.11	0.44	0.44	2.00	9.78	1.11	2.67
Baboon	0.00	0.00	1.33	0.00	0.00	22.44	42.00	0.22	4.00
Couple	0.00	0.00	3.33	0.00	0.00	0.44	10.44	0.00	2.89
Goldhill	0.00	0.00	0.00	0.00	0.00	1.33	7.33	0.22	1.33

Table 5.3 Comparison of BER (%) of recovered watermark under Gaussian filter and Sharpening filter attacks for watermark *TU* for watermarked image PSNR as 45 dB

Image	Gaussian Filter		Sharpening	Salt and Pepper Noise				
	3 × 3	***5 × 5***		***p=0.01***	***p=0.02***	***p=0.03***	***p=0.04***	***p=0.05***
Boat	0.44	0.44	5.11	2.00	6.44	10.67	14.22	14.89
Barbara	0.22	0.22	2.89	3.56	8.67	14.22	17.78	21.78
Peppers	0.44	0.44	5.78	3.11	6.00	11.56	15.33	18.44
Baboon	0.22	9.44	9.11	3.78	4.89	8.44	11.11	11.11
Couple	0.00	0.00	4.22	2.22	4.22	7.33	9.11	11.56
Goldhill	0.00	0.00	2.22	3.33	5.78	9.56	11.11	14.22



(a)



(b)

Figure 5.6 Plots of (a) AWGN variance attack with various values of AWGN variance and (b) JPEG compression attack with various quality factors with watermark *TU* embedded in six host images

Table 5.4 Performance comparison between DWT-SVD-DCT hybrid technique and DWT technique in terms of recovered watermark BER (%) under various attacks with three different sized watermarks and host image *Boat*, for watermarked image PSNR as 45 dB

Technique / Attack	DWT-SVD-DCT Technique			DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	8.67	24.10	29.37	15.33	24.40	30.44
AWGN (σ^2=20)	0.44	2.00	4.87	3.78	3.70	8.06
Median Filter (3×3)	2.44	7.90	17.69	3.78	7.10	14.19
Salt and Pepper (p=0.01)	2.00	6.30	12.37	10.22	12.50	16.56
Scaling (1.5)	0.00	0.10	3.69	0.22	0.70	2.94
Sharpening	5.11	7.00	13.12	12.00	21.20	24.00
Wiener Filter (3×3)	0.22	0.90	7.00	0.67	1.80	5.44
Gaussian Filter (3×3)	0.44	1.70	7.87	1.56	1.50	3.88

Table 5.5 Performance comparison between DWT-SVD-DCT hybrid technique and DWT technique in terms of recovered watermark BER (%) under various attacks with three different sized watermarks and host image *Barbara* for watermarked image PSNR as 45 dB

Technique / Attack	DWT-SVD-DCT Technique			DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	12.22	23.10	30.25	14.89	25.60	31.50
AWGN (σ^2=20)	1.11	1.40	3.75	1.78	4.40	7.31
Median Filter (3×3)	1.33	5.00	7.94	0.89	1.80	4.19
Salt and Pepper (p=0.01)	3.55	9.60	14.81	8.67	13.70	15.75
Scaling (1.5)	0.00	0.00	0.12	0.00	0.00	0.06
Sharpening	2.89	8.00	12.87	9.11	18.10	24.19
Wiener Filter (3×3)	0.22	1.20	1.44	0.67	0.90	1.06
Gaussian Filter (3×3)	0.22	1.90	3.25	2.00	3.30	3.38

Table 5.6 Performance comparison between DWT-SVD-DCT hybrid technique and DWT technique in terms of recovered watermark BER (%) under various attacks with three different sized watermarks and host image *Peppers* for watermarked image PSNR as 45 dB

Technique / Attack	DWT-SVD-DCT Technique			DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	14.22	22.70	29.25	18.67	26.80	32.75
AWGN (σ^2=20)	2.00	10.20	6.37	4.22	5.80	8.63
Median Filter (3×3)	2.00	4.70	10.06	0.67	3.30	8.44
Salt and Pepper (p=0.01)	3.11	9.50	13.12	7.11	14.20	19.12
Scaling (1.5)	0.44	1.70	3.75	0.00	0.90	3.69
Sharpening	5.78	8.30	10.62	7.78	13.90	17.88
Wiener Filter (3×3)	1.11	1.80	7.00	0.89	1.60	6.50
Gaussian Filter (3×3)	0.44	2.20	6.37	1.56	1.70	5.56

5.3.3 Comparison with other watermarking schemes

In this section comparison of the proposed DWT-SVD-DCT technique is done with two established watermarking techniques of literature. In the Table 5.7 to Table 5.9 comparison with Akhaee *et al.* (2009) has been made. In this comparison watermark of length 128 bits has been used with four images- *Baboon*, *Barbara*, *Bridge* and *Couple* of size 512×512. Proposed hybrid scheme shows much better robustness against scaling and AWGN attacks. In Table 5.10 and Table 5.11 comparison with Tsougenis *et al.* (2013) has been made. In this comparison watermark of 100 bits has been used with images *Lena* and *Peppers* of size 256×256. DWT-SVD-DCT based hybrid scheme shows better robustness results for median filter, random noise and scaling attacks.

In all these tables wherever the results of proposed DWT-SVD-DCT based hybrid technique are better, bold font has been used to highlight them. From these tables it can be said that proposed hybrid technique shows better robustness against most of the attacks

Table 5.7 Recovered watermark BER (%) comparison between proposed watermarking scheme and Akhaee *et al.* (2009) under scaling attack of different levels with watermark length of 128 bits and host image size 512×512 for watermarked image PSNR as 45 dB

Akhaee *et al.* (2009) watermarking Technique (with block size 16 and watermark length 128 bits)						**Proposed DWT-SVD-DCT Hybrid Technique**				
Host	Scaling Level					Scaling Level				
Image	***0.75***	***0.9***	***1.1***	***1.5***	***2***	***0.75***	***0.9***	***1.1***	***1.5***	***2***
Baboon	10.39	1.17	0.00	0.00	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Barbara	31.02	0.31	0.00	0.00	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Bridge	7.85	3.13	0.00	0.00	0.00	**0.00**	**0.00**	2.34	**0.00**	**0.00**
Couple	13.28	5.47	0.00	0.00	0.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

Table 5.8 Recovered watermark BER (%) comparison between proposed watermarking scheme and Akhaee *et al.* (2009) under Salt and Pepper noise attack with watermark length of 128 bits and host image size 512×512 for watermarked image PSNR as 45 dB

Akhaee *et al.* (2009) watermarking Technique (with block size 16 and watermark length 128 bits)						**Proposed DWT-SVD-DCT Hybrid Technique**				
Host	Salt and Pepper Noise Percentage					Salt and Pepper Noise Percentage				
Image	***1%***	***2%***	***3%***	***4%***	***5%***	***1%***	***2%***	***3%***	***4%***	***5%***
Baboon	0.63	0.31	0.63	1.56	2.89	**0.00**	0.78	0.78	1.56	**1.56**
Barbara	0.00	0.04	0.35	0.94	1.48	0.78	2.34	3.90	4.68	8.59
Bridge	0.43	1.29	2.50	4.92	8.32	0.78	1.56	**0.00**	**3.12**	**2.34**
Couple	0.59	0.98	3.05	5.20	8.71	**0.00**	0.78	**0.78**	**2.34**	**3.12**

Table 5.9 Recovered watermark BER (%) comparison between proposed watermarking scheme and Akhaee *et al.* (2009) under JPEG compression and AWGN noise attacks with watermark length of 128 bits and host image size 512×512 for watermarked image PSNR as 45 dB

Akhaee *et al.* (2009) watermarking Technique (with block size 16 and watermark length 128 bits)				**Proposed DWT-SVD-DCT Hybrid Technique**		
Host	AWGN attack		JPEG Comp.	AWGN attack		JPEG Comp.
Image	***σ^2=25***	***σ^2=30***	***10%***	***σ^2=25***	***σ^2=30***	***10%***
Baboon	0.50	1.50	7.30	**0.00**	**0.00**	**0.00**
Barbara	0.50	0.95	3.70	**0.00**	**0.00**	**1,56**
Bridge	2.30	5.00	8.10	**0.00**	**0.00**	**2.34**
Couple	2.30	6.00	7.00	**0.00**	**0.00**	**0.00**

Table 5.10 Recovered watermark BER (%) comparison between proposed watermarking scheme and Tsougenis *et al.* (2013) under JPEG compression and median filter attacks with watermark length of 100 bits, host image size 256×256 and watermarked image PSNR 45 dB

Attack	**JPEG Compression**				**Median Filter**	
Technique	*20*	*40*	*60*	*80*	*6×6*	*8×8*
Host Image Lena						
Tsougenis *et al.* (2013) PCET	0.01	0.00	0.00	0.00	0.46	0.54
Prop. DWT-SVD-DCT Technique	0.07	0.02	0.02	**0.00**	**0.32**	**0.34**
Host Image Peppers						
Tsougenis *et al.* (2013) PCET	0.02	0.00	0.00	0.00	0.31	0.45
Prop. DWT-SVD-DCT Technique	0.03	**0.00**	**0.00**	**0.00**	**0.30**	**0.34**

Table 5.11 Recovered watermark BER (%) comparison between proposed watermarking scheme and Tsougenis *et al.* (2013) under random noise and scaling attacks with watermark length of 100 bits, host image size 256×256 and watermarked image PSNR 45 dB

Attack	**Random Noise (%)**					**Scaling**					
Technique	*1*	*2*	*3*	*4*	*5*	*0.5*	*0.7*	*0.9*	*1.1*	*1.3*	*1.5*
Host Image Lena											
Tsougenis *et al.* (2013) PCET	0.00	0.01	0.04	0.22	0.38	0.05	0.03	0.04	0.08	0.08	0.12
Prop. DWT-SVD-DCT Technique	0.01	0.01	**0.01**	**0.01**	**0.01**	**0.01**	0.18	0.15	0.08	**0.03**	**0.00**
Host Image Peppers											
Tsougenis *et al.* (2013) PCET	0.00	0.03	0.17	0.28	0.48	0.13	0.05	0.08	0.17	0.17	0.20
Prop. DWT-SVD-DCT Technique	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.01**	0.14	0.09	**0.07**	**0.01**	**0.00**

5.4 CHAPTER SUMMARY

In this chapter a semi-blind hybrid watermarking technique has been introduced. This technique uses DWT, SVD and DCT together. The advantage of using of using this hybrid technique is that lesser distortion is observed in the recovered watermark obtained from both the attacked and unattacked watermarked images, in comparison to the DWT based watermarking technique results in the last chapter. The presented watermarking technique also shows better robustness results in comparison to the other two existing watermarking techniques of literature.

In the next chapter another hybrid watermarking technique is proposed which uses DWT, SVD and WHT together.

CHAPTER 6

DWT-SVD-WHT BASED HYBRID WATERMARKING TECHNIQUE

THIS chapter presents the hybridization of DWT, SVD and WHT for the development of a semi-blind robust watermarking scheme. Here three versions of the proposed technique have been used having their dynamic strength factors derived from three local properties of the image. Apart from the standard deviation, which has been used in the techniques proposed in previous chapters, two more local properties used in this technique are mean and entropy.

6.1 INTRODUCTION

A lot of hybrid watermarking techniques have been proposed in the available literature as discussed in the section 2.6. DWT and SVD have been used together in many techniques (Lai and Tsai, 2010; Rastegar *et al.*, 2011; Tsai *et al.*, 2012; Ali and Ahn, 2014). But no watermarking technique could be found in the available literature which has used DWT and SVD along with WHT. This unique combination of transforms has been employed in this chapter. Use of SVD and WHT along with DWT helps to increase the robustness of the watermarking scheme. A big advantage of using the SVD is that singular values obtained after applying SVD are not much affected by any kind of watermarking attack. Also, the benefit of using WHT is that it shows better performance in high noise conditions as compared to other transforms.

6.2 PROPOSED WATERMARKING SCHEME

In this section watermark embedding and detection of the proposed hybrid technique is explained.

6.2.1 Watermark Embedding

Host image is segmented into 8×8 non-overlapping blocks as shown in the embedding block diagram in Figure 6.1. The high entropy blocks among these are chosen for watermark

embedding. The number of high entropy blocks required for embedding is equal to the number of number of bits in the watermark. These selected blocks are subjected to DWT. Low frequency approximation coefficients obtained after application of DWT are the carriers of most crucial information about the image. SVD is applied on all the matrices containing approximation coefficients. SVD produces a diagonal matrix 'S' of singular unique values (Section 2.2.3). WHT is applied on every singular value matrix 'S'. A single bit '0' or '1' of the binary watermark is embedded in each one of the resultant matrices of WHT coefficients. For embedding the bits of watermark, same kind of multiplicative relation of spread spectrum method (Cox *et al.*, 1997) is used as seen in the previous chapters. Three dynamic strength factors derived from three local properties of the image are used for embedding the watermark.

Dynamic strength factor derived from standard deviations of Walsh-Hadamard coefficients is referred to as 'DSF from Standard Deviations', dynamic strength factor derived from means of Walsh-Hadamard coefficients is referred to as 'DSF from means' and dynamic strength factor derived from entropies of the 8×8 non-overlapping blocks is referred to as 'DSF from entropies' in this chapter.

After embedding of the watermark, inverse WHT is applied. This provides a matrix containing singular values in it. A modified singular values matrix 'S' is made from it by keeping only the diagonal values. By combining the modified 'S' matrix with unitary matrices 'U' and 'V', a modified approximation coefficient matrix of DWT is obtained. Now inverse discrete wavelet transform (IDWT) is applied and the modified high entropy blocks of the image are attained. These blocks are combined with other 8×8 blocks of the image to obtain the watermarked image.

Similar to the previously proposed techniques, this watermarking technique is also semi-blind. Side information required to extract the embedded watermark includes high entropy block positions, size of the watermark and means of Walsh-Hadamard coefficients prior to embedding of the watermark. Side information security is provided in the way as explained in the section 4.3.

6.2.2 Watermark Detection

Block diagram of watermark detection in the proposed watermarking scheme is shown in Figure 6.2. In watermark detection firstly the received image is segmented into 8×8 non-overlapping blocks. Then high entropy blocks embedded with watermark bits are identified using the side

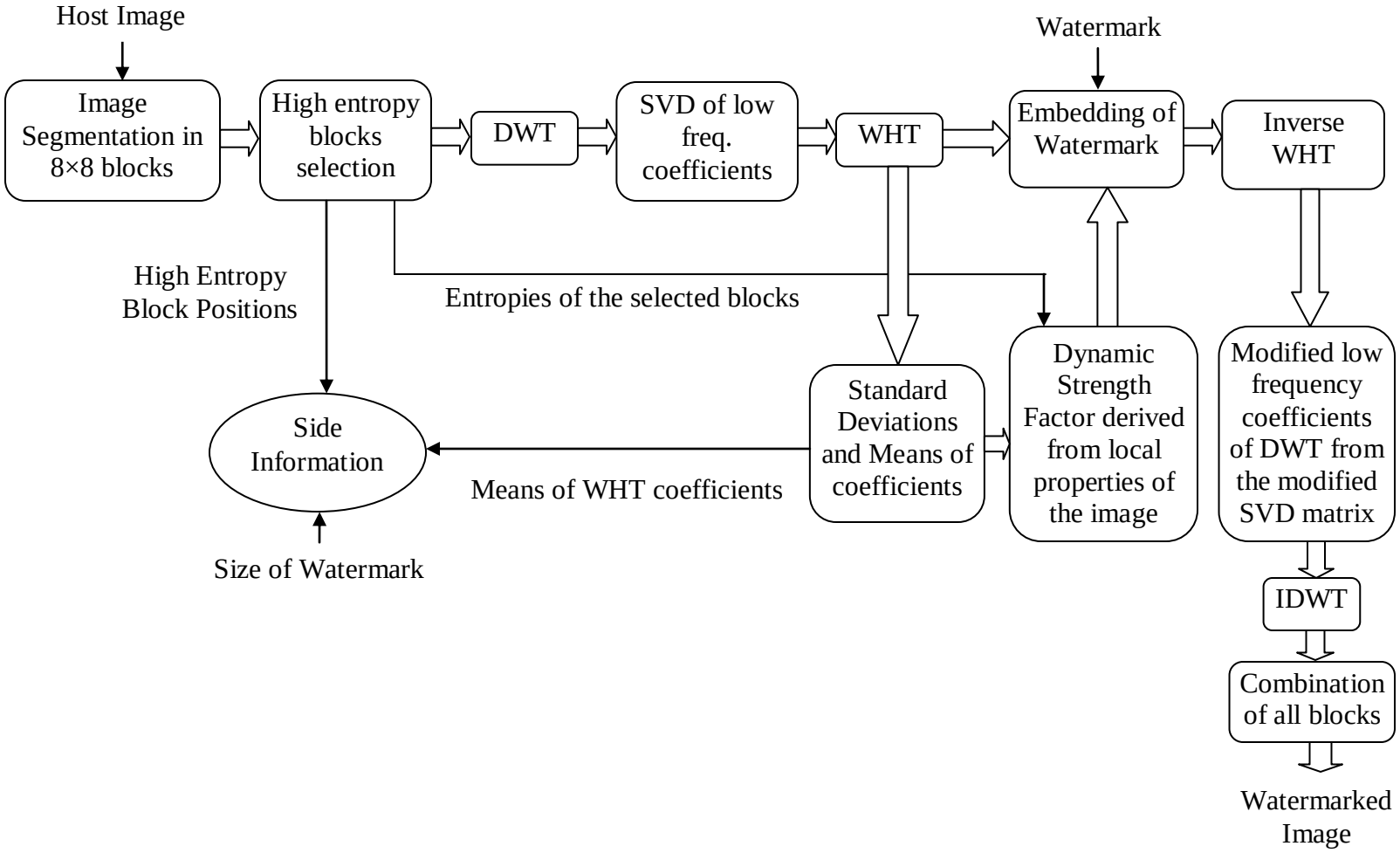


Figure 6.1 Embedding of watermark in the proposed watermarking scheme

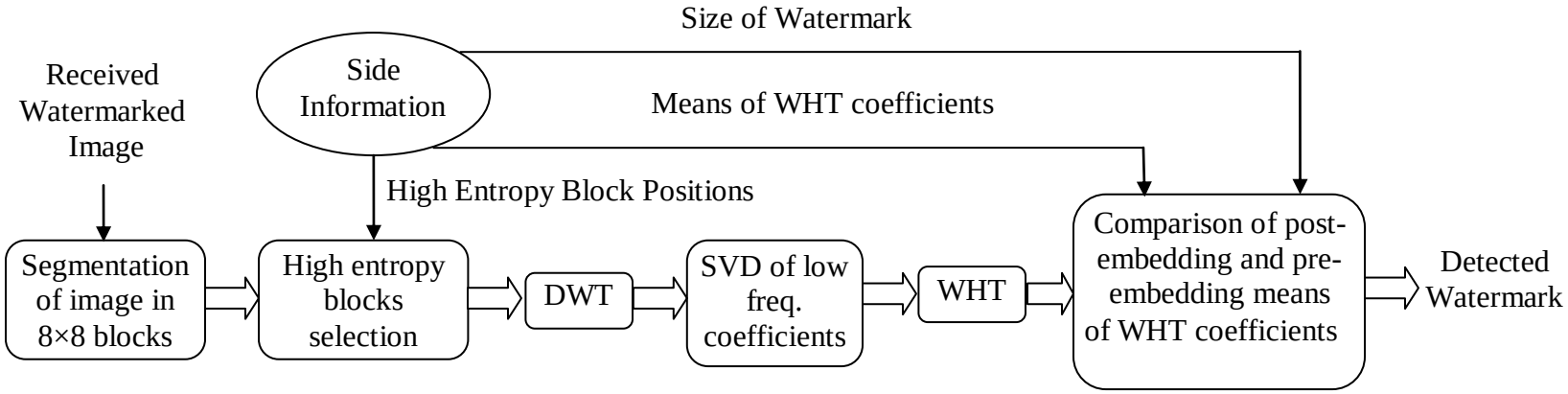


Figure 6.2 Detection of watermark in the proposed watermarking scheme

information. DWT is applied on them to obtain the low frequency approximation coefficients' matrices. SVD is applied on them and resultant singular values' matrices are subjected to WHT subsequently. Now the comparison of means of current Walsh-Hadamard coefficients with means of previous coefficients in the side information is done.

Assuming that H_mean_{curr} and H_mean_{prev} represent the current and previous means of Walsh-Hadamard coefficients.

If,

$H\_mean_{curr} > H\_mean_{prev}$ – Bit '1' is detected.

And if

$H\_mean_{curr} < H\_mean_{prev}$ – Bit '0' is detected.

In this way from the high entropy blocks of the watermarked image, all the watermark bits are obtained.

6.3 DYNAMIC STRENGTH FACTORS FROM LOCAL PROPERTIES OF THE IMAGE

Dynamic strength factor has also been used in the DWT watermarking technique and DWT-SVD-DCT based hybrid watermarking technique proposed in the previous chapters. In these techniques standard deviations of the transforms coefficients have been used to derive the dynamic strength factor. But in the presented DWT-SVD-WHT technique, apart from standard deviation, two more local properties of the image are used to derive two new strength factors. As shown in the block diagram in Figure 6.1, DWT is applied on the selected high entropy 8×8 blocks one by one. As a result, low frequency approximation coefficients matrix is obtained which carries most of the basic information about that specific image block. SVD is applied on this to obtain a matrix of singular values, which in turn is subjected to WHT. Two statistical properties of this transform's coefficients are used for obtaining two types of strength factors.

First strength factor is derived from standard deviations of the WHT coefficients. Standard deviations of the WHT coefficients matrices originated from all the high entropy 8×8 blocks are calculated and the strength factor belonging to one particular block is defined as:

$$DSF\ \ from\ standard\ deviations = \frac{\sigma_i}{(\sigma_{\max})^{\rho}} \qquad (6.1)$$

σ_i - Standard deviation of a WHT coefficients matrix obtained from any one of the 8×8 high entropy blocks

σ_{max} - Maximum standard deviation among all the WHT coefficients matrices

ρ - Adjusting parameter of the strength factor

Second strength factor is derived from means of the WHT coefficients. Means of the WHT coefficients matrices originated from all the high entropy 8×8 blocks are calculated and the strength factor belonging to one particular block is computed as:

$$DSF\ from\ means = \frac{\mu_i}{(\mu_{\max})^{\rho}} \tag{6.2}$$

μ_i - Mean of a Walsh-Hadamard coefficients matrix obtained from any one of the 8×8 high entropy blocks

μ_{max} - Maximum mean among all the Walsh-Hadamard coefficients matrices

ρ - Adjusting parameter of the strength factor

After segmentation of the image in 8×8 non-overlapping blocks, high entropy blocks are selected for watermark embedding. Third strength factor has been derived from the entropies of the selected blocks. Entropies of the selected blocks are calculated as described by Gonzalez *et al.* (2009) and the strength factor is defined as:

$$DSF\ from\ entropies = \frac{\varepsilon_i}{(\varepsilon_{\max})^{\rho}} \tag{6.3}$$

ε_i - Entropy value of any one of the selected 8×8 high entropy blocks

ε_{max} - Maximum entropy among all the selected 8×8 high entropy blocks

ρ - Adjusting parameter of the strength factor

These strength factors derived from three properties of the image imply that three watermarking techniques emerge from the proposed algorithm. Six host images, watermarked images and their detected watermarks are shown in Figures 6.3 to 6.5 for all the three techniques using their different strength factors. PSNR of all the watermarked images have been kept at 45 dB by using an appropriate value of ρ.

Discussion about adjusting parameter of strength factor ρ, has been done in the previous chapters. The effect of changing the strength factor adjusting parameter ρ consisting of the three

dynamic strength factors, on the PSNR of the watermarked image and BER (%) of the extracted watermark is shown in Figure 6.6 with the watermark *TU*.

Column 1 Column 2 Column 3

Figure 6.3 Original image (column 1), watermarked image with PSNR 45 dB (column 2) and recovered watermark (column 3) using dynamic strength factor derived from .standard deviations of the WHT coefficients of the chosen blocks

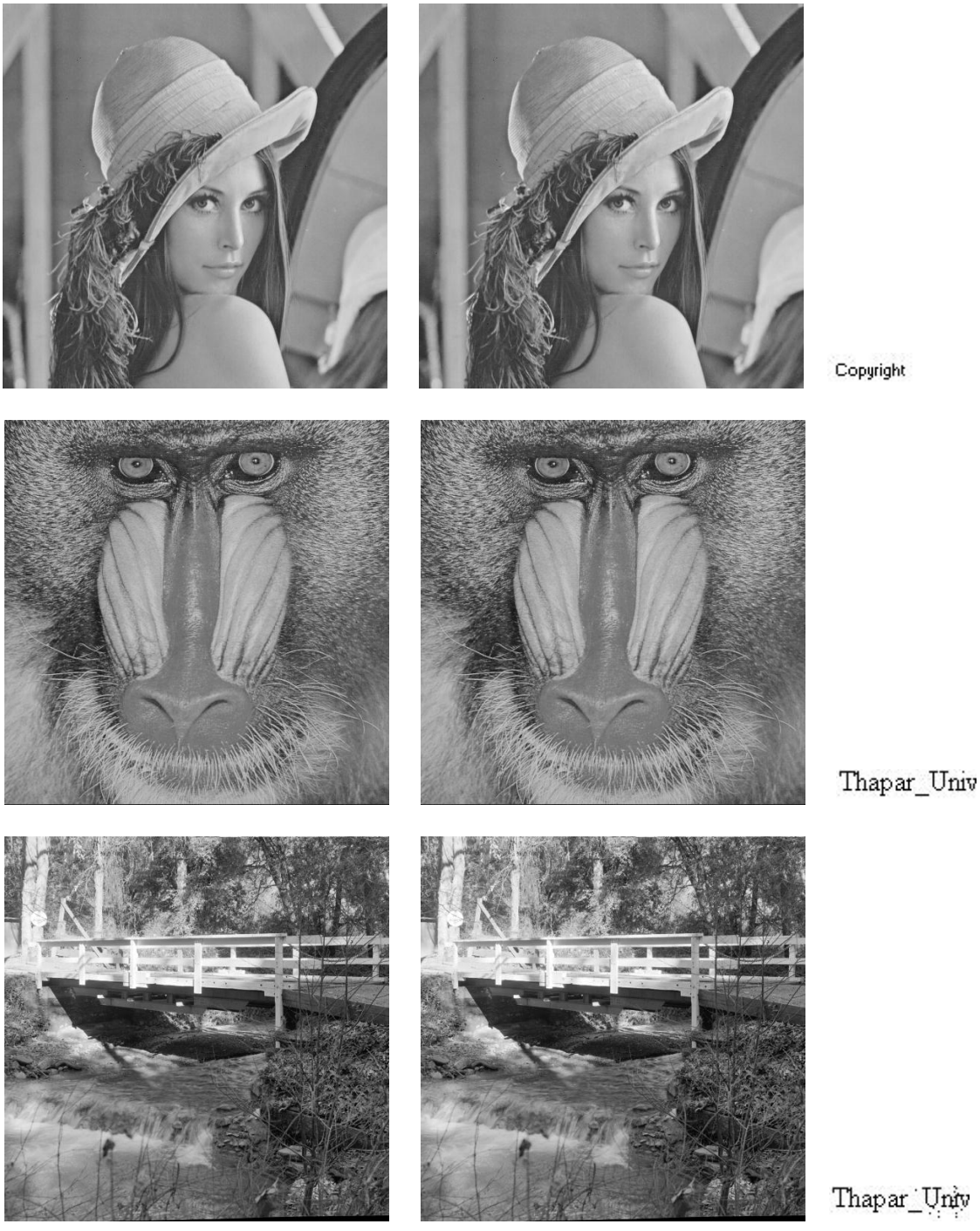


Figure 6.3 Original image (column 1), watermarked image with PSNR 45 dB (column 2) and recovered watermark (column 3) using dynamic strength factor derived from .standard deviations of the WHT coefficients of the chosen blocks

Column 1 Column 2 Column 3

Figure 6.4 Original image (column 1), watermarked Image with PSNR 45 dB (column 2) and recovered watermark (column 3) using dynamic strength factor derived from .means of the WHT coefficients of the chosen blocks

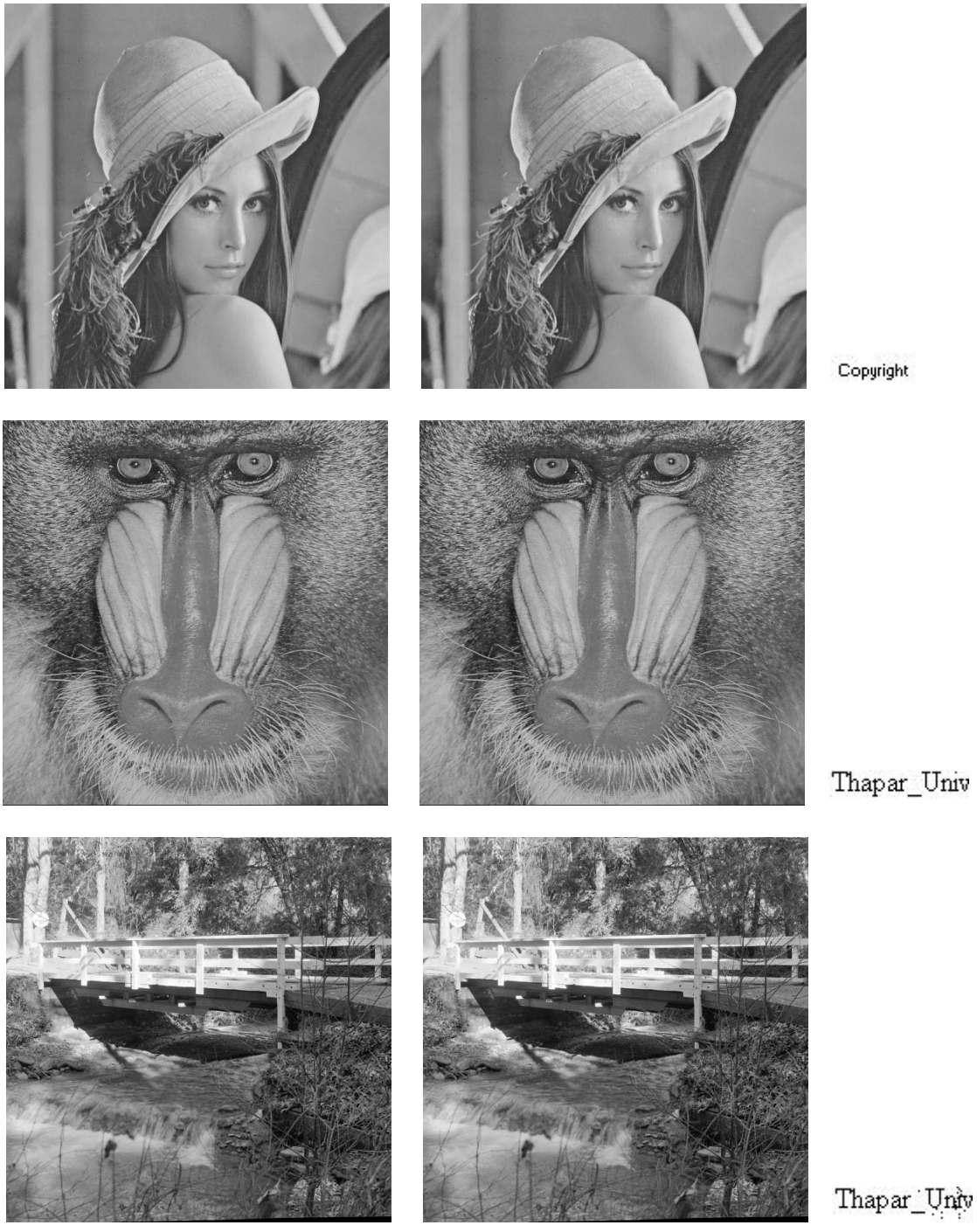


Figure 6.4 Original image (column 1), watermarked Image with PSNR 45 dB (column 2) and recovered watermark (column 3) using dynamic strength factor derived from .means of the WHT coefficients of the chosen blocks

Figure 6.5 Original image (column 1), watermarked Image with PSNR 45 dB (column 2) and recovered watermark (column 3) using dynamic strength factor derived from entropies of the chosen blocks

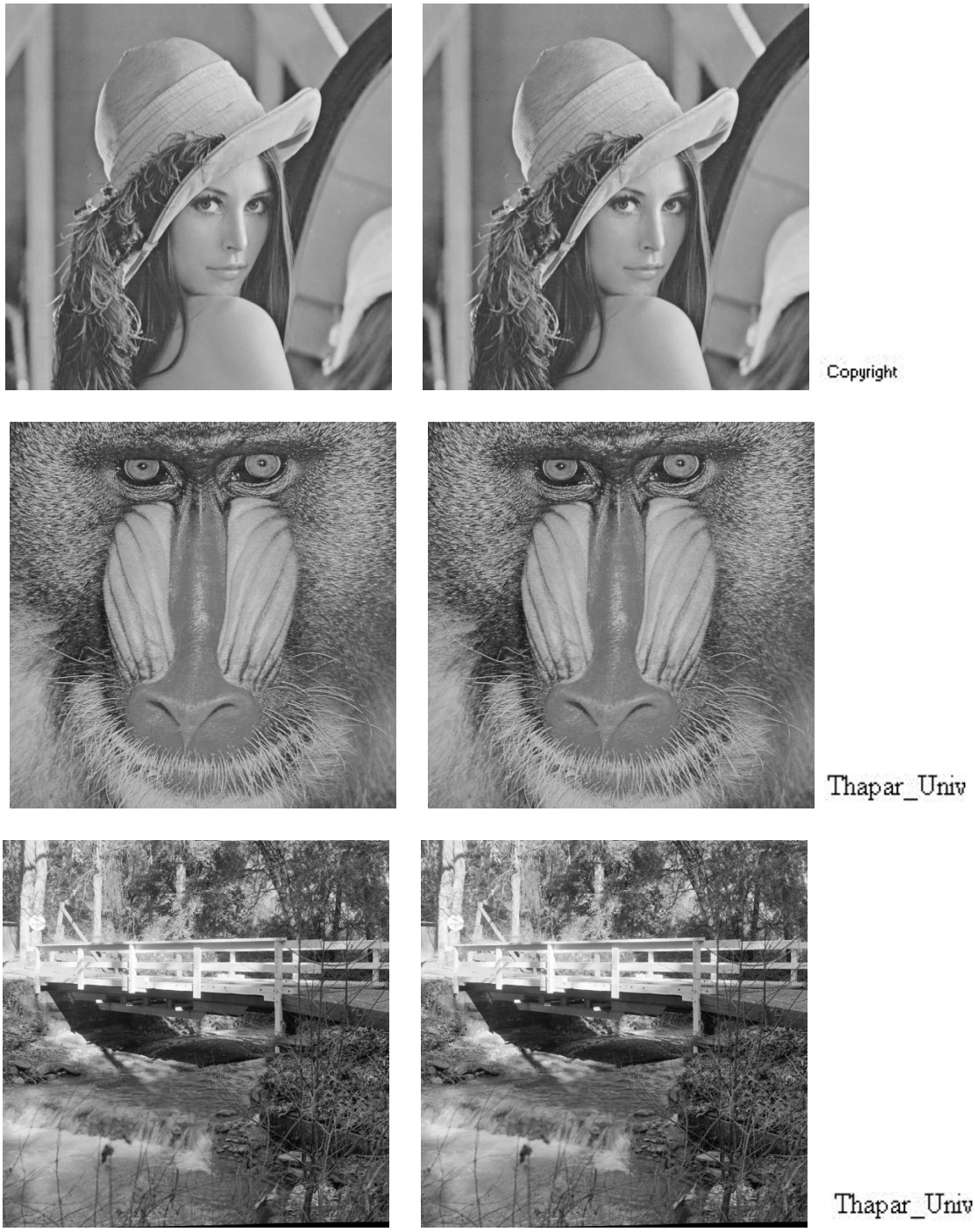
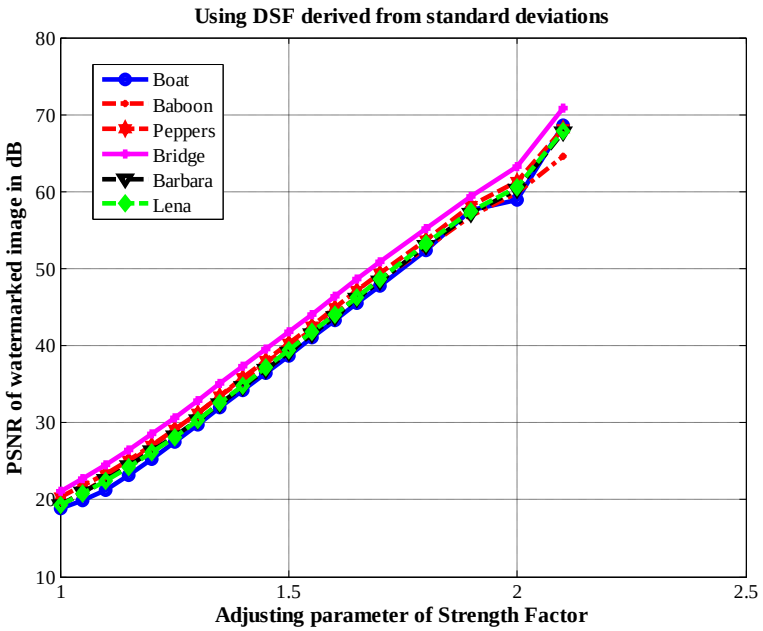
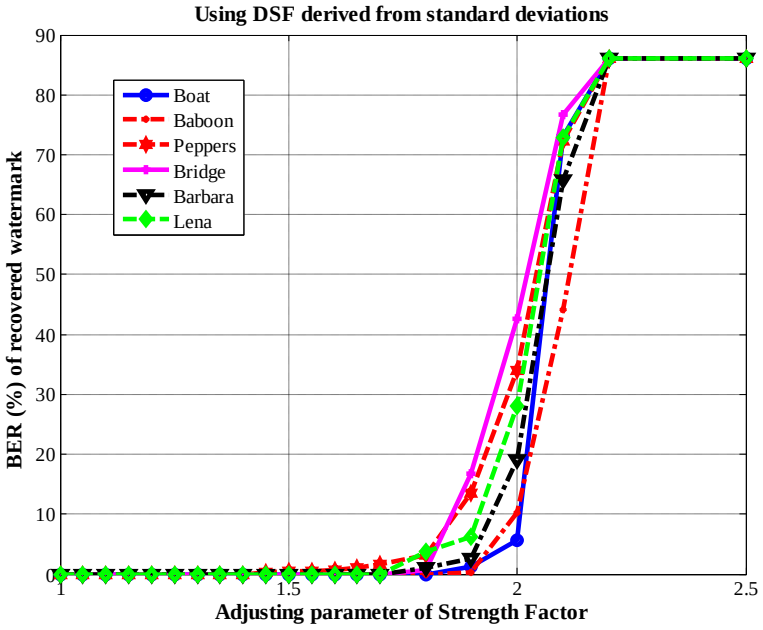


Figure 6.5 Original image (column 1), watermarked Image with PSNR 45 dB (column 2) and recovered watermark (column 3) using dynamic strength factor derived from entropies of the chosen blocks

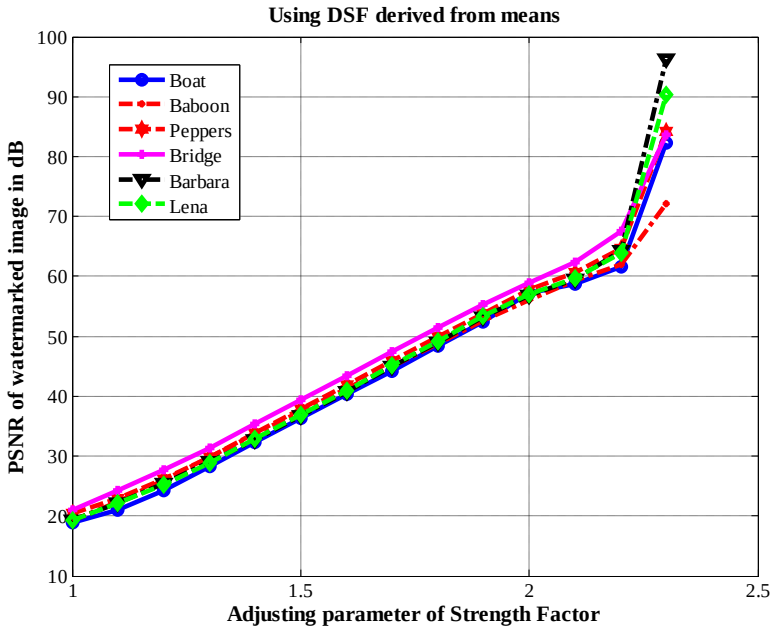


(a)

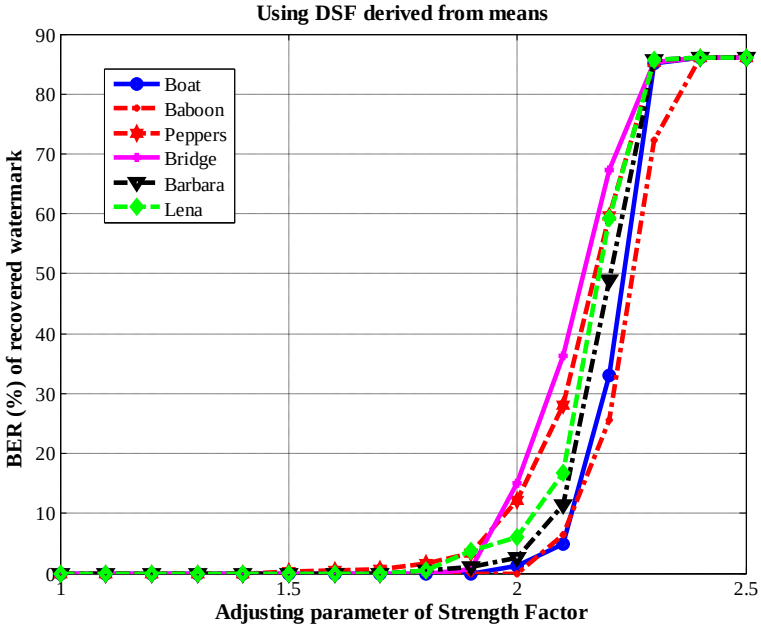


(b)

Figure 6.6 Plots of watermarked image PSNR (dB) and recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively for six different images with watermark *TU*; (a – b) Using DSF from Standard deviations, (c - d) Using DSF from means and (e - f) Using DSF from entropies

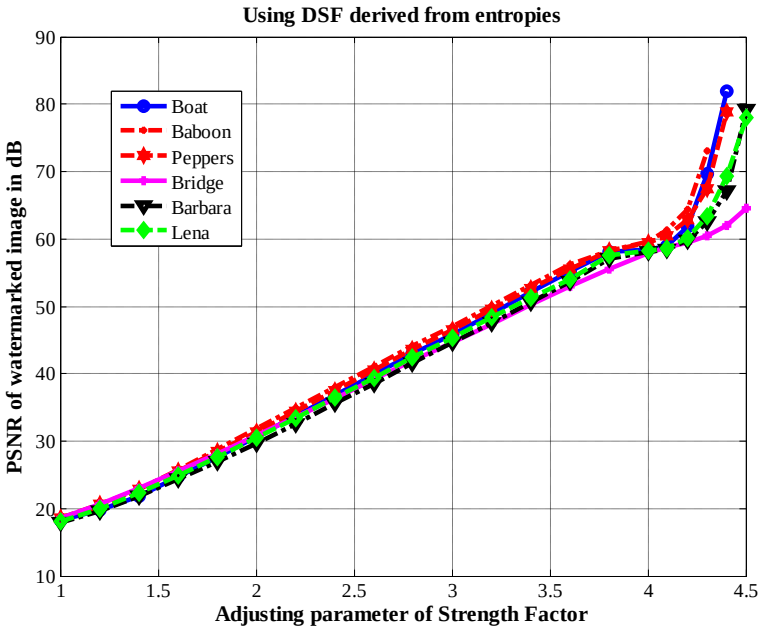


(c)

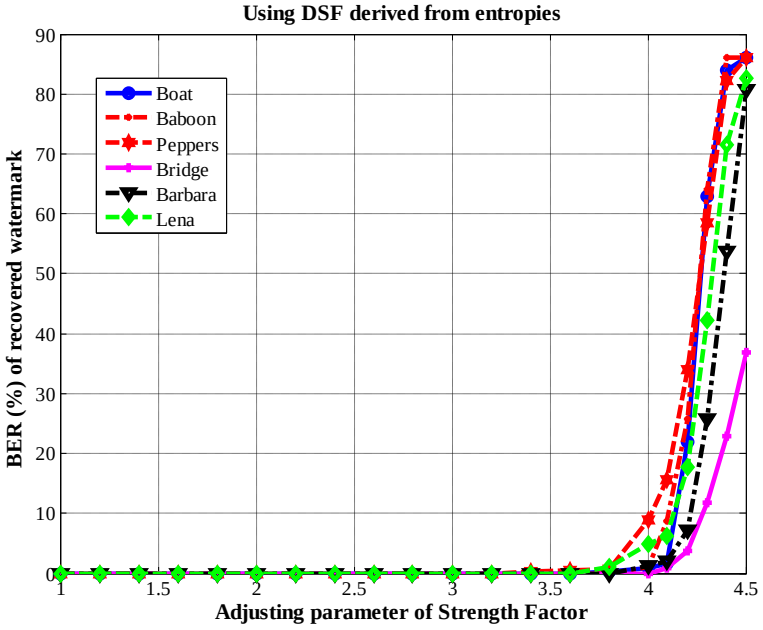


(d)

Figure 6.6 Plots of watermarked image PSNR (dB) and recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively for six different images with watermark *TU*; (a – b) Using DSF from Standard deviations, (c - d) Using DSF from means and (e - f) Using DSF from entropies



(e)



(f)

Figure 6.6 Plots of watermarked image PSNR (dB) and recovered watermark BER (%) with adjusting parameter ρ of strength factor respectively for six different images with watermark *TU*; (a – b) Using DSF from Standard deviations, (c - d) Using DSF from means and (e - f) Using DSF from entropies

6.4 EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section comparison among the three versions of the proposed hybrid technique has been made by applying common watermarking attacks. The version producing best results is then compared with the watermarking techniques proposed in the earlier chapters and two established techniques of literature.

6.4.1 Performance comparison among three versions of DWT-SVD-WHT

Three versions of the presented hybrid technique using three dynamic strength factors derived from standard deviations, means and entropies belonging to the selected 8×8 pixel blocks, have been called as DWT-SVD-WHT (standard deviation), DWT-SVD-WHT (mean) and DWT-SVD-WHT (entropy) respectively. Table 6.1 shows the adjusting parameter values to make the watermarked image PSNR 45 dB for six host images embedded with three different sized watermarks using every version of the proposed DWT-SVD-WHT technique. Common watermarking attacks results have been shown in Tables 6.2 to 6.4 for watermark *TU*.

Table 6.2 compares the BER (%) results of recovered watermarks of these techniques for scaling attack of levels 0.75, 0.9, 1.1, 1.5 and 2. Table 6.3 shows the results for median and wiener filter attacks while Table 6.4 shows the results for Gaussian filter and sharpening attacks. Figure 6.7 shows plot of the BER (%) of recovered watermark against different AWGN noise variances for all the three techniques. Figure 6.8 shows the similar plot for different JPEG compression quality factors.

From the performance Tables 6.2-6.4 and Figures 6.7-6.8, it is evident that two techniques DWT-SVD-WHT (standard deviation) and DWT-SVD-WHT (mean) produce quite similar BER (%) of the recovered watermark for a large number of attacks. Third watermarking technique DWT-SVD-WHT (entropy) gives the best results because for all the common watermarking attacks this technique gives the least BER (%) with all the six host images. For example, when scaling attack of level 0.75 is applied to *Peppers* image, DWT-SVD-WHT (standard deviation) and DWT-SVD-WHT (mean) give BER (%) value of 1.33 while DWT-SVD-WHT (entropy) gives BER (%) value as zero. Also when wiener filter (5×5) attack is applied to the watermarked image *Baboon*, first two techniques give BER (%) as 3.56 and 3.78 while third technique gives BER (%) as 1.56. Similarly on the application of sharpening attack to

watermarked image *Bridge*, first two techniques give BER (%) as 17.11 and 16.89 while third technique gives BER (%) as 11.78. Same is true for AWGN attack and JPEG compression attack shown in Figures 6.7 and 6.8. Thus it can be easily concluded that watermarking technique DWT-SVD-WHT (entropy) having DSF from entropies of the 8×8 blocks is better than the other two techniques DWT-SVD-WHT (standard deviation) and DWT-SVD-WHT (mean). Therefore this technique has been compared with two watermarking techniques DWT technique and DWT-SVD-DCT proposed in the previous chapters.

6.4.2 Comparison of DWT-SVD-WHT (entropy) with DWT technique and DWT-SVD-DCT technique

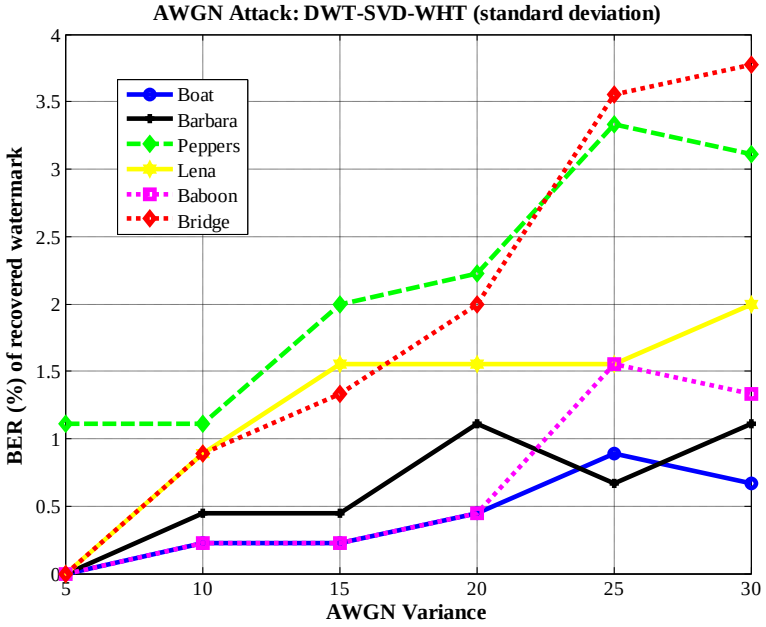
6.4.2.1 Performance comparison without applying attacks

For this comparison all the sixteen host images as shown in Appendix-I have been used. In the Figure 6.9 BER (%) of the recovered watermark from these sixteen unattacked watermarked images has been plotted against their corresponding images using proposed DWT-SVD-WHT (entropy) technique, DWT-SVD-DCT technique and DWT technique. It should be noted that all the watermarked images used in this experiment had PSNR value as 45 dB. As is clearly evident from the three plots (corresponding to the three watermarks) in this figure, that presented DWT-SVD-WHT (entropy) technique produces very less BER (%) for all images as compared to the DWT-SVD-DCT technique and DWT technique. With the watermark *TU*, BER (%) is zero in this technique for all the images. With the watermark *Copyright* BER (%) is zero for the fourteen images and for the remaining two it is 0.1 and 0.3. With the watermark *Thapar_Univ* BER (%) is zero for eleven images and among the remaining five the highest BER (%) is 0.56. Hence it could be said that hybrid technique DWT-SVD-WHT (entropy) is the best technique among the three watermarking techniques proposed in this work when no attack is applied on the watermarked images.

6.4.2.2 Performance comparison after applying attacks

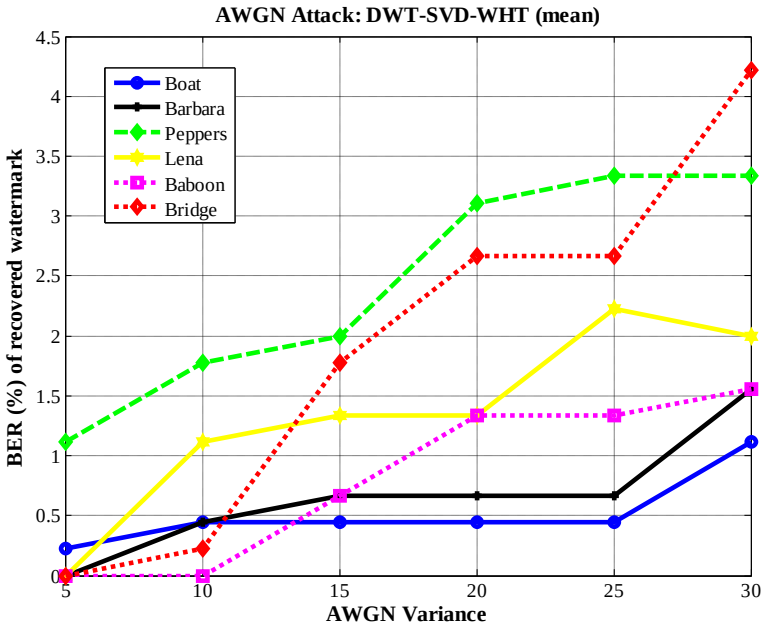
DWT-SVD-WHT (entropy) technique is compared with DWT technique and DWT-SVD-DCT technique in the Tables 6.5-6.7 by applying same set of attacks and using host images *Boat*, *Barbara* and *Peppers*. With all three watermarks DWT-SVD-WHT (entropy) technique having

DSF from entropies produces least BER (%) for all the attacks. For example, when the *Boat* image embedded with watermark *TU* is subjected to JPEG compression attack of quality factor 10%, DWT technique, DWT-SVD-DCT technique and DWT-SVD-WHT (entropy) technique produce BER (%) of recovered watermark 15.33, 8.67 and 6 respectively. Similarly when the *Barbara* image embedded with watermark *Copyright* is attacked by AWGN noise of variance 20, DWT technique, DWT-SVD-DCT technique and DWT-SVD-WHT (entropy) technique produce BER (%) of the recovered watermark 4.4, 1.4 and 0.4 respectively. From these three tables it is completely obvious that DWT-SVD-WHT (entropy) technique with DSF from entropies is the best among three compared techniques for the attacked watermarked images.

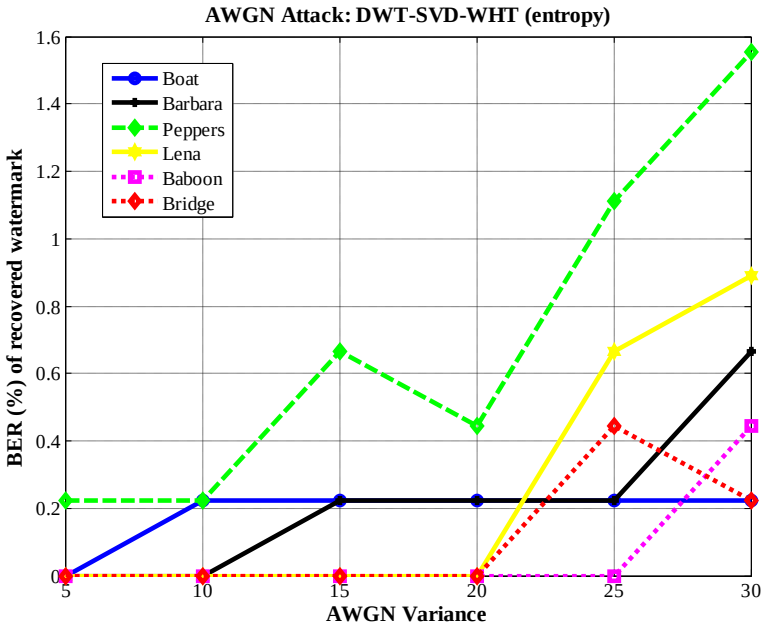


(a)

Figure 6.7 AWGN attack with different noise variances for watermark *TU* using (a) DWT-SVD-WHT (standard deviation), (b) DWT-SVD-WHT (mean) and (c) DWT-SVD-WHT (entropy)

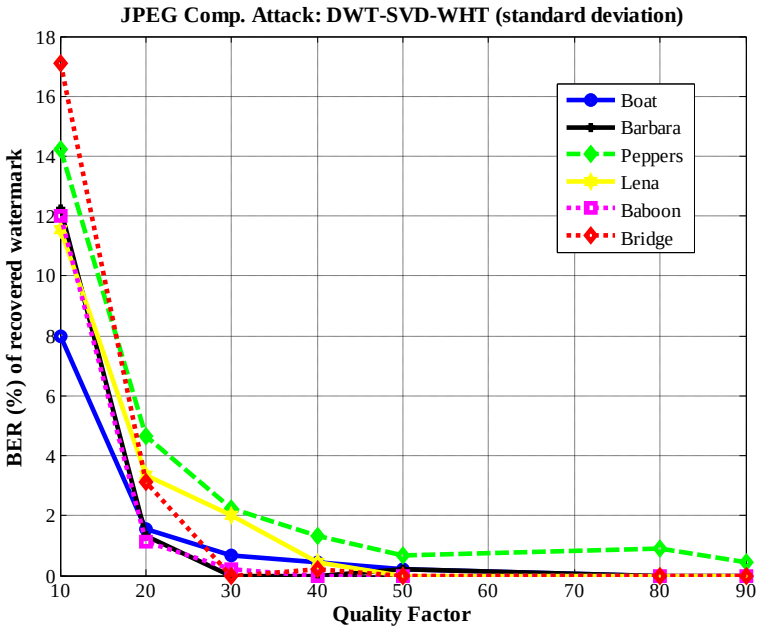


(b)

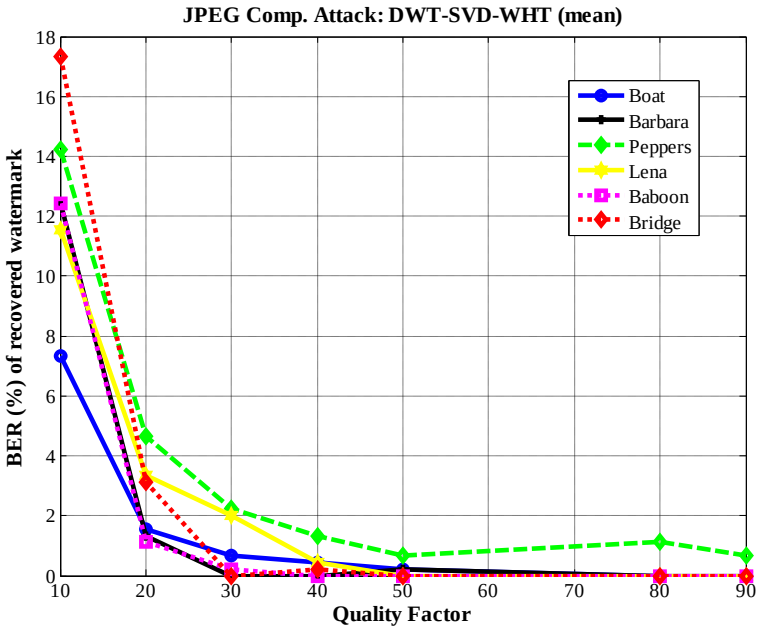


(c)

Figure 6.7 AWGN attack with different noise variances for watermark *TU* using (a) DWT-SVD-WHT (standard deviation), (b) DWT-SVD-WHT (mean) and (c) DWT-SVD-WHT (entropy)

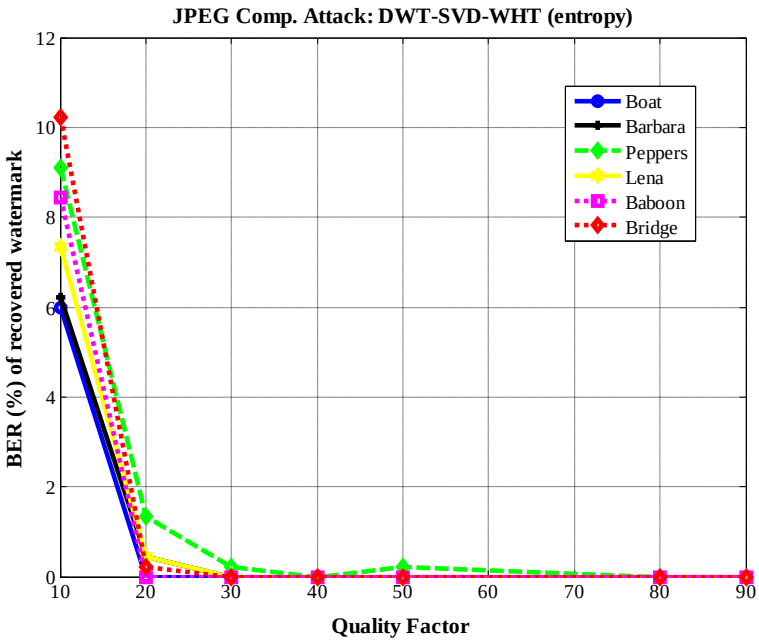


(a)



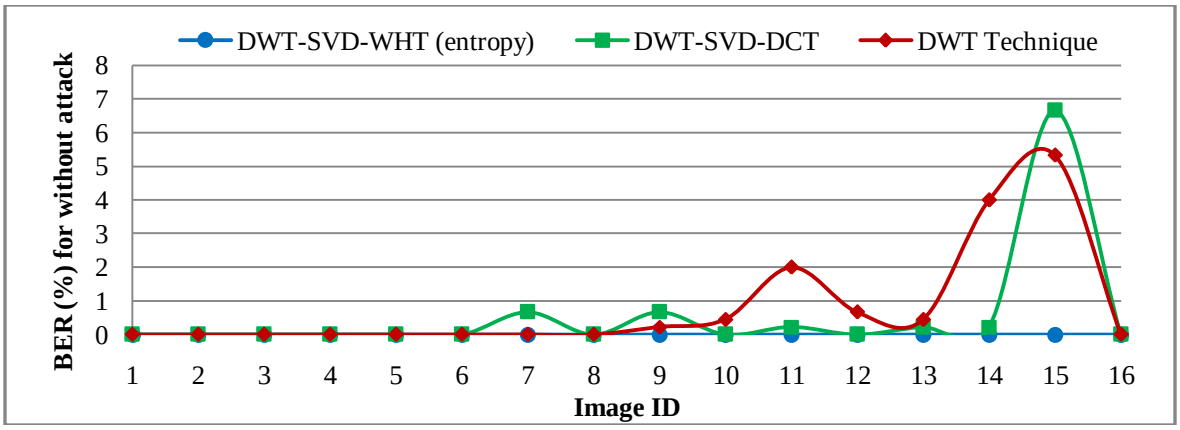
(b)

Figure 6.8 JPEG compression attack with various quality factors for watermark *TU* using (a) DWT-SVD-WHT (standard deviation), (b) DWT-SVD-WHT (mean) and (c) DWT-SVD-WHT (entropy)

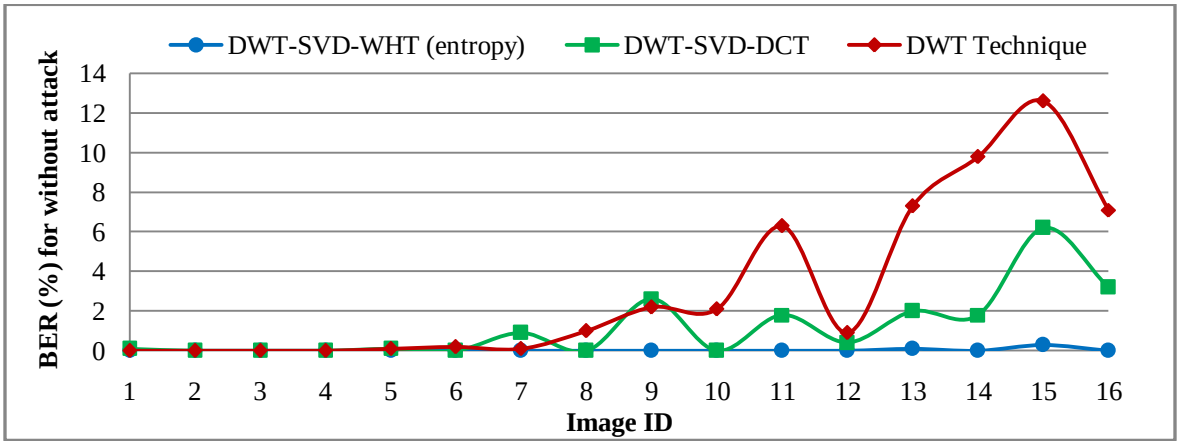


(c)

Figure 6.8 JPEG compression attack with various quality factors for watermark *TU* using (a) DWT-SVD-WHT (standard deviation), (b) DWT-SVD-WHT (mean) and (c) DWT-SVD-WHT (entropy)



(a)



(b)

(c)

Figure 6.9 BER (%) plot of recovered watermark without applying any attack on sixteen watermarked images having PSNR as 45 dB using DWT-SVD-WHT (entropy), DWT-SVD-DCT and DWT techniques with watermark (a) *TU* (b) *Copyright* (c) *Thapar_Univ*

Table 6.1 Values of adjusting parameter ρ for watermarked image PSNR 45 dB with DWT-SVD-WHT (standard dev.), DWT-SVD-WHT (mean) and DWT-SVD-WHT (entropy)

Host Image	Value of adjusting Parameter (ρ) with watermark *TU*			Value of adjusting Parameter (ρ) with watermark *copyright*			Value of adjusting Parameter (ρ) with watermark *Thapar_Univ*		
	DWT-SVD-WHT (standard dev.)	DWT-SVD-WHT (mean)	DWT-SVD-WHT (entropy)	DWT-SVD-WHT (standard dev.)	DWT-SVD-WHT (mean)	DWT-SVD-WHT (entropy)	DWT-SVD-WHT (standard dev.)	DWT-SVD-WHT (mean)	DWT-SVD-WHT (entropy)
Boat	1.639	1.718	2.938	1.691	1.776	3.135	1.720	1.809	3.235
Barbara	1.627	1.703	3.027	1.703	1.788	3.243	1.751	1.842	3.381
Peppers	1.603	1.679	2.896	1.674	1.759	3.118	1.705	1.793	3.196
Lena	1.622	1.699	2.98	1.676	1.759	3.148	1.704	1.791	3.204
Baboon	1.619	1.700	2.862	1.695	1.785	3.085	1.725	1.817	3.214
Bridge	1.571	1.641	3.024	1.648	1.729	3.297	1.681	1.765	3.415

Table 6.2 Comparison of BER (%) of recovered watermark under scaling attacks of different levels with watermark *TU*

Host Image	**DWT-SVD-WHT (standard dev.)**					**DWT-SVD-WHT (mean)**					**DWT-SVD-WHT (entropy)**				
	Scaling Level					Scaling Level					Scaling Level				
	0.75	***0.9***	***1.1***	***1.5***	***2***	***0.75***	***0.9***	***1.1***	***1.5***	***2***	***0.75***	***0.9***	***1.1***	***1.5***	***2***
Boat	0.22	1.33	12.00	0.00	0.00	0.22	1.33	11.78	0.00	0.00	0.00	0.00	8.89	0.00	0.00
Barbara	0.00	0.22	4.22	0.00	0.00	0.00	0.22	4.22	0.00	0.00	0.00	0.22	3.33	0.00	0.00
Peppers	1.33	3.55	9.11	0.22	0.44	1.33	3.56	9.11	0.22	0.44	0.00	0.44	6.67	0.00	0.00
Lena	0.00	2.22	9.78	0.00	0.00	0.00	2.22	9.78	0.00	0.00	0.00	1.11	7.33	0.00	0.00
Baboon	0.00	0.00	1.33	0.00	0.00	0.00	0.00	1.33	0.00	0.00	0.00	0.00	0.44	0.00	0.00
Bridge	0.00	0.44	4.67	0.00	0.00	0.00	0.44	5.11	0.00	0.00	0.00	0.00	2.89	0.00	0.00

Table 6.3 Comparison of BER (%) of recovered watermark under Median filter and Wiener filter attacks with watermark *TU*

Host Image	DWT-SVD-WHT (standard dev.)				DWT-SVD-WHT (mean)				DWT-SVD-WHT (entropy)			
	Median Filter		Wiener Filter		Median Filter		Wiener Filter		Median Filter		Wiener Filter	
	3 × 3	***5 × 5***	***3 × 3***	***5 × 5***	***3 × 3***	***5 × 5***	***3 × 3***	***5 × 5***	***3 × 3***	***5 × 5***	***3 × 3***	***5 × 5***
Boat	2.22	9.78	0.22	0.67	2.44	9.78	0.22	0.67	0.89	7.56	0.00	0.00
Barbara	0.89	13.78	0.22	2.89	0.89	13.78	0.22	2.89	0.22	11.56	0.00	1.56
Peppers	2.00	8.89	1.11	2.00	2.00	9.11	1.11	2.00	0.44	3.78	0.22	0.89
Lena	0.44	3.33	0.22	1.11	0.44	3.33	0.22	1.11	0.22	1.33	0.00	0.44
Baboon	20.67	38.67	0.22	3.56	21.33	38.67	0.22	3.78	16.89	36.89	0.00	1.56
Bridge	26.89	39.78	0.00	3.56	26.89	39.56	0.00	5.78	16.67	35.56	0.00	1.78

Table 6.4 Comparison of BER (%) of recovered watermark under Gaussian filter and Sharpening filter attacks with watermark *TU*

Host Image	DWT-SVD-WHT (standard dev.)			DWT-SVD-WHT (mean)			DWT-SVD-WHT (entropy)		
	Gaussian Filter		Sharpening	Gaussian Filter		Sharpening	Gaussian Filter		Sharpening
	3 × 3	***5 × 5***		***3 × 3***	***5 × 5***		***3 × 3***	***5 × 5***	
Boat	0.44	0.44	6.00	0.44	0.44	5.78	0.00	0.00	3.56
Barbara	0.22	0.22	3.56	0.22	0.22	3.33	0.22	11.56	2.22
Peppers	0.44	0.44	6.00	0.67	0.67	5.78	0.00	0.00	2.44
Lena	0.44	0.44	3.56	0.44	0.44	3.56	0.22	0.22	1.78
Baboon	0.44	0.22	9.11	0.44	0.44	9.11	0.22	0.22	8.00
Bridge	3.11	3.33	17.11	3.11	3.33	16.89	0.67	0.67	11.78

Table 6.5 Performance comparison of DWT-SVD-WHT (entropy) technique with DWT-SVD-DCT technique and DWT technique in terms of BER (%) of recovered watermark under various attacks on *Boat* watermarked image having PSNR as 45 dB with three different sized watermarks

Technique / Attack	DWT-SVD-WHT (entropy)			DWT-SVD-DCT			DWT Technique		
	***TU* (25×18)**	***Copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***Copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***Copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	6.00	20.8	26.62	8.67	24.10	29.37	15.33	24.4	30.44
AWGN (σ^2=20)	0.22	0.50	3.75	0.44	2.00	4.87	3.78	3.70	8.06
Median Filter (3×3)	0.89	5.90	11.62	2.44	7.90	17.69	3.78	7.10	14.19
Salt and Pepper (p=0.01)	1.33	5.20	9.94	2.00	6.30	12.37	10.22	12.5	16.56
Scaling (1.5)	0.00	0.00	0.00	0.00	0.10	3.69	0.22	0.70	2.94
Sharpening	3.56	6.40	11.75	5.11	7.00	13.12	12.00	21.20	24.00
Wiener Filter (3×3)	0.00	0.10	2.31	0.22	0.90	7.00	0.67	1.80	5.44
Gaussian Filter (3×3)	0.00	0.60	1.94	0.44	1.70	7.87	1.56	1.50	3.88

Table 6.6 Performance comparison of DWT-SVD-WHT (entropy) technique with DWT-SVD-DCT technique and DWT technique in terms of BER (%) of recovered watermark under various attacks on *Barbara* watermarked image having PSNR as 45 dB with three different sized watermarks

Technique / Attack	DWT-SVD-WHT (entropy)			DWT-SVD-DCT			DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	6.22	19.90	28.06	12.22	23.10	30.25	14.89	25.60	31.50
AWGN (σ^2=20)	0.22	0.40	2.81	1.11	1.40	3.75	1.78	4.40	7.31
Median Filter (3×3)	0.22	2.30	5.00	1.33	5.00	7.94	0.89	1.80	4.19
Salt and Pepper (p=0.01)	2.44	9.60	13.06	3.55	9.60	14.81	8.67	13.70	15.75
Scaling (1.5)	0.00	0.00	0.00	0.00	0.00	0.12	0.00	0.00	0.06
Sharpening	2.22	6.70	12.62	2.89	8.00	12.87	9.11	18.10	24.19
Wiener Filter (3×3)	0.00	0.20	0.44	0.22	1.20	1.44	0.67	0.90	1.06
Gaussian Filter (3×3)	0.22	0.60	2.50	0.22	1.90	3.25	2.00	3.30	3.38

Table 6.7 Performance comparison of DWT-SVD-WHT (entropy) technique with DWT-SVD-DCT technique and DWT technique in terms of BER (%) of recovered watermark under various attacks on *Peppers* watermarked image having PSNR as 45 dB with three different sized watermarks

Technique / Attack	DWT-SVD-WHT (entropy)			DWT-SVD-DCT			DWT Technique		
	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**	***TU* (25×18)**	***copyright* (50×20)**	***Thapar_Univ* (80×20)**
JPEG (Q=10%)	9.11	20.30	27.43	14.22	22.70	29.25	18.67	26.80	32.75
AWGN (σ^2=20)	0.44	1.60	4.31	2.00	10.20	6.37	4.22	5.80	8.63
Median Filter (3×3)	0.44	1.40	3.37	2.00	4.70	10.06	0.67	3.30	8.44
Salt and Pepper (p=0.01)	1.33	4.80	9.12	3.11	9.50	13.12	7.11	14.20	19.12
Scaling (1.5)	0.00	0.10	0.00	0.44	1.70	3.75	0.00	0.90	3.69
Sharpening	2.44	5.80	7.69	5.78	8.30	10.62	7.78	13.90	17.88
Wiener Filter (3×3)	0.22	0.20	0.87	1.11	1.80	7.00	0.89	1.60	6.50
Gaussian Filter (3×3)	0.00	0.10	0.75	0.44	2.20	6.37	1.56	1.70	5.56

Table 6.8 BER (%) comparison of recovered watermark for JPEG compression and median filter attack between DWT-SVD-WHT (entropy) technique and Kalantri *et al*. (2010) with watermark length of 256 bits, host image size 512×512 and watermarked image of PSNR 45 dB

Host Image	Kalantri *et al*. (2010)								DWT-SVD-WHT (entropy)							
	JPEG Compression Quality Factor (%)					Median Filter			JPEG Compression Quality Factor (%)					Median Filter		
	10	***20***	***30***	***40***	***50***	***3 × 3***	***5 × 5***	***7 × 7***	***10***	***20***	***30***	***40***	***50***	***3 × 3***	***5 × 5***	***7 × 7***
Boat	9.64	1.56	0.39	0.00	0.00	14.38	26.10	37.89	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.39**	**3.91**	**9.76**
Baboon	7.03	0.26	0.13	0.00	0.00	20.47	36.71	41.41	**0.78**	**0.00**	**0.00**	**0.00**	**0.00**	**7.42**	**24.22**	**37.50**
Peppers	8.07	2.21	0.78	0.26	0.00	3.44	14.45	25.07	**2.73**	**0.39**	**0.00**	**0.00**	**0.00**	**0.00**	**3.51**	**7.81**
Lena	9.24	1.74	0.78	0.13	0.00	10.16	21.48	28.52	**3.51**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**1.56**	**3.91**

Table 6.9 Recovered watermark BER (%) comparison between DWT-SVD-WHT (entropy) and Nezhadarya *et al*. (2011) under JPEG compression, median filter, Gaussian filter and scaling attacks with watermark length of 256 bits, host image size 512×512 and watermarked image of PSNR 42 dB

Attack / **Technique**	JPEG Compression					Median Filter		Gaussian Filter		Scaling
	20	30	40	50	60	3×3	5×5	3×3	5×5	2
Host Image Peppers										
Nezhadarya *et al*. (2011) GDWM	1.41	0.18	0.04	0.00	0.00	1.17	6.64	0.00	0.58	0.00
DWT-SVD-WHT (entropy)	**0.39**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**2.34**	**0.00**	**0.00**	**0.00**
Host Image Baboon										
Nezhadarya *et al*. (2011) GDWM	1.41	0.62	0.19	0.07	0.00	5.03	19.75	0.00	0.96	0.00
DWT-SVD-WHT (entropy)	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**2.73**	**15.23**	**0.00**	**0.00**	**0.00**
Host Image Barbara										
Nezhadarya *et al*. (2011) GDWM	1.69	0.16	0.05	0.00	0.00	1.10	8.14	0.00	0.13	0.00
DWT-SVD-WHT (entropy)	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**2.73**	**0.00**	**0.00**	**0.00**
Host Image Lena										
Nezhadarya *et al*. (2011) GDWM	1.65	0.41	0.22	0.10	0.00	0.00	7.10	0.00	0.17	0.00
DWT-SVD-WHT (entropy)	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.78**	**0.00**	**0.00**	**0.00**

6.4.3 Comparison of DWT-SVD-WHT (entropy) with other watermarking schemes

DWT-SVD-WHT (entropy) is first compared with a ridgelet domain technique Kalantri *et al*. (2010). In Table 6.8, for the JPEG compression attack and median filter attack, DWT-SVD-WHT (entropy) scheme shows remarkably good results. For example, with host image *Boat*, for JPEG compression of quality factor 10%, Kalantri's scheme gives BER (%) 9.64 while DWT-SVD-WHT (entropy) scheme gives BER (%) zero. Similarly with host image *Lena*, for median filter attack (3×3, 5×5 and 7×7), Kalantri *et al*. (2010) produces BER (%) as 10.16, 21.48, 28.52 while DWT-SVD-WHT (entropy) scheme gives results as 0, 1.56, 3.91. These results confirm that DWT-SVD-WHT (entropy) watermarking scheme shows much better performance than the compared scheme.

DWT-SVD-WHT (entropy) watermarking scheme has also been compared with Nezhadarya *et al*. (2011) which is a QIM based technique. The authors in this paper have used

watermark length of 256 bits and watermarked image PSNR value 42 dB with host image size of 512×512. Therefore the comparison in Table 6.9 has been done by employing all these attributes in DWT-SVD-WHT (entropy) scheme. In this table too, the presented scheme shows better performance for all the four attacks.

In the comparison tables all those results of the presented technique are shown in bold font where BER (%) of the recovered watermark is zero or has lesser BER (%) than the compared techniques.

6.5 CHAPTER SUMMARY

In this chapter a semi-blind hybrid watermarking technique using DWT, SVD and WHT has been proposed. Three dynamic strength factors derived from three local properties of the image have been used in this technique. Three versions of the proposed hybrid watermarking scheme, DWT-SVD-WHT (standard deviation), DWT-SVD-WHT (mean) and DWT-SVD-WHT (entropy) have been thoroughly analyzed and have been compared with each other by applying common watermarking attacks. Among these, DWT-SVD-WHT (entropy) produces least BER (%) for every attack. This version is also compared with watermarking techniques proposed in previous chapters (DWT technique and DWT-SVD-DCT technique) and two techniques of literature (Kalantri *et al.*, 2010 and Nezhadarya *et al.*, 2011). Based on the results of these comparisons, it can be clearly stated that DWT-SVD-WHT (entropy) is much more robust than all the compared techniques.

CHAPTER 7

CONCLUSIONS AND FUTURE SCOPE

THE research work discussed in the previous chapters has been summarized in this chapter. Some notable highlights of the work are mentioned. Scope and future prospects of the work are also presented.

7.1 CONCLUSIONS

Robust watermarking is used to protect the intellectual property rights of the genuine digital content provider/ owner. In this research work robust watermarking has been done by employing various image adaptive measures. Strength factor which determines the depth of watermarking has been derived by using local properties of the image.

A DWT based semi-blind image-adaptive technique has been used to compare the three sizes of the block segmentations of the images, 8×8, 16×16 and 32×32. Using a 512×512 sized host image there can be only 256 blocks in 32×32 block segmentation. As one watermark bit is embedded in every block therefore for the comparison of three block segmentations, two small watermarks are used having length less than 256 bits. Blocks having high values of entropy are used in watermark embedding. A dynamic strength factor is used which is derived from the standard deviations of the low frequency DWT coefficients. Side information is used in the extraction of embedded watermark. From the experimental results it is found that 8×8 block segmentation is best for the robustness of embedded watermark. That's why 8×8 block segmentation has been used in subsequent techniques proposed in the work.

Dynamic strength factor used in this proposed technique has different values for every image block. Dynamic strength factor is thoroughly analyzed by embedding different watermarks in a number of host images. Watermarked image of any desired PSNR value can be obtained by using a suitable value of the adjusting parameter of strength factor. Inverse relationship existing between imperceptibility and robustness of the watermark has been shown graphically. Provision of the side information security has been done. It has been shown

mathematically that, chances of success for a malicious interceptor of side information to know about the exact location of watermark embedding blocks is less than half percent. Comparisons with some well known techniques of literature (Akhaee *et al.* 2010, Kalantari *et al.* 2010, Tsougenis *et al.*, 2013 and Nezhadarya *et al*,. 2011) show the superiority of the proposed technique.

A hybrid watermarking technique which uses DWT, SVD and DCT is proposed in order to get an even better robust watermarking technique. In this technique too only high entropy blocks are used for watermarking of DCT coefficients. This technique is also a semi-blind technique and the side information generated at the time of watermark embedding is used in the watermark extraction. Dynamic strength factor is derived from the standard deviations of the DCT coefficients. This DWT-SVD-DCT technique shows better results when compared with earlier proposed DWT based technique and other techniques from the literature (Akhaee *et al.* 2009 and Tsougenis *et al.*, 2013).

Another hybrid watermarking technique is proposed which uses DWT, SVD and WHT together. In this technique three dynamic strength factors are derived from three local properties of the image. Two properties used are the standard deviation and mean of the WHT coefficients while third one is the entropy of those selected 8×8 blocks of the image which are used in watermark embedding. Three versions of the technique using these three strength factors are compared with each other by applying common watermarking attacks. The version of the proposed DWT-SVD-WHT watermarking technique that uses entropy to derive its strength factor shows the best results. This version named as DWT-SVD-WHT (entropy) is compared with earlier proposed techniques namely DWT based technique and DWT-SVD-DCT technique. It is also compared with two well established techniques of literature (Kalantari *et al.* 2010 and Nezhadarya *et al*,. 2011). DWT-SVD-WHT (entropy) shows the best performance in all the comparisons. Therefore it is the most robust technique of the presented research work.

7.2 HIGHLIGHTS OF THE WORK

Main highlights of all the robust image-adaptive watermarking techniques presented in this thesis are-

- 8×8 sized image pixel block segmentation found most suitable for robust watermarking.

- Visual quality of the watermarked image can be easily controlled in the proposed techniques.

- Proposed techniques are very simple to implement. No computational complexities for optimizing the strength factor.

- Proposed techniques are applicable to the host image of any size.

- Highly reliable side information security.

- DWT-SVD-WHT (entropy) found to be the most robust watermarking technique of the work.

7.3 FUTURE SCOPE

- More hybrid techniques could be derived by using different sets of transforms.
- More properties of the image could be used to derive an even more effective dynamic strength factor.
- Security of the side information could be more enhanced by employing some other innovative methods like the one shown in this thesis. Apart from the presented method of encoding, some more methods of encoding the side information could be used.
- Dynamic strength factor presented in this work has been used for robust watermarking. It may be tested for utilization in the fragile watermarking also, used for the image authentication.
- Proposed watermarking techniques which have been used on the still images, could be extended to the video and audio watermarking as well.
- Use of the proposed watermarking techniques could be explored in the real time applications also.

REFERENCES

Agarwal, C., Mishra, A. and Sharma, A. (2013). Gray-scale image watermarking using GA-BPN hybrid network. *Journal of Visual Communication and Image Representation*, 24(7), 1135-1146.

Ahmed, N. (1991). How I Came Up With the Discrete Cosine Transform. *Digital Signal Processing*, 1(1), 4-5.

Ahmed, N., Natarajan, T. and Rao, K. R. (1974). Discrete cosine transform. *IEEE Transactions on Computers*, C-23 (1), 90-93.

Ahumada Jr., A. J., Peterson, H. A. (1992). Luminance-Model Based DCT Quantization for Color Image Compression. *Proc. Of SPIE: Human Vision, Visual Processing and Digital Display III*, 1666, 365-374.

Akhaee, M. A., Sahraeian, S. M. E. and Marvasti, F. (2010). Contourlet Based Image Watermarking using Optimum Detector in a Noisy Environment. *IEEE Transactions on Image Processing*, 19(4), 967-980.

Akhaee, M. A., Sahraeian, S. M. E., Sankur, B. and Marvasti, F. (2009). Robust Scaling Based Image Watermarking using Maximum-Likelihood Decoder with Optimum Strength Factor. *IEEE Transactions on Multimedia*, 11(5), 822-833.

Akhbari, B. and Ghaemmaghami, S. (2005). Watermarking of still images using multiresolution singular value decomposition. *Proc. of IEEE International Symposium on Intelligent Signal Processing and Communication Systems*, 325-328.

Ali, M. (2015). Internet of things, everything and nano-things. *Proc. of Conference, World Congress on Engineering,* Imperial College, London, DOI:10.13140/RG.2.1.1670.7682.

Ali, M. and Ahn, C. W. (2014). An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain. *Signal Processing*, 94, 545-556.

Al-Otum, H. A. and Al-Taba'a, A. O. (2009). Adaptive color image watermarking based on a modified improved pixel-wise masking technique. *Computers and Electrical Engineering*, 35(5), 673-695.

Altun, O., Sharma, G., Celik, M. U. and Bocko, M. F. (2006). A Set Theoretic Framework for Watermarking and its Applications to Semi-fragile Temper Detection. *IEEE Transactions on Information Forensics and Security*, 1(4), 479-492.

Arnold, M.,Schmucker, M. and Wolthusen, S. D. (2003). *Techniques and Applications of Digital Watermarking and Content Protection*. Published by Atech House Inc.

Autonne, L. (1915). Sur les matrices hypohermitiennes et sur les matrices unitaires. *Annales de ÍUniversité de Lyon Nouvelle Sér. I. Sciences, médecine, fasc*. 38, 1-77.

Barni, M., Bartolini, F. and Pive A. (2001). Improved wavelet-based watermarking through pixel-wise masking. *IEEE Transactions on Image Processing*, 5(10), 783-791.

Baumert, L. D., Golomb, S. and Hall Jr, M. (1962). Discovery of an Hadamard matrix of order 92. *Bulletin of the American Mathematical Society*, 68, 237-238.

Beer, T. (1981). Walsh transforms. *American Journal of Physics*, 49(5), 466-472.

Beltrami, E. (1873). Sulle funzioni bilineari. *Giornale di Matematicihe ad Usodegli Studenti Delle Universtia*, 11, 98-106.

Bhatnagar, G., Raman, B. and Wu, Q. M. J. (2012). Robust watermarking using fractional wavelet packet transforms. *IET Image Processing*, 6(4), 386-397.

Bi H., Li, X., Zhang, Y. and Xu, Y. (2010). A blind robust watermarking scheme based on CT and SVD. *Proc. of IEEE International Conference on Signal Processing (ICSP)*, 881-884.

Bi, N., Sun, Q., Huang, D., Yang, Z. and Huang, J. (2007). Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition. *IEEE Transactions on Image Processing*, 16(8), 1956-1966.

Cauchy, A. L. (1829). Sur Íéquationá Í aide de laquelle on détermine les inégalitésséculaires des mauvements des planets. *Oeuvres Complétes* (*IIeSérie*), 9.

Celik, M. U., Sharma, G., Saber, E. and Tekalp A. M. (2002). Hierarchical Watermarking for Secure Image Authentication with Localization. *IEEE Transactions on Image Processing*, 11(6), 585-595.

Chang, C. C., Lin, P. Y. and Yeh, J. S. (2009). Preserving robustness and removability for digital watermarks using subsampling and difference correlation. *Information Sciences*, 179, 2283-2293.

Chen, B. and Wornell, G. (1999). Achievable performance of digital watermarking systems. *Proc. International Conference on Multimedia Computing and System* (*ICMCS '99*), Florence, Italy, 1, 13-18.

Chen, D. Y., Ouhyoung, M. and Wu, J. L. (2000). A shift-resisting public watermark system for protecting image processing software. *IEEE Transactions on Consumer Electronics*, 46(3), 404-414.

Chou, C. H., Liu, K. C. (2003). An oblivious and robust watermarking scheme using perceptual model. *Proc. of IEEE Conference Video Processing Multimedia Communications*, 713-720.

Cox, I. J., Kilian, J., Leighton, F. T. and Shamoon, T. (1997). Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673-1687.

Darazi, R., Callau, P. and Macq, B. (2009). Secure and HVS adaptive exhibition spread transform dither modulation watermarking for digital cinema. *Proc. First International Workshop on Information Forensics and Security*, 1-5.

Daubechies, I. (1988). Orthonormal bases of compactly supported wavelets. *Communications on Pure and Applied Mathematics*, 41(7), 909-996.

Dey, P. P. and Badkoobehi, H. (2011). Error flow analysis of abstract models. *International Journal on Computer Sciences and Technologies* (*IJCST*), 1(1), 1-4.

Dixit, A., Sharma, S. C. and Vijay, S. (2009). Simulation based study of bit error rate in CDMA communication network. *International Journal of Computing Science and Communication Technologies, Technia,* 1(2), 17-22.

Dong, P., Brankov, G., Galatsanos, N. P., Yang, Y. and Davoine, F. (2005). Digital Watermarking Robust to Geometric Distortions. *IEEE Transactions on Image Processing*, 14(12), 2140-2150.

Dony, R. D. (2001). Karhunen-Loeve Transform. *The Transform and Data Compression Handbook*, Chapter 1, Boca Raton, CRC Press LLC.

Eckart, C. and Young, G. (1936). The approximation of one matrix by another of lower rank. *Psychometrika*, 1, 211-218.

Ejaz, N., Anwar, J., Ishtiaq, M. and Baik, S. W. (2014). Adaptive image data hiding using transformation and error replacement. 73(2), 825-840

Falkowski, B. J. (2008). Phase watermarking algorithm using hybrid multi-polarity Hadamard transform. *Journal of Mathematical Imaging and Vision*, 30(1), 13-21.

Fami, E. S., Samavi, S., Kaviani, H. R. and Radani Z. M. (2012). Adaptive watermarking in Hadamard transform coefficients of textured image blocks. *Proc. of IEEE 16th CSI International Symposium on Artificial Intelligence and Signal Processing*, 503-507.

Feng, X. and Ji, X. (2009). A blind watermarking method with strong robust based on 2D barcode. *Proc. of IEEE International Conference on Information Technology and Computer Science*, 452-456.

Fike, C. T. (1968). *Computer Evaluations of Mathematical Functions*. Prentice-Hall, Section 7.4 and 7.5.

Furht, B., Muharemagic, E. and Socek, D. (2005). *Multimedia Encryption and Watermarking*. Published by Springer Science-Business Media Inc.

Gang, L. and Xin, K. Y. (2010). A novel chaos and HVS based image watermarking algorithm. *Proc. of IETE International Conference on Computer, Mechatronics, Control and Electronic Engineering* (*CMCE*), 31-34.

Ganic, E. and Eskicioglu, A. M. (2005). Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *Journal of Electronic Imaging*, 14(4), 043004-043009.

Gauss, C. F. (1823). Theoria combinationis observationum errorisbus minimis obnoxiae, pars posterior. Werke 4, *Koniglichen Gesselshaft der Wissenschaften Zu Gottingin*, 27-53.

Ghazy, R.A., El-Fishawy, N.A., Hadhoud, M.M., Dessouky, M.I. and El-Samie, F.E.A. (2007). An efficient block-by-block SVD based image watermarking scheme. *IEEE National Radio Science Conference*, 1-9.

Ghouti, L., Bouridane, A., Ibrahim, M. K. and Boussakta, S. (2006). Digital Image Watermarking using Balanced Multiwavelets. *IEEE Transactions on Signal Processing*, 54(4), 1519-1536.

Golub, G. H. and Kahan, W. (1965). Calculating the singular values and pseudo-inverse of a matrix. *Journal of the Society for Industrial and Applied Mathematics: Series B, Numerical Analysis*, 2(2), 205–224.

Golub, G. H. and Reinsch, C. (1970). Singular value decomposition and least squares solution. *Numerische Mathematik*, 14(5), 403-420.

Gonzalez, R. C. and Woods, R. E. (2009). *Digital Image Processing*. 3rd Edition, Pearson Education, Inc., New Delhi,

Gonzalez, R. C., Woods, R. E. and Eddins, S. L. (2009). *Digital Image Processing Using MATLAB*. 4th Edition, Pearson Education, Inc., New Delhi, Ch. 8, 301-302.

Grossmann, A. and Morlet, J. (1984). Decomposition of hardy functions into square integrable wavelets of constant shape. *SIAM Journal on Mathematical Analysis*, 15(4), 723–736.

Grossmann, A., Morlet, J. and Paul, T. (1985). Transforms associated to square integrable group representations. I: General results. *Journal of Mathematical Physics*, 26(10), 2473–2479.

Grossmann, A., Morlet, J. and Paul, T. (1986). Transforms associated to square integrable group representations. II: examples. *Annales de l'Institut Henri Poincaré*, 45(3), 293–309.

Guo, Q., Liu, Z., Liucora, S. (2011). Image watermarking algorithm based on fractional Fourier transform and random phase encoding. *Optics Communications*, 284(16), 3918-3923.

Haar, A. (1910). Zur theorie der orthogonalen funktionen systeme. *Mathematische Annalen*, 69, 331–371.

Hadamard, J. (1893). Resolution d'tune question relative aux determinants. *Bulletin des Sciences Mathématiques*, 17, 240-246.

Han, D., Yang, X. and Zhang, C. (2009). A novel robust 3D mesh watermarking ensuring the human visual system. *Proc. of IEEE 2nd International Workshop on Knowledge Discovery and Data Mining*, 705-709.

Hartung, F. and Kutter M. (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7), 1079-1107.

He, S., Kirovski, D. and Wu, M. (2009). High Fidelity Data Embedding for Image Annotation. *IEEE Transactions on Image Processing*, 18(2), 429-435.

Huang, J. and Shi, Y.Q. (1998). Adaptive image watermarking scheme based on visual masking. *IET Electronics Letters*, 34(8), 748-750.

Huang, J., Shi,Y. Q. and Shi Y. (2000). Embedding image watermarks in DC components. *IEEE Transactions on Circuits and Systems for Video Technology*, 10(6), 974-979.

Huang, S., Zhang, W., Wei, P. and Liu, Z. (2008). A robust watermarking scheme based on mean quantization. *Proc. of 3rd IEEE International Conference on Industrial Electronics*

and Applications, Singapore, 264-267.

Jacobi, C. G. J. (1846). Über ein leichtes Verfahren die in der Theeorie der Säculärstörungen vorkommenden Gleichungen numerisch aufzulösen. *Journal für die reine und angewandte Mathematik*, 30, 51-94.

Jadhav, S. D. and Bhalchandra, A. S. (2010). Blind source separation based robust digital image watermarking using wavelet domain embedding. *Proc. of IEEE Conference on Cybernatics and Intelligent Systems*, 162-167.

Jaffard, S., Yves, M. Y. and Ryan, R.D. (2001). Wavelets: tools for science & technology. *Society for Industrial Mathematics*, Philadelphia, PA

Jain, A. K. (2009). *Fundamentals of Digital Image Processing*. PHI Learning Pvt. Ltd., New Delhi.

Jankowsky, M. and Limiti, E. (2010). Freitag method improvement. *International Journal of Microwave and Optical Technology*, 5(4), 202-206.

Jordan, C. (1874a). Mémoire sur les formes bilinéaires. *Journal des Mathématiques Pures et Appliquées*, Deuxiéme Série, 2(19), 35-54.

Jordan, C. (1874b). Sur la réduction des formes bilinéaires. *Comptes Rendus de Í Academic Sciences*, Paris, 78, 614-617.

Kak, S. (1971). Classification of random binary sequences using Walsh-Fourier analysis. *Proc. of Applications of Walsh Functions*, Washington, D.C., 74-77.

Kalantari, N. K., Ahadi, S. M. and Vafadust, M. (2010). A Robust Image Watermarking in the Ridgelet Domain Using Universally Optimum Decoder. *IEEE Transactions on Circuits and Systems for Video Technology*, 20(3), 396-406.

Kang G. S. (2010). Blind digital image using adaptive casting energy in different resolutions of wavelet transform. *Proc. of IEEE International Conference on Computer & Technology*, 210-215.

Kang, X., Huang, J. and Zeng, W. (2008). Improving Robustness of Quantization-Based Image Watermarking via Adaptive Receiver. *IEEE Transactions on Multimedia*, 10(6), 953-959.

Kang, X., Huang, J., Shi, Y. Q. and Lin, Y. (2003). A DWT-DFT Composite Watermarking Scheme Robust To Both Affine Transform and JPEG Compression. *IEEE Transactions*

on Circuits and Systems for Video Technology, 13(8), 776-786.

Kennett, B. L. N. (1971). Introduction to the finite Walsh transform and the theory of the fast Walsh transform. *Proc. Symposium On Theory and Applications Of Walsh Functions, The Hatfield, Polytechnic, England*.

Kogbetliantz, E. G. (1955). Solution of linear systems by diagonalization of coefficients matrix. *Quarterly of Applied Mathematics*, 13, 123-132.

Komatsu, N. and Tominaga, H. (1988). Authentication System Using Concealed Images in Telematics. *Memoirs of the School of Science and Engineering*, Waseda University, 52, 45–60.

Kumsawat, P., Attakitimongcol, K. and Srikaew, A. (2005). A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms. *IEEE Transactions on Signal Processing*, 53(12), 4707-4719.

Kundur, D. and Hatzinakos, D. (1999). Digital Watermarking for Telltale Tamper Proofing and Authentication. *Proceedings of the IEEE*, 87(7), 1167-1180.

Kutay, M. A. and Ozaktas, H. M. (1998). Optimal image restoration with the fractional Fourier transform. *Journal of the Optical Society of America A*, 15(4), 825-833.

Kutter, M. and Winkler, S. (2002). A vision based masking model for spread-spectrum image watermarking. *IEEE Transactions on Image Processing*, 11(1), 16-25.

Lai, C. C. and Tsai, C. C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, 59(11), 3060-3063.

Lee, S. J. and Jung, S. H. (2001). A Survey of Watermarking Techniques applied to Multimedia. *Proc. of IEEE International Symposium on Industrial Electronics (ISIE, 01) Pusan, Korea*, 272-277.

Lewis, S., Knowles, G. (1992). Image compression using the 2-D wavelet transforms. *IEEE Transactions on Image Processing*, 2(1), 244-250.

Li, Q. and Cox, I. J. (2007). Using Perceptual Models to Improve Fidelity and Provide Resistance to Volumetric Scaling for Quantization Index Modulation Watermarking. *IEEE Transactions on Information Forensics and Security*, 2(3), 127-139.

Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L. and Lui, Y. M. (2001). Rotation,

Scale and Translation Resilient Watermarking for Images. *IEEE Transactions on Image Processing*, 10(5), 767-782.

Littlewood, J. E. and Paley, R. E. A. C. (1931). Theorems on Fourier series and power series. *Journal of the London Mathematical Society*, 6, 230–233.

Liu, J. and She, K. (2010). Robust image watermarking using dual tree complex wavelet transform based on human visual system. *Proc. of IEEE International Conference on Image Analysis and Signal Processing*, 675-679.

Liu, J. and She, K. (2012). A hybrid approach of DWT and DCT for rational dither modulation watermarking. *Circuits Systems and Signal Processing*, 31(2), 797-811.

Liu, J., Sun, J., Ji, W. and Li, Y. (2008). Novel image watermarking scheme based on ICA. *Proc. of IEEE International Conference on Neural Networks & Signal Processing*, Zhenjiang, China, 73-77.

Liu, K. (2009). Human visual system based watermarking for color images. *Proc. of IEEE Fifth International Conference on Information Assurance and Security*, 623-626.

Liu, S., Hennely, B. M. and Sheridan J. T. (2013). Digital image watermarking spread-space spread-spectrum technique based on double random phase encoding. *Optics Communication*, 300, 162-177.

Liyun, S., Hong, M. and Shifu, T. (2006). Adaptive image digital watermarking with DCT and FCM. Wuhan University *Journal of Natural Sciences*, 11(6), 1657-1660.

Lu, C. S. and Hsu, C. Y. (2007). Near-Optimal Watermark Estimation and Its Countermeasure: Antidisclosure Watermark for Multiple Watermark Embedding. *IEEE Transactions on Circuits and Systems for video technology*, 17(4), 454-467.

Mackenzie, D. (2001). Wavelets: seeing the forest and the trees. Article in *National Academy of Sciences, Washington*, DC. 1-8.

Maity, S. P. and Kundu, M. K. (2011). Perceptually adaptive spread transforms image watermarking scheme using Hadmard Transform. *Information Sciences*, 181(3), 450-465.

Makbol, N. M. and Khoo, B. E. (2013). Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEÜ-International Journal of Electronics and Communication*, 67(2), 102-112.

Mallat, S. G. (1989 a). A theory of multiresolution signal decomposition: the wavelet representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 11(7), 674–693.

Mallat, S. G. (1989 b). Multiresolution approximations and wavelet orthonormal bases of L^2 (R). *Transactions of the American Mathematical Society*, 315(1), 69–87.

Manz, J. W. (1972). A sequency-ordered fast Walsh transform. *IEEE Transactions on Audio and Electroacoustics*, 20(3), 204-205.

Meyer, Y. (1989). Orthonormal wavelets. In: Combers, J.-M. et al. (eds.) *Wavelets, time-frequency methods and phase space*, Springer-Verlag, Berlin, 2-20.

Meyer, Y. (1993). Wavelets, algorithms and applications. *Society for Industrial Mathematics*, Philadelphia, PA.

Milican, S., Ramanathan, P. and Saluja, K. K. (2014). CryptIP: An approach for encrypting intellectual property cores with simulation capabilities. *Proc. of 13th International Conference on Embedded Systems and VLSI design*, 92-97.

Minghui, D. and Jingbo, Z. (2009). Robust image watermarking algorithm against geometric attack based on BEMD. *Proc. of IEEE International Conference on Computer and Communication Security*, 36-39.

Mohammad, A. A., Alhaj, A. and Shaltaf, S. (2008). An improved SVD based watermarking scheme for protecting rightful ownership. *Signal Processing*, 88(9), 2158-2180.

Mohanty, S. P., Guturu, P., Kougianos, E. and Pati, N. (2006). A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction. *Proc. of the eighth IEEE International Symposium on Multimedia*, 153-160.

Moon, H. S., You, T., Sohn, M. H., Kim, H. S. and Jang, D. S (2007). Expert system for low frequency adaptive image watermarking: Using psychological experiments on human image perception. *Expert Systems with Applications*, 32(2), 674-686.

Nafornita, C. (2005). Improved detection for robust image watermarking. *Proc. International Symposium on Signals*, Circuits and Systems, 2, 473-476.

Nema, S., Goel, A. and Singh R. P. (2010). Integrated DWDM and MIMO-OFDM system for 4 G high capacity mobile communication. *Signal Processing: An International Journal*, 3(5), 132-143.

Newland, D. E. (1993). Harmonic wavelet analysis. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 443(1917), 203–225.

Nezhadarya, E., Wang, Z. J., Ward, R. K. (2011). Robust Image Watermarking Based on Multiscale Gradient Direction Quantization. *IEEE Transactions on Information Forensics and Security*, 6(4), 1200-1213.

Niu, P. P., Wang, X. Y., Jin, H. B. and Lu, M. Y. (2011). A feature-based robust digital image watermarking scheme using bandelet transform. *Optics & Laser Technology*, 43(3), 437-450.

Osberger, W. and Maeder, A. J. (1998). Automatic identification of perceptually important regions in an image. *Proc. of the 14th IEEE International Conference on Pattern Recognition,* 701-704.

Ozaktas, H. M., Barshan, B.,Mendlovic, D. and Onural, L. (1994). Convolution filtering and multiplexing in fractional Fourier domain and their relation to chirp and wavelet transform. *Journal of the Optical Society of America A*, 11(2), 547-559.

Pal, N. S., Sarin, R. K., Singhal, K. and Ranjan, R. (2012). Distributed arithmetic algorithm for raised cosine FIR filter in WCDMA systems. *MIT International Journal of Electronics and Communication Engineering*, 2(1), 5-10.

Paley, R. E. A. C. (1933). On orthogonal matrices. *Journal of Mathematical Physics*, 12, 311-320.

Peng, H., Wang, J. and Wang, W. (2010). Image watermarking method in multiwavelet domain based on support vector machines. *The Journal of Systems and Software*, 83(8), 1470-1477.

Petitcolas, F., Anderson, R. and Kuhn, M. (1998). Attacks on copyright marking systems. *Information Hiding* (D. Aucsmith, ed.), 1525 of Lecture Notes in Computer Science, (Berlin), Springer-Verlag., 218–238.

Pi, M. H., Li, C. H. and Li, H. (2006). A Novel Fractal Image Watermarking. *IEEE Transactions on Multimedia*, 8(3), 488-499.

Picard, E. (1909). Quelques remarques sur les équations intégrales de premiére espéce et sur certains probléms de Physique mathématique. *Comptes Rendus de L' Academie Sciences, Paris*, 148, 1563-1568.

Pickholtz, R. L., Schilling, D. L. and Millstein L. B. (1982). Theory of spread spectrum communications-A tutorial. *IEEE Transactions on Communication*, COMM-30, 855-884.

Podilchuk, C. I. and Zeng, W. J. (1998). Image-adaptive watermarking using visual models. *IEEE Selected Areas in Communications*, 16(4), 525-539.

Prasad, R. (2000). Pade type model order reduction for multivariable system using routh approximation. *Computers & Electrical Engineering*, 26(6), 445-459.

Pujara, C., Bhardwaj, A. and Gadre, V. M. (2007). Secure watermarking in fractional wavelet domain. *IETE Journal of Research*, 53(6), 573-580.

Qi, X. and Qi, J. (2007). A robust content-based digital image watermarking scheme. *Signal Processing*, 87(6), 1264-1280.

Rahimi, F., Rabani, H. (2010). A visually imperceptible and robust image watermarking scheme in contourlet domain. *Proc. of IEEE 10th International Conference on Signal Processing* (*ICSP*), 1817-1820.

Rastegar, S., Namazi, F., Yaghmaie, K. and Aliababadian, A. (2011). Hybrid watermarking algorithm based on singular value decomposition and radon transform. *AEÜ-International Journal of Electronics and Communication*, 65(7), 658-663.

Rawat, S. and Raman, B. (2012a). A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. *Signal Processing*, 92(6), 1480-1491.

Rawat, S. and Raman, B. (2012b). A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion. *AEÜ-International Journal of Electronics and Communication*, 66(11), 955-962.

Ricker, N. (1953). The form and laws of propagation of seismic wavelets. *Geophysics*, 18(1), 10–40.

Run, R. S., Horng, S. J., Lai, J. L., Kao, T. W. and Chen, R. J. (2012). An improved SVD-based watermarking technique for copyright protection. *Expert Systems with applications*, 39(1), 673-689.

Sakr, N., Zhao, J. and Groza, V. (2005). A dynamic fuzzy logic approach to adaptive HVS-based watermarking. *Proc. of IEEE International Workshop on Haptic Audio Video Environments and their Applications*, Ottawa, Ontario, Canada, 121-126.

Sang, J. and Alam, M. S. (2008). Fragility and Robustness of Binary-Phase-Only-Filter Based Fragile/Semifragile Digital Image Watermarking. *IEEE Transactions on Instrumentation and Measurement*, 57(3), 595-606.

Santhi, V. and Arulmozhivarman, P. (2013). Hadamard transform based adaptive visible/invisible watermarking scheme for digital images. *Journal of Information Security and Applications*, 18(4), 167-179.

Sarla, S. and Jain, P. (2000). A circular statistical method for extracting rotation measures. *arXiv: Astrophysics/ 0007251*, 1, 1-17.

Schmidt, E. (1907). Zur Theeorie der linearen und nichtlinearen Integralgleichungen. I Teil. Entwicklung willkürlichen Funktionen nach System Vorgeschriebener. *Mathematische Annalen*, 63, 433-476.

Sheng, N. L., Hui, D. G. (2009). Watermarking scheme of color image based on chaotic sequences. *Optoelectronic Letters*, 5(3), 227-231.

Shetty, N. K. and Rodriguez, J. J. (2006). Equalized spectrum watermarking using perceptual modeling. *Proc. of IEEE Southwest Symposium on Image Analysis and Interpretation*, 1-5.

Shih, Y. and Han, J. (1978). Double Walsh series solution of first-order partial differential equations. *International Journal of Systems Science*, 9(5), 569-578.

Shijie, R., Xin, S (2009). A chaos-based blind wavelet-domain watermarking scheme using fast ICA. *Proc. of IEEE 2nd International Workshop on Computer Science and engineering*, 68-71.

Singh, J., Singh, S., Singh, D. and Uddin, M. (2011). A signal adaptive filter for blocking effect reduction of JPEG compressed images. *AEÜ-International Journal of Electronics and Communication*, 65(10), 827-839.

Solanki, K., Jacobsen, N., Madhow, U., Manjunath, B. S. and Chandrasekaran, S. (2004). Robust Image Adaptive Data Hiding Using Erasure and Error Correction. *IEEE Transactions on Image Processing*, 13(12), 1627-1639.

Song, H.,Yu, S., Yang, X. et al. (2008). Contourlet based image adaptive watermarking. *Signal Processing: Image Communication*, 23(3), 162-178.

Stankovic, S., Orovic, I. and Zaric, N. (2010). An Application of Multidimensional Time-Frequency Analysis as a base for the Unified Watermarking Approach. *IEEE Transactions on Image Processing*, 19(3), 736-745.

Stewart, G. W. (1993). On the Early History of the Singular Value Decomposition. *SIAM Review*, 35(4), 551–566.

Stollnitz, E. J., Derose, T. D. and Salesin, D. H. (1996). Wavelets for Computer Graphics: Theory and Applications. *Morgann Kaufmann*, San Francisco, CA.

Strang G. (1998). *Introduction to Linear Algebra*. Wellesley-Cambridge Press, ISBN 0-9614088-5-5.

Strang, G. (1999). The Discrete Cosine Transform. *SIAM Review*, 41(1), 135-147.

Strömberg, J. O. (1983). A modified Franklin system and higher-order spline systems on Rn as unconditional bases for Hardy space. *Proc. of Conference on Harmonic Analysis in Honor of Antoni Zygmund*, 2, 475–494.

Swanson M. D., Zhu, B. and Tewfik A.H.(1996). Transparent robust image watermarking. *Proc. of IEEE International Conference on Image Processing*, 3, 211-214.

Sylvester, J. J. (1867). LX. Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 34(232), 461-475.

Sylvester, J. J. (1889). A new proof that a general quadric may be reduced to its canonical form (that is, a linear function of squares) by means of a real orthogonal substitution. *Messenger of Mathematics*, 19, 1-5.

Tamane S. C. and Manza, R. R. (2009). 3D models watermarking using fuzzy logic. *Proc. of IEEE International Conference on Advances in computing, control and telecommunication technologies*, 195-197.

Tian, L., Zheng, N., Xue, J., Li, C. and Wang, X. (2011). An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection. *Signal Processing: Image Communication*, 26(8), 427-437.

Tsai, H. H., Jhuang, Y. J. and Lai, Y. S. (2012). An SVD based watermarking in wavelet domain using SVR and PSO. *Applied Soft Computing*, 12(8), 2442-2453.

Tsougenis, E. D., Papakostas G. A., Koulouriotis D. E. and Tourassis V. D. (2013). Towards adaptivity of image watermarking in polar harmonic transforms domain. *Optics and Laser Technology*, 54, 84-97.

Tsui, T. K., Zhang, X. and Androutsos, D. (2008). Color Image Watermarking using Multidimensional Fourier Transforms. *IEEE Transactions on Information Forensics and Security*, 3(1), 16-27.

Turyn, R. J. (1970). Complex Hadamard matrices. *Combinatorial Structures and Their Applications*, Gordon and Breach, London, 435-437.

Vetterli, M. and Kovacevic, J. (1995). *Wavelets and Subband Coding*. Prentice Hall.

Walsh, J. L. (1923). A closed set of normal orthogonal functions. *American Journal of Mathematics*, 45, 5-24.

Wang, Y., Ji, X. (2009). A new algorithm for watermarking based on DCT and chaotic scrambling. *Proc. of IEEE 4th International Conference on Computer Science and Education*, 1957-1961.

Wang, Z., Zhai, G. and Wang, N. (2006). Digital watermarking algorithm based on wavelet transform and neural network. *Wuhan University Journal of Natural Sciences*, 11(6), 1667-1670.

Watson, A. B. (1993). DCT quantization matrices optimized for individual images. *Proc. of SPIE: Human Vision, Visual Processing and Digital Display* IV, 1913, 202-216.

Watson, A. B., Borthwick, R. and Taylor, M. (1997a). Image quality and entropy masking. In *Electronic Imaging'97, International Society for Optics and Photonics*, 2-12.

Watson, A. B., Yang, G. Y., Solomon J. A. and Villasenor, J. (1997b). Visibility of wavelet quantization noise. *IEEE Transactions on Image Processing*, 6(8), 1164-1175.

Weierstrass, K. (1868). Zur Theorie der bilinearen und quadratischen Formen. *Monatshefte Akademie Wissenschaften Berlin*, 310-338.

Wen, X. B., Zhang, H., Xu, X. Q. and Quan, J. J. (2009). A new watermarking approach based on probabilistic neural network in wavelet domain. *Soft Computing*, 13(4), 355-360.

Williamson, J. (1944). Hadamard's determinant theorem and the sum of four squares. *Duke Mathematical Journal*, 11(1), 65-81.

Wolfgang, R. B. and Podilchuk, C. I. (1999). Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, 87(7), 1108-1126.

Wu, J. and Ke, J. (2003). Adaptive image watermarking scheme based on HVS and fuzzy clustering theory. *Proc. of IEEE International Conference on Neural Networks and Signal Processing*, Nanjing, China, December 14-17, 1493-1496.

Wu, X. and Xiong, Y. (2010). Adaptive watermarking algorithm based on chaotic map. *Proc. of IEEE International Conference on Computer Application and System Modeling*, V6-477 – V6-480.

Xiang, S., Kim, H. J. and Huang, J. (2008). Invariant Image Watermarking Based on Statistical Features in the Low Frequency Domain. *IEEE Transactions on Circuits and Systems for video technology*, 18(6), 777-790.

Xiao, L., Wu, H., Wei, Z. and Bao, Y. (2005). Research and application of a new computational of human vision system based on ridgelet transform. *Proc. of the IEEE 4th International Conference on Machine Learning and Cybernatics*, Guangzhou, 5170-5175.

Yan, Y., Cao, W. and Li, S. (2009). Block-based image watermarking scheme using just noticeable differences. *Proc. IEEE International Workshop on Imaging Systems and Techniques*, Shenzhen, China, 377-380.

Yuan, H. and Zhang, X. P. (2006). Multiscale Fragile Watermarking Based on the Gaussian Mixture Model. *IEEE Transactions on Image Processing*, 15(10), 3189-3200.

Yuen, C. (1972). Remarks on the ordering of Walsh functions. *IEEE Transactions On Computers*, C-21, 1452.

Zaid, A. O., Makhloufi, A., Bouallegue, A. and Olivier, C. (2010). JP3D compressed domain watermarking of still and volumetric medical images. *Signal, Image and Video Processing*, 4(1), 11-21.

Zhang, C., Cheng, L. L., Qiu, Z. and Cheng, L. M. (2008a). Multipurpose watermarking based onmultiscalecurvelet transform. *IEEE Transactions on Information Forensics and Security*, 3(4), 611-619.

Zhang, X. P., Li, K. and Wang, X. (2008b). A novel look-up table design method for data hiding with reduced distortion. *IEEE Transactions on Circuits and Systems for Video Technology*, 18(6), 769-776.

Zhang, Y. (2009). Digital Watermarking Technology: A Review. *Proc. of IEEE International Conference on Future Computer and Communication* (*FCC'09*), 250-252.

Zheng, D., Wang, S. and Zhao, J. (2009). RST Invariant Image Watermarking Algorithm with Mathematical Modeling and Analysis of the Watermarking Processes. *IEEE Transactions on Image Processing*, 18(5), 1055-1068.

Zhu, P., Jia, F. and Zhang, J. (2013). A copyright protection watermarking algorithm for remote sensing image based on binary watermark. *Optik-International Journal for Light and Electron Optics*, 124(20), 4177-4181.

Zolghadrasli, A. and Rezazadeh, S. (2007). Evaluation of spread spectrum watermarking schemes in the wavelet domain using HVS characteristics. *Proc. of IEEE 9th International Symposium on Signal Processing and its Applications*, Sharjah, 1-4.

APPENDIX-I

SAMPLE HOST IMAGES (512×512) (http://sipi.usc.edu/database/)

Image ID 1 (Bridge)

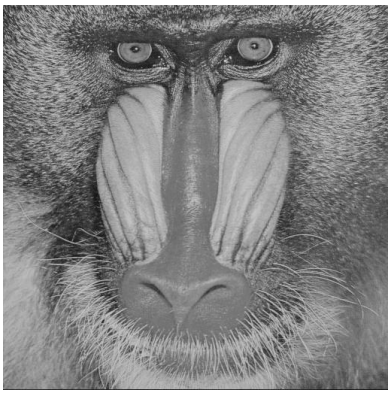


Image ID 2 (Baboon)

Image ID 3 (Aerial)

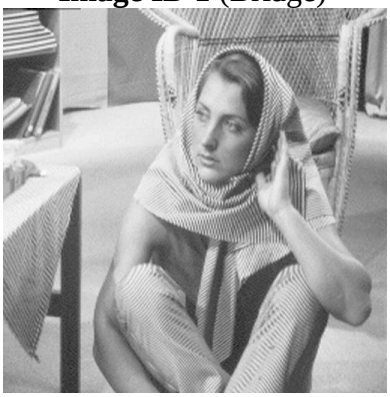


Image ID 4 (Barbara)

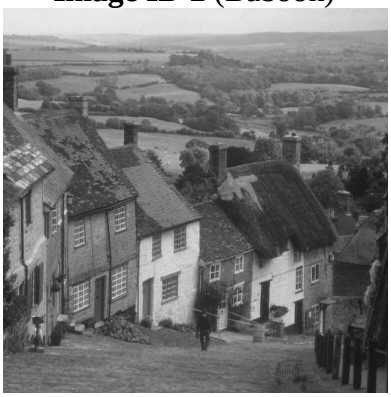


Image ID 5 (Goldhill)

Image ID 6 (Couple)

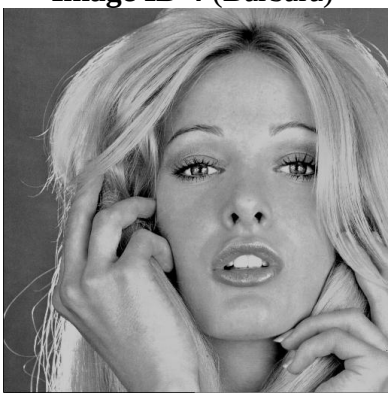


Image ID 7 (Woman_Blondehair)

Image ID 8 (Pirate)

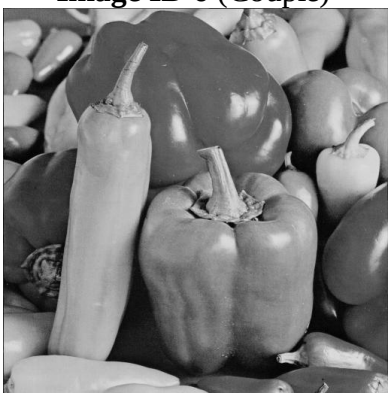


Image ID 9 (Peppers)

Image ID 10 (Lena)

Image ID 11 (Lake)

Image ID 12 (Boat)

Image ID 13 (Plane)

Image ID 14 (Woman_Darkhair)

Image ID 15 (Cameraman)

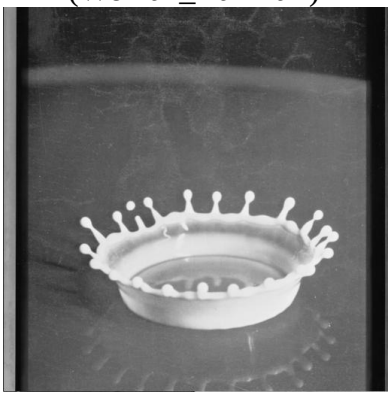


Image ID 16 (Milkdrop)

APPENDIX-II

WATERMARKS

Small sized watermarks

TU **(12 × 9)**

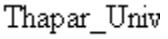
T UNIV **(27×8)**

TU **(25 × 18)**

Medium sized watermark

Copyright **(50×20)**

Large sized watermark



Thapar_Univ **(80×20)**