uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Nizar Sakr

AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.A.Sc. (Electrical Engineering)

GRADE / DEGREE

School of Information Technology and Engineering

FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Adaptive Digital Image Watermaking based on Predictive Embedding and a Dynamic Fuzzy Inference System Model

TITRE DE LA THÈSE / TITLE OF THESIS

Jiying Zhao

DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

Voicu Groza

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Wail Gueaieb

Peter X. Liu

Gary W. Slater

LE DOYEN DE LA FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES /
DEAN OF THE FACULTY OF GRADUATE AND POSTDOCORAL STUDIES

Adaptive Digital Image Watermarking based on Predictive Embedding and a Dynamic Fuzzy Inference System Model

by

Nizar Sakr, B.A.Sc.

A thesis
submitted to the Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of
Master of Applied Science in Electrical Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering
School of Information Technology and Engineering (SITE)
University of Ottawa

Your file Votre référence
ISBN: 978-0-494-14944-7
Our file Notre référence
ISBN: 978-0-494-14944-7

Abstract

A novel image watermarking scheme is introduced that consists of an adaptive watermarking algorithm based on a model of the Human Visual System (HVS) and a Dynamic Fuzzy Inference System (DFIS). This scheme relies on the DFIS to extract the human eye sensitivity knowledge using the HVS model. The DFIS and the HVS combined are used to adjust and select the appropriate watermark length as well as the watermarking strength for each pixel in an image. The main goal of the algorithm is to provide a more robust and imperceptible watermark. The primary contribution of this work is to present a unique approach to perform image-adaptive watermarking by introducing a dynamic fuzzy logic technique. This logic relies on the statistical distributions of the HVS-generated data in order to accurately approximate the relationship found between all properties of the human perceptual system. In addition, we introduce a *Predictive Watermark Embedding* (PWE) algorithm that exploits the average power of the frequency-domain image coefficients as well as the aforementioned DFIS model in order to insure that the watermark insertion process is adaptively and accurately performed in lower-frequency components and significant DCT coefficients. The aforementioned has been implemented and tested under various attacks including image compression, cropping, additive Gaussian noise distortion, scaling, low-pass filtering, as well as collusion attacks. The results achieved demonstrate that the watermark can survive these attacks while remaining imperceptible. Furthermore, the obtained results are compared with three other popular schemes and demonstrate that our proposed scheme yields better results in terms of watermark imperceptibility and robustness.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Dr. Voicu Groza for his encouragement, and support in various research projects throughout the pursuit of my Master's degree. I would also like to extend my sincere thanks to my co-supervisor Dr. Jiying Zhao for his valuable supervision and support throughout the preparation of this thesis. I want to also thank Dr. Wail Gueaieb and Dr. Peter X. Liu for kindly accepting to be on my examining committee.

I would like to express my appreciation to Mom and Dad for their patience and sacrifice, as well as their constant support and encouragement toward the pursuit of excellence. I am also very grateful to my brother and sisters for their constant positive reinforcement throughout the course of my education. Last but not least, thanks are also due to my friends for their advice, and encouragement.

Contents

List of Tables

List of Figures

Acronyms and Common Variables

Acronyms

AAD Average Absolute Deviation

DCT Discrete Cosine Transform

DFIS Dynamic Fuzzy Inference System

DFT Discrete Fourier Transform

DMFE Dynamic Membership Function Engine

DWT Discrete Wavelet Transform

FIS Fuzzy Inference System

HVS Human Visual System

IDCT Inverse Discrete Cosine Transform

JND Just Noticeable Difference

JPEG Joint Photographic Experts Group

MF Membership Function

PSNR Peak Signal to Noise Ratio

PWE Predictive Watermark Embedding

Variables

α	Watermark embedding strength
f	Embedding region factor
i	Inferred value (output of the fuzzy inference system)
k	An 8×8 block of an image
l	Sub-watermark length
n	Size of embedding region
P	Average power of the DCT components
R	Frequency range
V	Cover work (Original)
V'	Watermarked work

Chapter 1

Introduction

The fast development of the Internet and the World Wide Web as well as the rapid emergence of multimedia applications in the past decade have yielded a significant growth in the transmission of digital media over the Internet, including images, audio and video. However, the transmission of information over various networks is often unsafe. This lack of security can be critical depending on the nature of the transmitted media. This issue gave rise to digital watermarking, a research field which deals with the process of embedding information into digital data in an inconspicuous manner. A digital watermark is a signal that typically consists of a pattern of bits that is embedded directly into the digital contents of an image, video or audio. This in turn enables information security for various multimedia applications including copyright protection.

The technique presented in this thesis focuses on the watermarking of digital images. The following terminology is adopted throughout the remainder of this document. The term *Work* is sometimes used when referring to a copy of a specific song, video or image. The original image is often referred to as the *cover image*. In addition, the term *Media* is occasionally used to refer to the means of representing, transmitting and recording digital content. The purpose of this first chapter is to briefly introduce the topic and to provide the reader with the necessary background information to facilitate reading the remainder of the thesis.

1.1 Background

A generic watermarking system of the type that will be investigated here, encompasses two primary components: a *Watermark embedder* as well as a *Watermark Detector*. As it is illustrated in Fig. 1.1, two inputs are fed to the watermark embedder. The first input is the cover work in which we want to embed a watermark, whereas the second input is the watermark message itself, and it may take on various formats (real values, binary values, etc.). The watermarked work is subsequently recorded or transmitted by the user. The watermark detector on the other hand, takes a specific work (not necessarily watermarked) as an input and it attempts to determine whether a watermark is present in the digital content, and if so, detect and output the corresponding message.

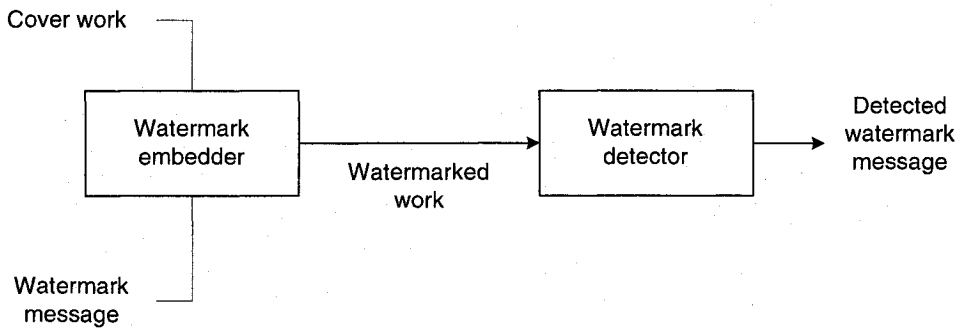


Figure 1.1: A generic watermarking system. Reprinted from [1]

Digital image watermarking has been extensively researched in literature, where various approaches have been proposed. These techniques can generally be divided into two important categories: spatial-domain and frequency-domain. In spatial-domain, the most popular methods are based on the Least-Significant-Bit (LSB) insertion scheme [2, 3] and the patchwork technique [4]. The former method consists of embedding the watermark into the least significant bits of selected pixels of the cover image, while the latter inserts a single bit of data in the cover work by means of a statistical method and the luminance information extracted from the image. An advantage of the spatial techniques is their robustness against

cropping and translation attacks. However, a possible disadvantage of these schemes is their weakness against signal processing attacks, including additive noise and lossy compression. In addition, adaptive watermarking techniques can be slightly more difficult to perform in the spatial domain [5]. Conversely, frequency-domain techniques are generally more robust against signal processing and geometric transformations than spatial domain based methods. The most common frequency-domain watermarking methods use the following data transformation techniques: the discrete cosine transform (DCT) [6, 7, 8, 10, 11, 12], the discrete Fourier transform (DFT) [13, 14], and the discrete wavelet transform (DWT) [15]. The DCT has been extensively used in image processing and digital watermarking for several important reasons. First, it divides the image into three distinguishable frequency bands, enabling easy access to the perceptually significant low and middle frequency components [16], as it is illustrated in Fig. 1.2. Appropriate selection of the frequency bands is crucial in digital watermarking, because the watermark must be inserted in low or middle frequency coefficients, otherwise, it can be easily suppressed by compression or low-pass filtering attacks.

Furthermore, the sensitivity of the human visual system in DCT domain has been significantly studied [17], which has resulted the default JPEG quantization table [18]. This also demonstrates that this domain can easily be exploited to incorporate the HVS characteristics, which in turn are used to minimize the visual degradations of the digital data, commonly introduced during the watermark embedding process. The drawback of DCT based watermarking schemes is their vulnerability against geometric attacks, such as rotation, scaling and translation. The DWT is another important frequency-domain transform as it provides a multi-resolution representation of an image. This property is used by various watermarking schemes in order to generate an efficient watermark detection scheme as it is illustrated in [15]. Conversely, the DFT generally provides a magnitude and a phase representation of the cover work. However, most of the significant information about the image is contained within the phase component. In consequence, watermarking techniques based

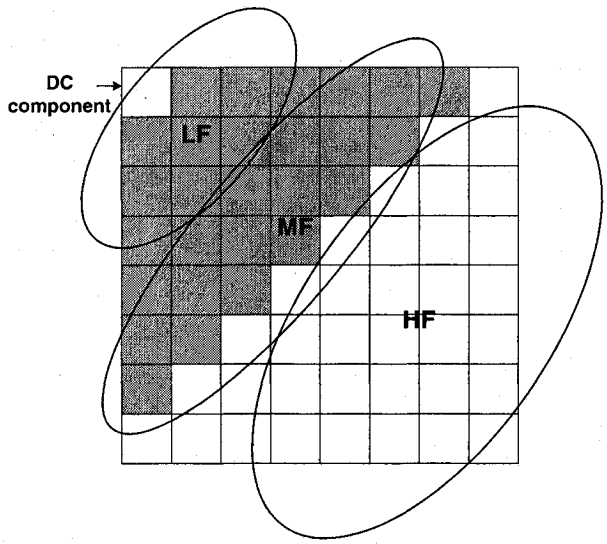


Figure 1.2: This diagram illustrates the location of the Low-Frequencies (LF), Mid-Frequencies (MF) and High-Frequencies (HF) when the DCT is performed on an 8×8 block of an image. The shaded area encompasses the AC DCT coefficients commonly used by image watermarking schemes to insert a watermark.

on this transform typically add the watermark to the phase coefficients [14]. This insures a robust watermark, since any attempt to remove the watermark will result in significant degradation of the image.

There are many requirements that must be considered when designing an effective and accurate watermarking scheme, including robustness, imperceptibility and capacity. However, in order to maintain the quality of the image and increase the probability of the watermark detection, two requirements are indispensable: robustness and imperceptibility (or transparency). Robustness is the ability of the watermark to survive various distortions that may be introduced unintentionally during certain random manipulations of the digital data, or intentionally, when a malicious attack is introduced to deliberately alter or remove the embedded watermark. Malicious attacks may consist of signal processing operations (such as filtering, lossy compression and additive noise) and geometric transformations (such as cropping, rotation, scaling and translation). Conversely, imperceptibility refers to the in-

visible degradation of the image when watermarked. Ideally, the perceptual quality of the watermarked image must be identical to the original.

The proposed is an adaptive image watermarking algorithm based on a HVS model and a DFIS. The dynamic FIS and the HVS combined are used to adjust the watermarking strength and to generate the maximum possible watermark length that can be embedded without noticeably degrading the quality of the cover image. The watermark is embedded into the low frequency range of the image after being transformed by the Discrete Cosine Transform (DCT).

1.2 Applications of Watermarking

In this section, we discuss some of the most important watermarking applications, including owner identification, proof of ownership, data authentication, access control, copy control, broadcast monitoring as well as fingerprinting. These potential applications can be categorized in several ways. The classification is generally performed based on the nature of the information revealed by the watermark [19, 20]. The applications can therefore be classified as follows:

- Copyright Control: In this class, a watermark is embedded in order to carry information related to content ownership. It encompasses the following primary types of applications: owner identification, proof of ownership, copy control and fingerprinting.

- Content Validation: A watermark is exploited in this case to detect any tampering that could have been performed on the original multimedia content. It encompasses several types of applications, including data authentication.

- Information Hiding: In this class, a watermark is exploited as a side channel to convey addition information. It is generally applied in applications such as broadcast monitoring and device control.

1.2.1 Owner Identification

Owner identification is typically achieved using a copyright notice of the form "Copyright date owner" (or "© date owner"), and "℗ date owner" for visual works and phonorecords embodying a sound recording, respectively [1]. However, a textual copyright notice has several drawbacks for identifying copyright ownership. The most obvious disadvantage is the ease to intentionally or unintentionally remove the visible copyright notice. Hence, embedding an imperceptible and robust watermark is likely to be far more superior for owner identification than a visible textual copyright notice. Furthermore, the embedded watermark can be easily extracted from a digital content, whether audio, video or images, to identify the corresponding copyright owner. This is made possible by providing a user with a simple watermark detector.

1.2.2 Proof of Ownership

A watermark can also convey certain information in order to not only identify the copyright ownership but to also prove the ownership. In this case, a textual notice is irrelevant as it can easily be forged by an adversary. This technique is commonly considered to resolve a dispute between an adversary that steals or attempts to forge a digital content to claim ownership and the legal owner of the original work. However, in such a scenario, proof of ownership using watermarks can prove to be rather unreliable, making digital watermarking a technology that is currently undependable to prove ownership in a court of law. This is due to several reasons introduced in [1], where one significant problem is the wide availability of watermark detectors to adversaries.

[1] Under Canadian and U.S. law, a copyright protection is automatically granted upon the creation of a work. The copyright symbol is used as a reminder to the public that copyright exists in the work. It may also serve for protection in other countries [21]

1.2.3 Data Authentication

The wide range of sophisticated multimedia editing software tools currently available in the high-tech market has made it easy to tamper with digital works. In consequence, the detection of digital tampering has become a difficult and complicated task, which in turn led to the desperate need of data authentication in order to validate the authenticity of the digital content. A cryptographic approach can be exploited in order to answer this problem, where a summary of the digital content is created and assembled into a *digital signature*. In the case where the digital work is tampered with, the digital signature will be modified, revealing that some sort of digital tampering has taken place. Digital signatures are undesirable in certain cases as the information must always be transmitted with the original digital data, from which it was created [1]. A more popular and often the preferred approach, is to embed a watermark in the digital data, that is designed in such a manner to become invalid with the slightest modification of the work. These type of watermarks are referred to as *fragile watermarks*. In the case where small modifications to the work are tolerated, *semi-fragile watermarks* are used.

1.2.4 Broadcast Monitoring

Broadcast monitoring is generally performed in order to reliably confirm that a transmission over a television network or another medium has occurred. There are various techniques to achieve this, some less automated than others. A less automated approach would be to hire human observers to watch the broadcast content and collect the necessary information. This method is however costly as well as inefficient as it is prone to errors. Conversely, automated approaches can be taken, and they are divided into two different categories: passive and active. Passive systems rely on a computer system that monitors broadcasts and then compares the monitored content with a set of works stored in a database. A potential problem of such an approach is the complexity involved to perform such non-trivial

comparisons. Active monitoring on the other hand introduces additional information to the original broadcast content in order to identify the transmitted work. It can be performed using watermarking techniques, where the watermark is created such that it encompasses information related to the broadcast content. It is then inserted in the actual broadcast work in order to identify the transmitted content when necessary.

1.2.5 Fingerprinting

Fingerprinting (also known as transaction tracking), is a watermarking application in which a different watermark is placed in each copy of the work in order to record and identify each legal recipient. In the case where the work is misused or illegally redistributed, the owner can then trace and identify the person responsible. An example of watermarking for fingerprinting is in the distribution of movie dailies, which is often achieved in Hollywood movie studios. If a daily is leaked to the press, a studio can easily track the source and identify the adversary [1].

1.2.6 Copy Control

Digital watermarking can also be used for copy control, generally achieved to prevent illegal action, such as copying or recording copyrighted material. Furthermore, watermark insertion can prove to outperform traditional techniques (used to prevent illegal copying) such as encryption, as a watermark is inserted within the digital content of the work, and it is therefore present in the entire representation of the work. In the ideal scenario, every recording device should encompass a watermark detector in order to forbid recording whenever a *copying-prohibited* watermark is detected. However, copy control mechanisms based on watermarking schemes are not widely used due to a nontechnical problem: most recorder manufacturers do not include watermark detectors in their recording devices, as it seems to increase the manufacturing price and reduce the demand. The reduction in demand is

mainly due to the fact that customers prefer recording devices with which they can produce illegal copies. An obvious solution to this problem would be to enforce a law that would oblige recorder manufacturers to include watermark detectors in their recording devices.

1.2.7 Device Control

Device control (also known as legacy system enhancement), similarly to copy control, is used in various applications where a watermark is embedded in a device to convey or transmit certain information. However, unlike copy control, it plays a valuable role as it enhances the functionality of a device rather than reduce its value and restrict its use. An example of an device control application is Digimarc's MediaBridge system [22], which essentially inserts a watermark into printed media, such as magazine advertisements. The digital content is then recollected using a digital camera or a scanner, and the watermark is extracted to link the data with an associated web site.

1.3 Importance of Human Perceptual Models

In digital watermarking, watermarks embedded in cover works are supposed to be imperceptible and robust. This raises two significant questions. First, how does one embed a watermark in such a manner that it cannot be perceived by the human eye? Second, how is it possible to assess whether distortions introduced by inserting a watermark are perceptible. This is certainly a non-trivial task. However, the imperceptibility of a watermark should not be evaluated using a rigid true or false approach, since the perceptibility of visual distortions is greatly dependent on the perceptual abilities of an observer. This section discusses some of the most important experimental procedures for measuring watermark imperceptibility. These techniques are divided into two categories, where one relies on subjective and rigorous methods involving human observers, whereas the other follows an automated algorithmic approach which essentially computes a measure of the perceptual distances be-

tween watermarked and unwatermarked works. Furthermore, this section also introduces various techniques used to exploit human visual models to perform adaptive, imperceptible and robust watermarking.

1.3.1 Evaluating Watermark Imperceptibility

The imperceptibility criterion can be described using two slightly different types of perceptibility measures: *fidelity* or *quality*. Fidelity consists of a similarity measure between the original signal and the processed signal (i.e. the original work and the watermarked work). A reproduction of the original work is assigned a high-fidelity measure if it is almost identical to the original. Conversely, a reproduction of the original work is assigned a low-fidelity measure if it is distinct from the original. Quality, however, is a measure of the degree of acceptability (or appeal) of the reproduced or watermarked work. Fidelity and quality are both considered when designing a watermarking system. However, quality is the most important measure of perceptibility in the case when a recipient of a watermarked work does not have access to the original work. Conversely, when the recipient has access to the original work, fidelity is in this case the primary focus when designing the watermarking algorithm as the watermarked work must be undistinguishable from the original work. A method that is rarely used when evaluating both types of perceptibility measures involves human observers. It is evident that different observers will have distinct perceptual abilities and will consequently perceive visual discrepancies differently. The *Just Noticeable Difference* (JND) is a type of measure for evaluating the level of distortion that can be perceived in one-half (or 50%) of experimental trials. An example for measuring perceptual variations is the *two alternative, forced choice* (2AFC) [23]. In this method, an observer is presented with two versions of a work: the original and the watermarked. The observer, uninformed about the distinctions between the works, must choose the work with the higher quality. A statistical analysis is normally performed in order to determine whether the watermark is

imperceptible. For example, if the watermarked work is significantly similar to the original work, 50% of the observers will choose the original image to have the higher quality, and the remaining 50% of the observers will choose the watermarked image to have the higher quality. This result, where 50% of the observers are correct, generally corresponds to zero JND.

Another more general approach, commonly used to measure the quality, provides the observers with more freedom in their choice of answers when examining a work. Rather than simply stating which work has the higher quality, observers are requested to rate the quality of the work under test. An example of such a scheme is based on the ITU-R Rec.500, which defines a five-grade quality scale going from "excellent" to "bad" and a five-grade impairment scale going from "imperceptible" to "very annoying". This technique is commonly used to evaluate the quality of a television picture [24], and has also been investigated in the evaluation of image watermarking [25].

Although all of the techniques presented up to this point rely entirely on human observers, they can prove to demonstrate accurate results when evaluating the fidelity and/or the quality of a work. However, they suffer from several drawbacks such as: they can be very expensive, the observations cannot be repeated in most cases as different observers behave differently, and probably the most important reason, the tests cannot be automated. An alternative automated approach relies on human perceptual models to measure fidelity. Generally, a perceptual model is used to compute an estimate of the perceptual distances between the watermarked and unwatermarked works. An example of such a technique was proposed by Watson [26]. It consists of a human visual system used to provide an estimate of the perceptual characteristics of all 8×8 blocks of an image. These estimates are then gathered and used to compute a single estimate of the perceptual distance, $D_{wat}(c_0, c_w)$, where c_0 is an original image, and c_w is the watermarked version of c_0. This visual model encompasses a frequency sensitivity table, two masking components based on luminance and

contrast masking, as well as a pooling function used to compute the perceptual distance. However, humans visual systems are rather complex to model, and their resulting perceptual distance measures so far provided do not demonstrate a more precise advantage over simpler techniques [27].

A simple technique to measure the perceptual distance is the mean square error (MSE) function defined as:

$$D_{mse}(c_o, c_w) = \frac{1}{N}\sum_{i}^{N}(c_w[i] - c_0[i])^2 \tag{1.1}$$

However, MSE is rarely used when an accurate perceptual evaluation of a watermarking system is required as it can easily underestimate or overestimate the perceptual distance between two works [28, 29]. The most widely used distortion measures in digital watermarking are the Signal to Noise Ratio (SNR) and the Peak Signal to Noise Ratio (PSNR) which are defined as follows:

$$D_{SNR}(c_o, c_w) = \sum_{i}^{N} c_0^2[i] / \sum_{i}^{N}(c_w[i] - c_0[i])^2 \tag{1.2}$$

$$D_{PSNR}(c_o, c_w) = 10 \cdot \log_{10}\left(\max_{N} c_0^2[i] / D_{mse}(c_o, c_w)\right) \tag{1.3}$$

These distortion measures are popular due to their simplicity, however their primary drawback is their inability to properly model human vision. In consequence, high fidelity is not guarantied if a small distance is obtained when computing the difference between the original and watermarked works.

1.3.2 Watermarking using Human Visual Models

Watermarking systems often use the information about the cover work in order to improve the watermark embedding performance. This type of watermarking also referred to as watermarking with informed embedding is very desirable as it can yield perfect effectiveness

(zero false negative rate). In image watermarking, effective informed embedding is generally achieved by taking advantage of the characteristics of human visual models. These models are used to perform imperceptible and robust watermarking by taking advantage of the perceptual characteristics of the image. Moreover, some of the simplest perceptual model based watermarking techniques perform the watermark insertion in the perceptually least significant components of the image in order to minimize the possible degradation of the original work and in turn enable transparent watermarking. In other words, a watermark with a low signal amplitude is selected and it is embedded into the low-order components of the image. However, watermarks embedded in this fashion are significantly ineffective as they can be easily removed or altered through basic signal processing or geometric attacks. This issue has motivated the use of sophisticated visual models to perform robust and transparent watermarking.

A significant amount of research has been achieved in the literature to model human visual systems (HVS) and to understand their response to frequency and luminance variations. Visual models encompass three types of frequency response: spatial frequencies, spectral frequencies and temporal frequencies. Spatial frequencies are commonly perceived as patterns or textures, whereas spatial frequency sensitivity is the eye's sensitivity to changes in luminance. Moreover, the human eye is most sensitive to luminance variations at mid-range frequencies and the sensitivity declines at lower and higher frequencies. Furthermore, the eye sensitivity is also affected by the orientation of different patterns, as it is very sensitive to lines and edges with horizontal or vertical orientations, and it is less sensitive to lines and edges with varying slopes [30, 31, 32]. Spectral frequencies on the other hand are perceived as colors, whereas temporal frequencies can be used to describe the eye's sensitivity to motion.

A variety of image watermarking techniques have been suggested where the frequency sensitivity of human visual models is investigated in order to guaranty the imperceptibility of the watermark. Most of these proposals use frequency domain techniques such as DCT, DFT

and DWT, and add the watermark into the transformed components of the image. More sophisticated and refined techniques have also been introduced which take full advantage of the HVS characteristics including its sensitivity to luminance and texture variations as well as other masking capabilities, which are used to hide or mask a signal with the presence of another. Human visual models with such characteristics have primarily been used to perform image-adaptive watermarking. This technique relies on an HVS to adjust the watermark embedding strength in different areas of an image while maintaining a fixed fidelity. This is a challenging task since by increasing the embedding strength, the robustness of the system will also increase at the cost of increasing the embedding distortion resulting in a more perceptible watermark, which in turn causes a loss of fidelity. Therefore the HVS is exploited to control the tradeoff between watermark robustness and its imperceptibility. Moreover, the ultimate goal is to perform image adaptive watermarking by maximizing the energy of the watermark signal in different areas of the work, without increasing the perceptible degradation of the watermarked image.

1.4 Basics of Fuzzy Theory

Fuzzy theory relies on mathematical concepts to define what is called *fuzziness*, a notion which reveals the aspect of uncertainty. Fuzziness generally refers to the ambiguity that is commonly found in our daily linguistic expressions, such as "tall person", "low temperature" and "old person". Up until recently, probability theory had been the only mathematical approach to provide an approximate measure of uncertainty [33]. However, probability provides a measure of the degree of certainty based on the occurrence of an event. Conversely, fuzziness expresses a much more common measure of uncertainty as it attempts to mimic human thinking and intelligence. The most general terms of fuzzy theory are fuzzy set theory and fuzzy logic. Both rely on the concept of fuzziness, however fuzzy set theory introduces fuzziness in a specific manner as it exploits the concept of sets, whereas fuzzy

logic extends fuzzy sets and incorporates it into a framework of multivalued logic. The applications of fuzzy logic and fuzzy set theory has expanded to various areas such as signal analysis and interpretation, controls applications, as well as in research related to scheduling and optimization. Refer to [34, 35, 36, 37, 38] for additional applications. In this section, a concise introduction of fuzzy sets is first provided and it is compared to traditional classical (crip) sets. A general description of membership functions and linguistic variables is then presented. Lastly, fuzzy if-then rules are illustrated along with a brief introduction of fuzzy reasoning.

1.4.1 Fuzzy Sets

A fuzzy set is defined as a generalization of a classical set (also known as a crisp set or standard set). The former is a set without a fix boundary whereas the latter is a set with a clearly defined boundary whose membership function only takes on two values, zero and unity. Moreover, fuzzy sets are generally used when a gradual transition from "belonging to a set" to "not belonging to a set" is required. This smooth transition is characterized by membership functions used to provide fuzzy sets the flexibility required to model commonly known linguistic expressions, such as "the water is cold" or "the temperature is low". Moreover, a membership function provides a basic measure of the degree of likeliness or similarity (also known as the *extent* or *grade*) of a fuzzy set to an element in the universe of discourse. The universe of discourse is the range in a continuous space, of all possible values for an input to a fuzzy system. Also, membership functions are defined in greater detail in the next subsection. Furthermore, a fuzzy set A in universe of discourse U is defined as a set of ordered pairs of a generic object x and its corresponding membership function grade, as follows:

$$A = \{(x, \mu_A(x)) \mid x \in U\} \tag{1.4}$$

where the membership function $\mu_A(x)$ associates each element x in U to a membership grade (or a degree of membership) in the range [0,1]. In order to clearly illustrate how a fuzzy set can be specified using a membership function, let's consider the often unclear observations or opinions when dealing with the height of human beings. Height of humans can be viewed differently from different perspectives. For example, height may vary by culture or age. A person that's considered tall in one culture might be perceived as average or short in another. The fuzziness of different perspectives is therefore evident as the opinions of different people from varying backgrounds, cultures or age groups may differ significantly. Consequently, this can be illustrated as in Fig. 1.3, where $U = Height(cm)$, and the fuzzy sets are "Short", "Average" or "Tall" that are characterized by membership functions $\mu_{Short}(x)$, $\mu_{Average}(x)$ and $\mu_{Tall}(x)$, respectively.

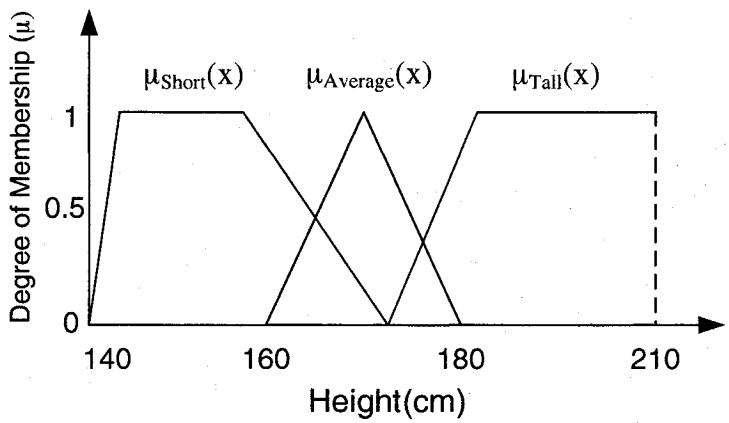


Figure 1.3: Membership functions of the fuzzy sets in which people are considered "Short", "Average" or "Tall".

It can be seen from Fig. 1.3 that there are two basic attributes that control the fuzzy sets. First, the horizontal axes which represents the universe of discourse which corresponds to the entire set U and it is usually called the support set of the fuzzy set, or simply the support. Furthermore, the vertical axis, is the membership function, with which the degree of membership can be depicted for each element [33]. For example, the membership

function $\mu_{Average}(x)$ would typically be interpreted as the age value around the middle, however, the grade of about 160 cm or 180 cm can vary subjectively depending on each person's perspective. Fuzzy sets are therefore seen as being subjective, as opposed to the aforementioned classical sets which are very objective.

1.4.2 Fuzzy Membership Functions

As aforementioned, a fuzzy set is uniquely characterized by its membership function (MF). Furthermore, a MF μ provides a membership grade between zero and one that defines the degree to which an element x of a set X (or of the universe of discourse U) is included in this subset. Membership functions can be associated with various shapes, the most commonly used shapes however are triangular, trapezoidal and Gaussian. In order to define a MF in a concise manner, a mathematical approach is often used. A triangular MF can be defined using three parameters a,b,c as follows:

$$triangle(x; a, b, c) = \begin{cases} 0, & x \leq a, \\ \dfrac{x-a}{b-a}, & a \leq x \leq b, \\ \dfrac{c-x}{c-b}, & b \leq x \leq c, \\ 0, & c \leq x. \end{cases} \tag{1.5}$$

where the parameters a, b and c specify the horizontal x coordinates of all three corners of the triangular MF. In Fig. 1.4(a), an example of a triangular MF is shown were the coordinates a, b and c are set to 0, 30 and 60, respectively.

Furthermore, a trapezoidal MF can be defined using four parameters a,b,c and d as follows:

$$trapezoid(x; a, b, c, d) = \begin{cases} 0, & x \leq a, \\ \dfrac{x-a}{b-a}, & a \leq x \leq b, \\ a, & b \leq x \leq c, \\ \dfrac{d-x}{d-c}, & c \leq x \leq d, \\ 0, & d \leq x. \end{cases} \tag{1.6}$$

the parameters a,b, c and d specify the horizontal x coordinates of all four corners of the trapezoidal MF. In Fig. 1.4(b) an example of a trapezoidal MF is shown were the coordinates a, b, c, and d are set to 0, 5, 30 and 60, respectively. Triangular MFs and trapezoidal MFs are extensively used in various engineering applications due to their simple mathematical representation and their computational efficiency. However, because the MFs are created using linear segments, they don't offer a smooth representation of the degree of membership at the corner points specified by the parameters [39]. In addition, a Gaussian MF can be specified with only two parameters c, and σ as it is shown below:

$$gaussian(x; c, \sigma) = e^{-\frac{1}{2}\left(\frac{x-c}{\sigma}\right)^2}, \tag{1.7}$$

where c denotes the MF's center and σ represents the MF's width. In Fig. 1.4(c) an example of a Gaussian MF is shown were the coordinates c and σ are set to 30 and 10, respectively. Gaussian MFs have become significantly popular for specifying a fuzzy set. This is due to their immense use in probability and statistics. Although Gaussian MFs can achieve tremendous smoothness, they are incapable of defining asymmetric MFs which are of great relevance in various applications. Asymmetric MFs can be specified using sigmoidal functions as it is shown in [39]. Sigmoidal MFs will not be discussed as they are beyond the scope of this thesis.

The choice of the shape of a membership function is commonly done arbitrarily by a fuzzy system designer. However, in more recent fuzzy logic research, membership functions have been developed using optimization procedures [40, 41, 42, 43]. The number of membership functions depends on the application and the user. However, a tradeoff exists between efficiency and computational complexity when specifying the number of membership functions.

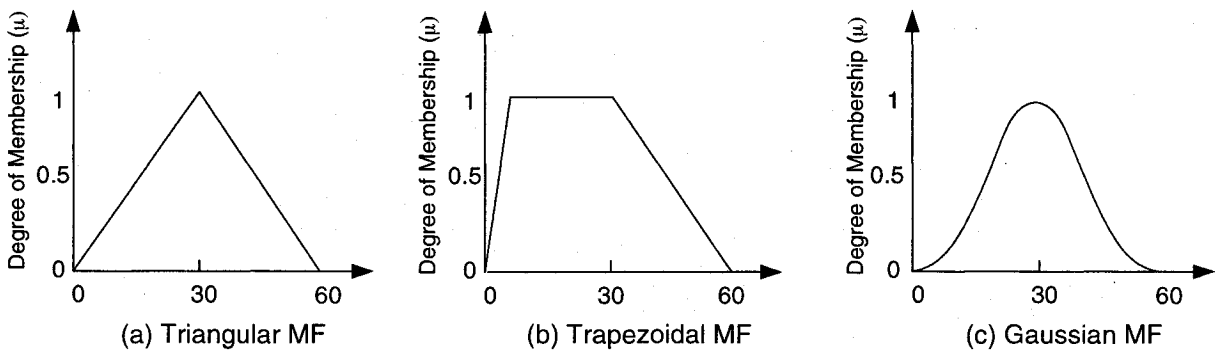


Figure 1.4: Examples of three classes of MFs: (a) Triangular MF, (b) Trapezoidal MF, (c) Gaussian MF.

1.4.3 Linguistic Variables

Linguistic variables were introduced as an alternative approach to represent and model human reasoning. In [44], Zadeh states the following: "In retreating from precision in the face of overpowering complexity, it is natural to explore the use of what might be called *linguistic variables*, that is, variables whose values are not numbers but words or sentences in a natural or artificial language". This approach which is based on linguistic characterization is used to summarize and express human thinking in terms of fuzzy sets rather than crisp numbers which rely on a numerical characterization. A linguistic variable can be specified using the following terms: x, $T(x), U$, G and $M(s)$ [39]. The term x corresponds to the name of the linguistic variable, $T(x)$ is the set of linguistic terms or linguistic values of x which cover the universe of discourse U, it is also known as the term set of x, G denotes a syntactic rule used to generate the terms in $T(x)$, and $M(s)$ is a semantic rule which described a linguistic value s.

Fig. 1.5 illustrates the use of linguistic variables and linguistic values and their association with fuzzy sets. The universe of discourse U is often associated with the linguistic variable. In this particular case U = "Grade". The linguistic variable *Grade* is partitioned into various fuzzy sets whose MFs cover the continuous space U. The term set $T(Grade)$ is as follows:

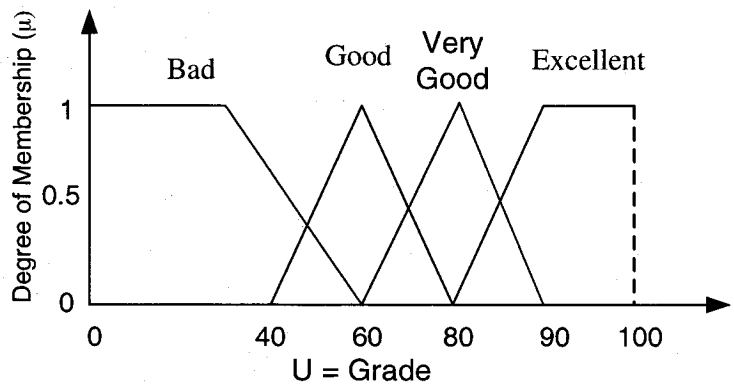


Figure 1.5: Membership functions of the fuzzy sets in which *Grade* is the linguistic variable and "Bad", "Good", "Very Good" and "Excellent" are the linguistic values.

$$T(Grade) = \{\text{“}Bad\text{”},\ \text{“}Good\text{”},\ \text{“}Very\ Good\text{”}\ and\ \text{“}Excellent\text{”}.\}, \tag{1.8}$$

where each term in *T(Grade)* is characterized by a fuzzy set of a universe of discourse U = [0,100]. In addition, the words "Bad", "Good", "Very Good" and "Excellent" correspond to the linguistic values of the linguistic variable *Grade*. The syntactic rule in this case refers to the approach taken to generated the linguistic values in *T(Grade)*, whereas the semantic rule specifies the MF associated with each linguistic value of the term set *T(Grade)*.

1.4.4 Fuzzy Rules and Fuzzy Reasoning

A fuzzy rule (also called a fuzzy implication or a fuzzy conditional statement) is a general proposition that is divided into a left hand side and a right hand side, where the left hand side encompasses a set of conditions linked together through logical operators and the right hand side contains the fuzzy end result. In consequence, fuzzy rules generally take the following if-then form:

$$if\ x\ is\ A\ then\ y\ is\ B, \tag{1.9}$$

where A and B are linguistic values specified by fuzzy sets, whereas x and y are input values contained within the universe of discourses X and Y, respectively. The left hand side of the if-then rule is commonly called the antecedent or premise, while the right hand side is called the consequence or conclusion. Examples of if-then rules are very common in our daily expressions, such as the following:

- if the service is good, then the tip is generous.
- if the temperature is cold, then the heater is on low.
- if the snow is melting, then the temperature is high.
- if the coffee is very hot, then don't drink it.

Fuzzy reasoning (also known as approximate reasoning) is an inference technique that relies on fuzzy if-then rules and already known information in order to derive appropriate conclusions. A fuzzy *modus ponens* is a basic rule of inference based on two-valued logic of which binary modus ponens is a special case. For example, let's consider the case where A and B are linguistic values and they are associated with "the temperature is cold" and "the heater is on low", respectively. Let's consider the following fuzzy reasoning,

$$\begin{array}{ll} \text{premise 1 (rule):} & \text{if x is A then y is B} \\ \text{premise 2 (fact):} & \text{x is A'} \\ \hline \text{conclusion} & \text{y is B'.} \end{array}$$

where x and y are elements and A, A' and B, B' are fuzzy sets in the universe of discourses X, X and Y, Y, respectively. Consequently, if "the temperature is *very* cold", it is also true that "the heater is on *very* low". Fuzzy reasoning and fuzzy rules involving multiple antecedents will be discussed in further details in Chapter 3.

1.5 Contributions of Thesis

The contributions of the thesis are summarized as follows:

- A Dynamic Membership Function Engine (DMFE) is introduced that relies on the statistical distributions of the input data set to accurately adapt a membership function for any nonlinear input/output mapping.

- A Dynamic Fuzzy Inference System (DFIS) model is depicted which incorporates the aforementioned DMFE and takes on HVS-generated data as inputs to accurately approximate the relationship found between all properties of a human perceptual system.

- The dynamic fuzzy logic scheme is exploited to provide a novel method to compute the maximum possible watermark length that can be inserted in a cover image without introducing visual degradation. Moreover, this logic is also used to determine the adaptive watermark strength for each pixel in the cover image.

- A novel *predictive watermark embedding* (PWE) technique is also presented. It relies on the average power of the DCT coefficients in order to provide an accurate estimate of the embedding regions in which the watermark insertion should be performed.

- An automated test-bench is developed that relies on an exhaustive testing scheme to generate a robust watermark that meets the desired user-specifications.

The presented work has been published in [45, 46]. However, in [45], a simplified version of the proposed dynamic fuzzy logic scheme was introduced, and a binary watermark was exploited instead of a real-valued sequence.

1.6 Outline of Thesis

In this chapter a brief introduction of certain concepts in digital watermarking and fuzzy theory was provided in order to equip the reader with the basic background knowledge required to understand the thesis topic. The remainder of the thesis is organized as follows. In Chapter 2, a literature review of several image watermarking schemes is provided in order

to familiarize the reader with previous works that dealt with spread spectrum techniques, HVS-based watermarking as well as the application of fuzzy logic to perceptual watermarking. In Chapter 3, the adaptive behavior of the proposed technique is then described using a dynamic fuzzy inference system and a visual model. In Chapter 4, the proposed watermarking scheme is depicted. In Chapter 5, the experimental results are presented to prove the robustness and the imperceptibility of the generated watermark. Finally, in Chapter 6, concluding remarks are provided and possible extensions and improvements to the proposed method are also discussed.

1.7 Summary

This chapter has discussed the background information necessary for an adequate understanding of this thesis. A generic watermarking system which essentially incorporates a watermark embedder and a detector was first presented along with a brief introduction to spatial and frequency domain watermarking. It was mentioned that the robustness and the imperceptibility of the watermark is essential for a well-designed watermarking system. In addition, several possible applications of watermarking have been discussed and they were classified into three categories: copyright control, content validation and information hiding. The imperceptibility criterion was discussed and its association with human perceptual models. Finally, a concise description of fuzzy theory was presented, in which we defined fuzziness as a common measure of uncertainty as it attempts to mimic human thinking.

Chapter 2

Literature Review

The goal of this chapter is to familiarize the readers with several image watermarking schemes that have been suggested in literature during the past few years. The proposed approach extends some of these techniques in many ways as it will be discussed in Chapters 3 and 4.

This chapter begins with a concise introduction to spread spectrum techniques and its applications to digital watermarking (Section 2.1). Section 2.2 describes several important schemes that perform perceptual image watermarking using visual models. Finally, Section 2.3 gives a brief description of some of the most recent watermarking techniques that rely on fuzzy logic schemes to perform adaptive image watermarking.

2.1 Spread Spectrum Watermarking Techniques

Spread spectrum watermarking was suggested by Cox et al. in [8, 9]. This method is analogous to spread spectrum radio communications, a technology used by the military in order to resist against jamming and interference. This technique is characterized by a narrow band signal that is distributed (or *spread*) over a much wider band of frequencies. The process used to spread the signal is kept confidential and known only by the transmitter and the receiver [1]. Spread-spectrum communication theory was found to be an appropriate technique for watermarking as it enables the watermark signal to be spread with a low amplitude but in a wide enough spectrum to hold sufficient signal energy for it to be detected.

The spread spectrum based digital watermarking technique was initially introduced in [8]. Their scheme was primarily for image watermarking, however, with minor modifications, it could be extended to secure audio, video and other media. It relies on embedding an independent identically distributed watermark that consists of random numbers that follow a Gaussian distribution according to *N(0,1)* (where $N(\mu, \sigma^2)$ corresponds to a normal distribution with mean μ and variance σ^2). They argue that a watermark should be inserted in a spread-spectrum-like fashion into the perceptually most significant components of the data. In addition, they illustrate the watermark insertion process as follows:

$$V_i' = V_i + \alpha w_i \tag{2.1}$$

$$V_i' = V_i(1 + \alpha w_i) \tag{2.2}$$

$$V_i' = V_i(e^{\alpha w_i}), \tag{2.3}$$

where V_i denotes the selected coefficients into which the watermark $W = w_1, \ldots, w_n$ is inserted in order to produce the watermarked work $V' = V_1', \ldots, V_n'$. Furthermore, the parameter α denotes the watermarking strength. It is evident that Equ. (2.1) is always invertible, whereas Equ. (2.2) and (2.3) are invertible if $V_i \neq 0$. However, Equ. (2.1) may not be appropriate when the V_i coefficients vary significantly. Conversely, watermark insertion methods based on Equ. (2.2) and (2.3) proved to be more robust against strong variations in V_i. However, this scheme does not rely on a human perceptual system in order to identify the perceptually significant components of an image. The watermark insertion is performed into the coefficients of the transform matrix with the highest magnitude. This does not guarantee that the watermark will be placed in the low-frequency components of the image. Thus, for certain images, the algorithm may prove to be vulnerable against signal processing attacks, such as low-pass filtering and lossy compression as well as geometric

attacks such as image scaling. In addition, the selection of adaptive watermarking strength and watermark length parameters were not discussed, as constant values were used.

Although spread spectrum based watermarking has been exploited for almost a decade now, it remains a popular technique to perform digital watermarking of images [47, 48], audio [49, 50] and video [51, 52]. In the next subsections, a concise introduction of several spread spectrum based techniques will be provided, in which it is illustrated how this approach can be improved using accurate human perceptual systems.

2.2 HVS-based Watermarking Techniques

As aforementioned, perceptual watermarking schemes take advantage of the characteristics of a human perceptual system in order to modify the information without causing perceptible changes in the original work. The applications of such HVS models to image watermarking has been proposed by various authors.

In [10], Huang and Shi propose an adaptive image watermarking algorithm based on a HVS model which incorporates both luminance and texture masking. This scheme relies on a block classification method in order to adaptively set the watermarking strength applied to different 8×8 blocks of an image during the watermark insertion process. The blocks are classified into three classes: dark and weak texture (class 1), bright and strong texture (class 2), and other conditions (class 3), where each class is assigned a specific watermarking strength value. The embedding process is achieved in the DCT domain as follows:

$$V'_k(x,y) = V_k(x,y) + \alpha_k w_i, \tag{2.4}$$

where $3k \leq i < 3(k+1)$ and $(x,y)\ \epsilon\ \{(0,1),(1,0),(1,1)\}$. Also, α_k is the adaptive watermarking strength for the k'th 8×8 block of the image. There are several drawbacks to this scheme. The most important is that the block classification method does not take full advantage of the HVS as the watermarking strength components can only be set to three possible

values. Furthermore, the embedding is limited to the first three low-frequency AC components in each block. This does not ensure that the watermark insertion will be performed in high magnitude DCT coefficients, which could result in watermarked images with low Peak Signal to Noise Ratio (PSNR) and little resilience to signal processing and geometric attacks.

In [53], Podilchuk and Zeng propose an image-adaptive watermarking scheme in which they exploit visual models commonly used in image compression techniques. The perceptually based watermarking method can be performed in both the DCT or DWT frequency domains. Their approach relies on Watson's visual model [26] that take into account the frequency sensitivity, the local luminance sensitivity as well as contrast masking. Their watermark is defined as a sequence $w = w_1, w_2, \cdots, w_{n_I}$ that is generated from a normal distribution with zero mean and unit variance, where n_I corresponds to the length of the watermark for an image I determined by their visual model. The DCT domain based watermark embedder is defined as follows:

$$V'_{x,y,k} = \begin{cases} V_{x,y,k} + t^C_{x,y,k} w_{x,y,k}, & if\ V_{x,y,k} > t^C_{x,y,k}, \\ V_{x,y,k}, & otherwise. \end{cases} \tag{2.5}$$

where $V_{x,y,k}$ denotes the DCT coefficients, $V'_{x,y,k}$ refers to the watermarked DCT coefficients, $w_{x,y,k}$ is the adaptive watermarking strength, and $t^C_{x,y,k}$ is the contrast masking threshold that defines the *Just Noticeable Difference* (JND) and it is described as,

$$t^C_{x,y,k} = [t^L_{x,y,k}, |V_{x,y,k}|^{w_{x,y}} (t^L_{x,y,k})^{1-w_{x,y}}], \tag{2.6}$$

where $t^L_{x,y,k}$ is the local luminance masking, $w_{x,y}$ is a number between one and zero and may be different for each frequency coefficient. In their scheme, $w_{x,y} = 0.7$. The primary weakness of this method is the approach taken when performing the watermark insertion. First, they do not limit the watermark insertion to only the perceptually significant parts of the image. In addition, their method generates significantly weak image-adaptable watermarks when the characteristics of the original images are fairly uniform. Furthermore, the JND threshold for

each DCT coefficient is generated independently of the other coefficients in the same block k. This in turn demonstrates that their visual model is not accurate and does not adapt to the local characteristics of each block of an image.

Podilchuk and Zeng's scheme was however extended in [54] by Suthaharan et al., where the HVS was improved using an entropy masking model which takes into account the excitatory-inhibitory interaction between pixels. In addition, they exploit a bounded normally distributed watermark in order to avoid any degradation of the watermarked image that could be due to pixel values exceeding the JND threshold.

2.3 Image Watermarking using Fuzzy Logic

As aforementioned, fuzzy logic techniques have been used in a wide range of applications, including digital image and signal processing, computer vision as well as control systems. However, fuzzy theory has been scarcely investigated in the field of digital watermarking. Only recently, basic fuzzy logic approaches have been examined a little in the literature to perform efficient perceptual watermarking.

In [7], Wu and Xie propose an image watermarking technique that relies on a fuzzy clustering algorithm and a human visual system to adapt the watermarking strength with respect to the original image. The adaptive strength for each block is determined using a fuzzy c-means (FCM) algorithm, as follows:

$$\alpha_k = FCM(f_k), \tag{2.7}$$

where f_k is a feature vector that serves as an input to the FCM algorithm and it is computed based on the brightness and texture sensitivities extracted from the image using the visual model. FCM is a data clustering technique used to map each data input to a cluster depending on some degree that is specified by a membership grade. Furthermore, The watermark insertion is performed in high magnitude DCT coefficients of selected 8×8 blocks. The em-

bedding is however limited to the middle frequency range of the image, which restricts the size of the watermark and its robustness against signal processing attacks, such as low-pass filtering. The embedding process is described as,

$$V'_{x,y,k} = V_{x,y,k}(1 + \beta \cdot \alpha_k \cdot w_{x,y,k}), \tag{2.8}$$

where α_k is the adaptive strength for a selected block k, and β is a scaling factor. Furthermore, binary watermarks are used in this scheme, making it less resistant to tampering attacks, such as collusion. Moreover, this method does not consider the maximum possible length of the watermark, and the watermarking strength α is computed for every block, rather than for each pixel. In addition, clustering algorithms are computationally intensive, making them impractical for real-time applications, such a real-time digital watermarking.

In [6], Lou and Yin propose an adaptive watermarking algorithm based on fuzzy logic techniques. This scheme is similar to our own proposal as it introduces a Fuzzy Inference System (FIS) to extract the human knowledge using a HVS. Their HVS model encompasses four different properties: luminance sensitivity, texture sensitivity, entropy sensitivity as well as frequency sensitivity. Furthermore, the fuzzy logic approach is used in order to determine the different strengths and lengths of a watermark based on the local characteristics of a specific image. Their watermark insertion process is performed as follows,

$$V'_{x,y,k} = V_{x,y,k}(1 + \alpha_{x,y,k} w_{x,y,k}), \quad \text{for} \quad r(x,y) = R_{n_k}, \tag{2.9}$$

where $\alpha_{x,y,k}$ is the adaptive strength of watermark $w_{x,y,k}$ of the k'th 8×8 block of the original image, whereas R_{n_k} consists of the n coefficients selected when inserting the watermark in the k'th block. It is described as follows:

$$R_{n_k} = \{r_k(1,2)_1, r_k(2,1)_2, r_k(3,1)_3, r_k(2,2)_4, r_k(1,3)_5, r_k(1,4)_6\} \quad (2.10)$$

However, this scheme relies on a static FIS model, resulting in a poor representation of the relationship found between the visual characteristics of certain images (such as brightness and texture). In addition, similarly to Huang and Shi's method, this scheme presents an important drawback in the watermark insertion process. Although the watermark insertion is performed adaptively in the low-frequency range of the image, the high magnitude DCT coefficients are not considered. As aforementioned, this can significantly impact the robustness and the imperceptibility of the watermark.

In the undertaken system, we make use of a simplified human perceptual system and we demonstrate that an accurate modeling of a fuzzy inference system and its fuzzy membership functions can smoothly represent the relationship found between the properties of a HVS model. Moreover, the watermarking strength values are accurately determined even when the characterized of the cover image are quite uniform as it will be demonstrated in Chapter 5. In addition, we introduce an *predictive watermark embedding* (PWE) algorithm that exploits the aforementioned DFIS model in order to insure that the watermark insertion process is accurately performed in low-frequency and high magnitude DCT coefficients, while insuring that the watermark remains robust and imperceptible.

2.4 Summary

This chapter has presented several image watermarking schemes that can be classified into three categories: spread spectrum watermarking, HVS-based watermarking, and image watermarking using fuzzy logic.

First, spread spectrum watermarking was described and it is based on spread spectrum

communication theory. This technique enables a watermark signal to be spread with low amplitude but in a wide enough spectrum to hold sufficient signal energy for it to be detected. Furthermore, it was demonstrated that HVS have been widely used in watermarking systems in order to perform imperceptible watermarking without degrading the quality of the cover work. Finally, fuzzy logic has been investigated in the literature to perform efficient perceptual watermarking. It can better depict the local characteristics of the image, which in turn enables an improved approach to performing adaptive image watermarking.

Chapter 3

A Novel Approach to Refining Human Visual Models using a DFIS

The first two chapters of this thesis have discussed the field of image watermarking at a fairly general level. We believe that it is essential for the readers to be familiarized with digital watermarking and fuzzy logic techniques in order to understand and fully appreciate the proposed work. With the present chapter, we begin a detailed description of the novel image-adaptive watermarking technique. The proposed algorithm encompasses several independent modules that are interconnected to achieve a desired output.

The goal of this chapter is to introduce the readers to the primary components that enable the *adaptive* behavior of the watermarking algorithm. Section 3.1 describes the basic model of the human visual system exploited in the proposed scheme. A basic visual model (rather than a more sophisticated HVS) has been used in order to clearly demonstrate the perceptual improvements the suggested dynamic FIS can achieve. In Section 3.2, the DFIS model is introduced and a detailed description of its components is also provided. Although an attempt is made to generalize the DFIS architecture, the main focus is however on its application to image watermarking. Finally, in Sections 3.3 and 3.4, we illustrate how the DFIS is used in order to compute the adaptive watermarking strength and watermark length, respectively.

3.1 The Human Visual System

The HVS model used in this project was suggested in [26] and [55], and it employs the general form and breaks it up into three different properties that are used when generating the DFIS. This model is also used throughout the watermark embedding and detection schemes.

1. *Luminance sensitivity (L_k):* The brighter the background, the lower the visibility of the embedded signal. Therefore a longer and a stronger embedded signal can be used. The luminance sensitivity is estimated by the following formula:

$$L_k = \left(\frac{V_{DC,k}}{\overline{V}_{DC}} \right)^{\gamma}, \tag{3.1}$$

where $V_{DC,k}$ is the DC coefficient of the DCT of the k'th block, $\overline{V}_{DC}$ is the mean value of all $V_{DC,k}$ coefficients of a specific image, and γ is set to 0.649 to control the degree of luminance sensitivity.

2. *Texture sensitivity (T_k):* The stronger the texture, the lower the visibility of the embedded signal. Therefore a longer and a stronger embedded signal can be used. Texture sensitivity can be estimated by quantizing the DCT coefficients of an image V using the JPEG quantization table (Q). The result is then rounded to the nearest integers. The number of non-zero coefficients is then computed. This method can be estimated by the following formula:

$$T_k = \sum_{x,y=1}^{N} cond\left(\left[\frac{V_k(x,y)}{Q(x,y)} \right] \right), \tag{3.2}$$

where *cond(R)* takes the rounded value of R and returns '1' if the value is not equal to zero, '0' otherwise. Furthermore, *(x,y)* represents the location in the k'th block.

3. *Frequency sensitivity (F_k):* It can be defined as the response of a human visual system to variations in the frequencies of stimuli [1]. Moreover, according to the human perceptual system, the human eye is more sensitive to variations in low frequencies than it is to higher frequency components. In this model, the frequency sensitivity is represented by the luminance JPEG quantization table shown in Fig. 3.1.

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

Figure 3.1: Frequency sensitivity which corresponds to the JPEG quantization table.

3.2 The Dynamic Fuzzy Inference System Model

Fuzzy inference systems are widely used computing frameworks and they are based on concepts of fuzzy set theory, fuzzy if-then rules and fuzzy reasoning [39]. They are recognized to provide a simple fuzzy logic approach in order to perform the mapping from a given input to an output without the use of conventional mathematical models. The simplicity of the design procedure of such systems has made them a dominant attraction in a wide variety of fields such as automatic control, data classification, decision analysis, expert systems, and computer vision [56, 33, 57].

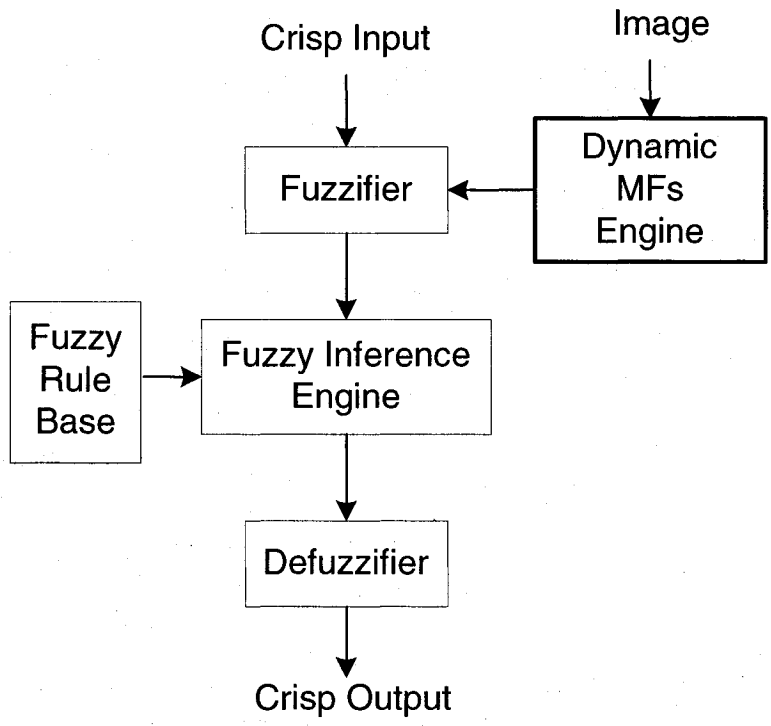


Figure 3.2: DFIS model

The proposed DFIS model is based on Mamdani's fuzzy inference method [58]. It encompasses five conceptual components, as illustrated in Fig. 3.2: A fuzzifier, a dynamic membership function engine module, a fuzzy rule base, a fuzzy inference engine as well as a defuzzifier. First, the fuzzifier transforms crisp inputs into fuzzy sets. The fuzzy rule base module on the other hand, is used to store a selection of fuzzy rules. Furthermore, the dynamic membership function engine provides the system with adaptive capabilities in order for the DFIS to not only incorporate human expertise in the form of fuzzy if-then rules but also fine-tune the membership functions according to a desired input-output data set. Moreover, the fuzzy inference engine is a generic control mechanism that exploits the fuzzy rules and the fuzzy sets that represent task-specific data to reach a certain conclusion. Finally, the defuzzifier converts the fuzzy sets into crisp output data. A detailed description of the DFIS components is provided in the following subsections.

3.2.1 Fuzzifier

The fuzzifier determines the degree of membership of the input values to defined fuzzy sets. A fuzzy set is characterized by a membership function, which maps each element of the universe of discourse to a membership grade between 0 and 1. In the case of the aforementioned human perceptual system, the input linguistic variables are associated with the image dependent part of the visual model, which correspond to the luminance sensitivity (L_k) and the texture sensitivity (T_k). The frequency sensitivity (F_k) describes the human eye sensitivity to various frequencies and is independent of the image content, it is therefore only considered following the defuzzification process. The output linguistic variable is the inferred value associated with the watermarking strength (S_k). The term sets $T(\cdot)$ of the linguistic variables correspond to the sets of their linguistic values and are described as follows:

$$T(L_k) = \{bright, lightly\ dark, dark\}, \tag{3.3}$$

$$T(T_k) = \{rough, slightly\ rough, rough\}, \tag{3.4}$$

$$\begin{aligned} T(S_k) \quad = \quad & \{very\ small, slightly\ small, slightly \\ & large, medium\ large, very\ large\}. \end{aligned} \tag{3.5}$$

Furthermore, each term in $T(W_k)$ and $T(S_k)$, where $W_k = \{x|x = L_k, T_k\}$, is characterized by a fuzzy set of a universe of discourse $X = [0, \rho]$ and X = [A,E], respectively, as it is illustrated in the fuzzy system shown in Fig. 3.3, generated by the dynamic membership function engine and used throughout the watermarking scheme.

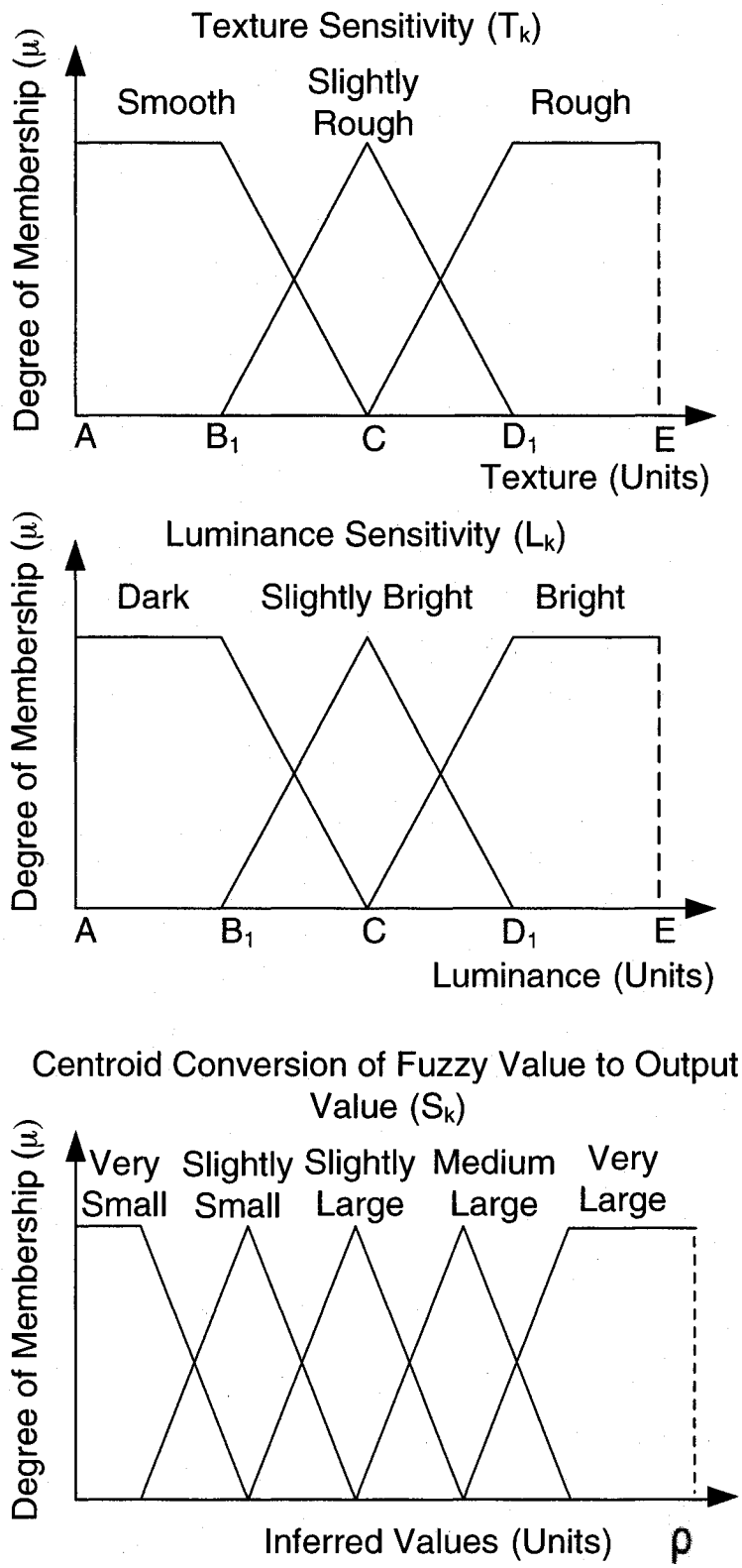


Figure 3.3: Dynamic membership functions and mapping of their input/output variables to fuzzy sets.

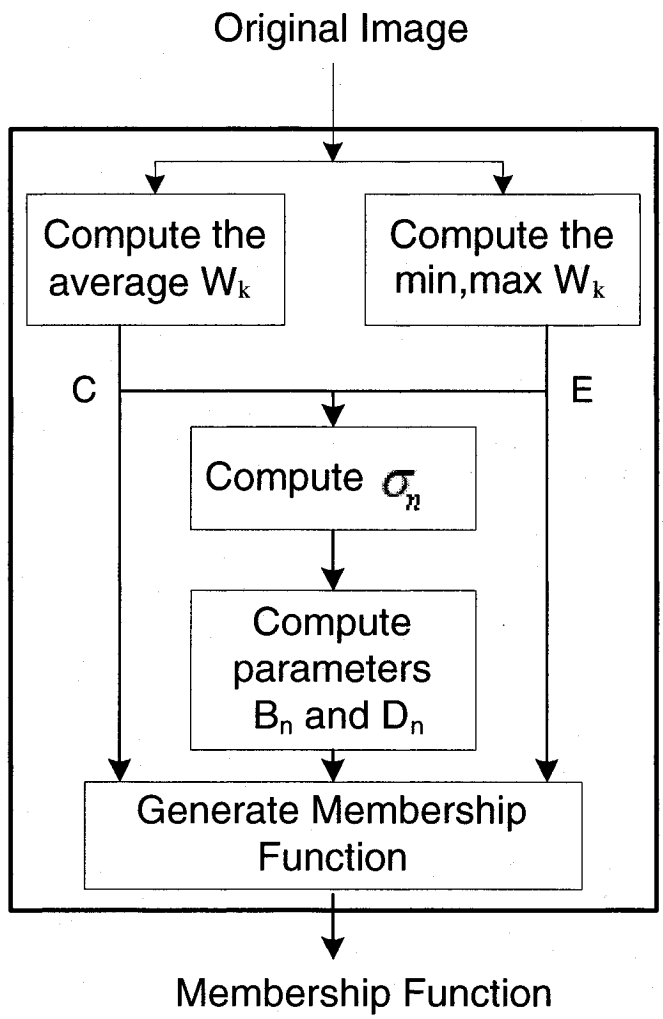


Figure 3.4: Dynamic membership function engine architecture

3.2.2 Dynamic Membership Function Engine

The dynamic membership function engine (DMFE) has been implemented in order to approximate with great accuracy the relationship established between all the properties of the human perceptual model. Distinct input membership functions are dynamically generated for every image prior to the watermarking process. Although the membership functions used in this scheme consist of triangular and trapezoidal functions, they are not restricted to these shapes. This is made possible as the DMFE can be adjusted in such a manner to accurately adapt a membership function for any nonlinear input/output mapping, provided that an

initial approximate membership function is presented along with an appropriate number of fuzzy if-then rules.

The DMFE is modelled as in Fig. 3.4 and can be described as follows:

$$A = \left\lfloor \min_{1 \le k \le N}(W_k) \right\rfloor \tag{3.6}$$

$$C = \frac{1}{N}\sum_{k=1}^{N}(W_k) \tag{3.7}$$

$$E = \left\lceil \max_{1 \le k \le N}(W_k) \right\rceil \tag{3.8}$$

$$\sigma_n = \begin{cases} \lambda_n \cdot \sqrt{\dfrac{\sum_{k=1}^{N}(W_k - C)^2}{N}}, & \text{if } W_k \text{ is n.d.;} \\ \lambda_n \cdot \dfrac{\sum_{k=1}^{N}(|W_k - C|)}{N}, & \text{otherwise.} \end{cases} \tag{3.9}$$

$$B_n = C - K_{1n} \cdot \sigma_n \tag{3.10}$$

$$D_n = C + K_{2n} \cdot \sigma_n \tag{3.11}$$

The membership function engine depicted in Fig. 3.4 attempts to adjust the fuzzy membership functions in such a manner to accurately model the distribution of the input data. When an input data range varies significantly, the fuzziness of the corresponding membership function is increased. Conversely, when the variation of the input data is small, the fuzziness of the membership function is reduced. To illustrate this process, the general case is presented in Fig. 3.5. The number of approximate membership functions exploited to model the distribution of a data set, generally relies on the level of variation of the input

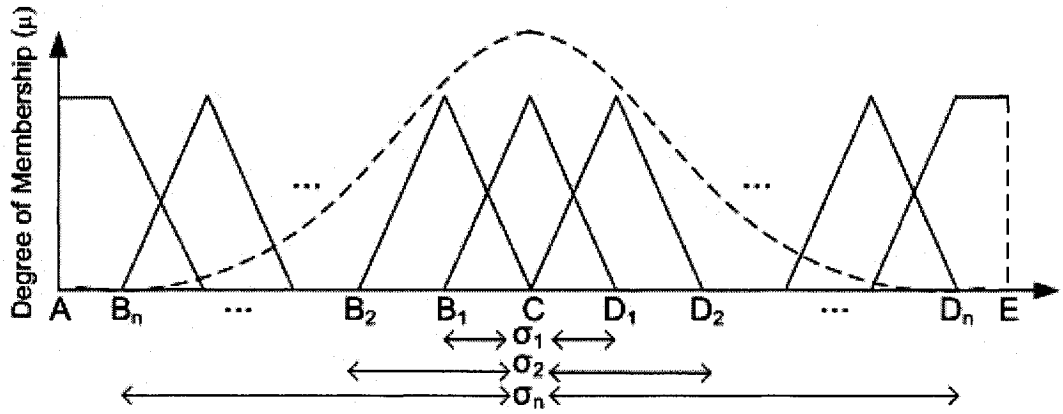


Figure 3.5: The general model used to demonstrate the dynamics of the membership functions.

data as well as the required precision. Consequently, an analysis of the statistical deviation of the data is considered in order to best model the fuzzy membership functions.

In order to describe this process, the variable A is first set to take the minimum value computed for W_k as it is illustrated in Equ. (3.6), where $W_k = \{x|x = L_k, T_k\}$ and N is the number of 8×8 blocks. In addition, to compute the value at point C, we calculate the mean of W_k of all 8×8 blocks of the image as defined in Equ. (3.7). Next, the variable E is computed as in Equ. (3.8), where *max* corresponds the maximum value of W_k computed from the entire image. Subsequently, the deviation of the input data is estimated as in Equ. (3.9), where the standard deviation is computed if the input data follows a normal distribution (n.d.), otherwise, the Average Absolute Deviation (AAD) is evaluated. This approach is followed because the AAD is less affected by extremes in the tails of a specific distribution, making it a better candidate when computing the deviation for non-normally distributed data [59]. Furthermore, λ_n is used in order to control the deviation of the input data among the membership functions. Once σ_n is computed, variable B_n and D_n are calculated as in Equ. (3.10) and Equ. (3.11), where K_{1n} and K_{2n} are used to further tune-up the position of the membership functions, if necessary. In our system, $K_{1n} = K_{2n} = 1$.

In order to determine whether the input data follows a normal distribution, we make use

of the kurtosis and the skewness measures, commonly used to compute the variability and location of a specific data set [59]. The skewness is a measure of the asymmetry of a known distribution around the sample mean, whereas, the kurtosis is a measure of the peakedness or flatness of the data relative to a normal distribution. From the histogram of a data set, it can be observed that a distribution with high kurtosis tend to have a sharp peak around the mean with heavy tales, whereas a distribution with a small kurtosis tend to have a flatter peak near the mean. The kurtosis and the skewness measures are computed as follows:

$$kurtosis = \frac{\sum_{i=1}^{N}(X_i - \overline{X})^3}{(N-1)s^3}, \tag{3.12}$$

$$skewness = \frac{\sum_{i=1}^{N}(X_i - \overline{X})^4}{(N-1)s^4}, \tag{3.13}$$

where $\overline{X}$ denotes the mean of the sample input data, s is the standard deviation, and N is total number of W_k (luminance or texture) values extracted from the original image. The skewness of a normal distribution or any other symmetrical distribution is zero, whereas the kurtosis for a normal distribution is equal to three. Moreover, a small margin of error is tolerated in this scheme when computing the skewness and the kurtosis, to permit a certain flexibility when determining the distribution of a data set. The normal probability plot is an alternative approach to determine whether a data set is normally distributed [59]. It is a graphical technique where a set of data is plotted against a theoretical normal distribution. In the case where the data set is normally distributed, the resulting points should form a graph of an approximate straight line. A significant deviation of the points from the straight line indicates a departure from normality. Although the skewness-kurtosis and the normal probability plot methods can both be used to determine the normality of a specific distribution, the latter was however exploited as it permits an automated approach to achieve this goal.

3.2.3 Fuzzy Rule Base

The fuzzy rule base essentially contains a selection of fuzzy rules. It provides a knowledge acquisition base that is of great relevance when building the fuzzy inference system. The knowledge consists of a set of IF-THEN rules that can be given by a human expert or can also be extracted from the linguistic description of the data. A fuzzy if-then rule generally takes the following form:

$$IF\ X_1 = A_1\ AND\ X_2 = A_2\ \ldots\ AND\ X_n = A_n\ THEN\ Y = B, \quad (3.14)$$

where $A_1 \ldots A_n$, and B are linguistic values defined by fuzzy sets on universes of discourse X and Y, respectively. In addition, it can be observed from the general if-then rule form above, that each rule base has an antecedent (or premise) part as well as a consequent (or conclusion) part. The antecedent part is a set of conditions linked together through conditional (or logical) operators (i.e. AND, OR, NOT), whereas the consequence part consists of the corresponding action.

In Table 3.1, the fuzzy rules associated with the fuzzy system generated by the aforementioned DMFE are illustrated. These rules are carefully depicted to best describe the desired approximate behavior of our fuzzy system in order to establish an accurate relationship between the image characteristics and the watermark embedding strategy.

3.2.4 Fuzzy Inference Engine

An inference engine is generally defined as a system that can give a conclusion (an output) from a fact (an input) and a set of control rules (knowledge). In the case where the knowledge includes fuzzy linguistic terms (or values) which are normally generated by the aforementioned fuzzification process, it is referred to as a fuzzy inference engine. Moreover, the fuzzy inference engine performs the rule evaluation process, which is divided into two

Table 3.1: Fuzzy Inference Rules

Rule Number	Rule Description
1	If (Luminance is *dark* and Texture is *smooth*) then (watermark strength and length are *very small*)
2	If (Luminance is *dark* and Texture is slightly *rough*) then (watermark strength and length are *slightly small*)
3	If (Luminance is *dark* and Texture is *rough*) then (watermark strength and length are *slightly large*)
4	If (Luminance is *slightly bright* and Texture is *smooth*) then (watermark strength and length are *slightly small*)
5	If (Luminance is *slightly bright* and Texture is *slightly rough*) then (watermark strength and length are *slightly large*)
6	If (Luminance is *slightly bright* and Texture is *rough*) then (watermark strength and length are *medium large*)
7	If (Luminance is *bright* and Texture is *smooth*) then (watermark strength and length are *slightly large*)
8	If (Luminance is *bright* and Texture is *slightly rough*) then (watermark strength and length are *medium large*)
9	If (Luminance is *bright* and Texture is *rough*) then (watermark strength and length are *very large*)

separate tasks: the aggregation and the composition. The aggregation process consists of evaluating the antecedent part of each rule, whereas, the composition process consists of evaluating the conclusion part of each rule. Furthermore, during the aggregation process, the degree of membership (or truth value) for each rule is evaluated and then assigned as the degree of truth to the consequent part. In addition, the min-max inference method was used in order to determine the inference output when dealing with composite rules. It is a common technique that can be depicted in two different steps. First, for each of the antecedents, the minimum value of the membership function is determined for the input values,

and subsequently applied to the consequent. A fuzzy set is then constructed from the union of all the rules, using the maximum of the membership values previously determined.

3.2.5 Defuzzifier

The last step in the dynamic fuzzy inference system is the defuzzification of the output fuzzy sets into crisp values. The defuzzifier is essentially used to determine the value that best represents the information contained in the fuzzy set. The most widely used techniques for defuzzification are the Center-of-Maximum and the Centroid-of-Area, also known as the Center-of-Gravity technique. The latter approach is used in this scheme and it relies on the gravity method to determine the center of gravity of the output fuzzy region. This is achieved by first dividing the membership functions of each linguistic term at their corresponding degree of membership. The divided areas are then superimposed and the weighted mean of the fuzzy region is computed to determine the inferred output value. In this case, the defuzzification process is described as follows:

$$i_k = \frac{\sum_{n=1}^{N} \mu_c(i_n) i_n}{\sum_{n=1}^{N} \mu_c(i_n)} , \tag{3.15}$$

where i_k corresponds to the overall crisp value obtained based on the relationship establish among the crisp input values (luminance and texture sensitivity), μ_c is the aggregated resultant membership function of the output fuzzy sets and i_n is the universe of discourse corresponding to the centroid of μ_c.

Although the centroid of area is the most commonly adopted defuzzification strategy today, it is considered undesirable in certain real-time applications as the area calculation under the membership functions of the output region is highly computationally intensive.

In Fig. 3.6, an example of a fuzzy system generated for a specific image is shown in order to illustrate how the defuzzification process as well as the fuzzy inference mechanism work. The example will demonstrate the process for only one 8×8 block of the image. Let's

assume that the extracted luminance value for this block is 0.6, whereas the texture value is equal to 22. The luminance value maps into degree of membership values $\mu_{(slightly\ rough)} = 0.6$ and $\mu_{(rough)} = 0.4$, in the fuzzy sets *slightly rough* and *rough*, respectively. Similarly, The texture value maps into degree of membership values $\mu_{(dark)} = 0.7$ and $\mu_{(slightly\ bright)} = 0.3$, in the fuzzy sets *bright* and *slightly dark*, respectively. By associating these four degrees of membership to the fuzzy rule base, four rules will be triggered: Rule 2, 3, 5 and 6. If we first consider Rule 2, it states the following as it was illustrated in Table 3.1:

If (Luminance is *dark* and Texture is *slightly rough*) then (watermark strength and length are *slightly small*)

As mentioned earlier, the degrees of membership are $\mu_{(dark)} = 0.7$ and $\mu_{(slightly\ rough)} = 0.6$. Furthermore, the fuzzy AND of the two expressions consists of the lesser value. Therefore the resultant degree of membership of the input condition for Rule 2 is $\mu_{CONDITION} = 0.6$. Similar steps are followed in order to determine the resultant degree of membership for Rules 3, 5 and 6 as follows:

(Rule 2) $\mu_{(slightly\ small)} = 0.6$,

(Rule 3) $\mu_{(slightly\ large)} = 0.4$,

(Rule 5) $\mu_{(slightly\ large)} = 0.3$,

(Rule 6) $\mu_{(medium\ large)} = 0.3$.

These values are then evaluated to produce a crisp output value. This is achieved using the aforementioned centroid technique as it is illustrated in Fig. 3.6. For Rule 4, the membership function of the fuzzy set *slightly small* is sliced off at the corresponding degree of membership, $\mu = 0.6$, and the centroid of the resulting area is computed and is equal to 1. A similar approach was followed for the other three rules and the centroid values are 1.5, 1.5 and 2 for Rules 3, 5 and 6, respectively. The final inferred output was then obtained using the defuzzification equation (Equ. (3.15)) as follows:

$$i_k = ((0.6 \cdot 1)(0.4 \cdot 1.5)(0.3 \cdot 1.5)(0.3 \cdot 2))/(0.6 + 0.4 + 0.3 + 0.3) = 1.41.$$

3.3 Computing the Adaptive Watermarking Strength

As aforementioned, the DFIS along with a perceptual model are used in the proposed method in order to determine the optimal weights for the DCT coefficients of all 8×8 blocks of an image. The DFIS establishes a relationship between the luminance (L_k) and texture (T_k) sensitivity, which correspond to the image's dependent part of the visual model. This in turn enables smoother control of the watermark adaptability with respect to the image's characteristics. The luminance and texture sensitivity values are therefore used as the input data to the DFIS to determine the adaptive watermarking strength values and length of the watermark for the cover image. The DFIS outputs (also known as the inference result) are computed by means of the centroid defuzzification method, where the inferred value i_k of a specific block k of an image is calculated as in Equ. (3.15).

In order to compute the adaptive watermarking strength, the inferred value i_k is multiplied the frequency sensitivity (the image-independent part of the HVS) and by a scaling factor β as it is depicted in the following equation:

$$\alpha_{x,y,k} = F_{x,y} \cdot i_k \cdot \beta \ , \tag{3.16}$$

where $\alpha_{x,y,k}$ corresponds to the adaptive strength of a watermark at index (x,y) of the k'th block of an image. Furthermore, $F_{x,y}$ denotes the frequency sensitivity at index (x,y), whereas β is a constant used to scale and adjust the generated watermarking strength values for a specific image. It typically varies as $1 \leq \beta \leq 3$. A high β value is commonly used to increase the robustness of the watermark at the expense of possibly degrading the quality of digital data. Conversely, a smaller β value generally refers to a not-so-robust watermark, however preventing any visual degradation to the cover image.

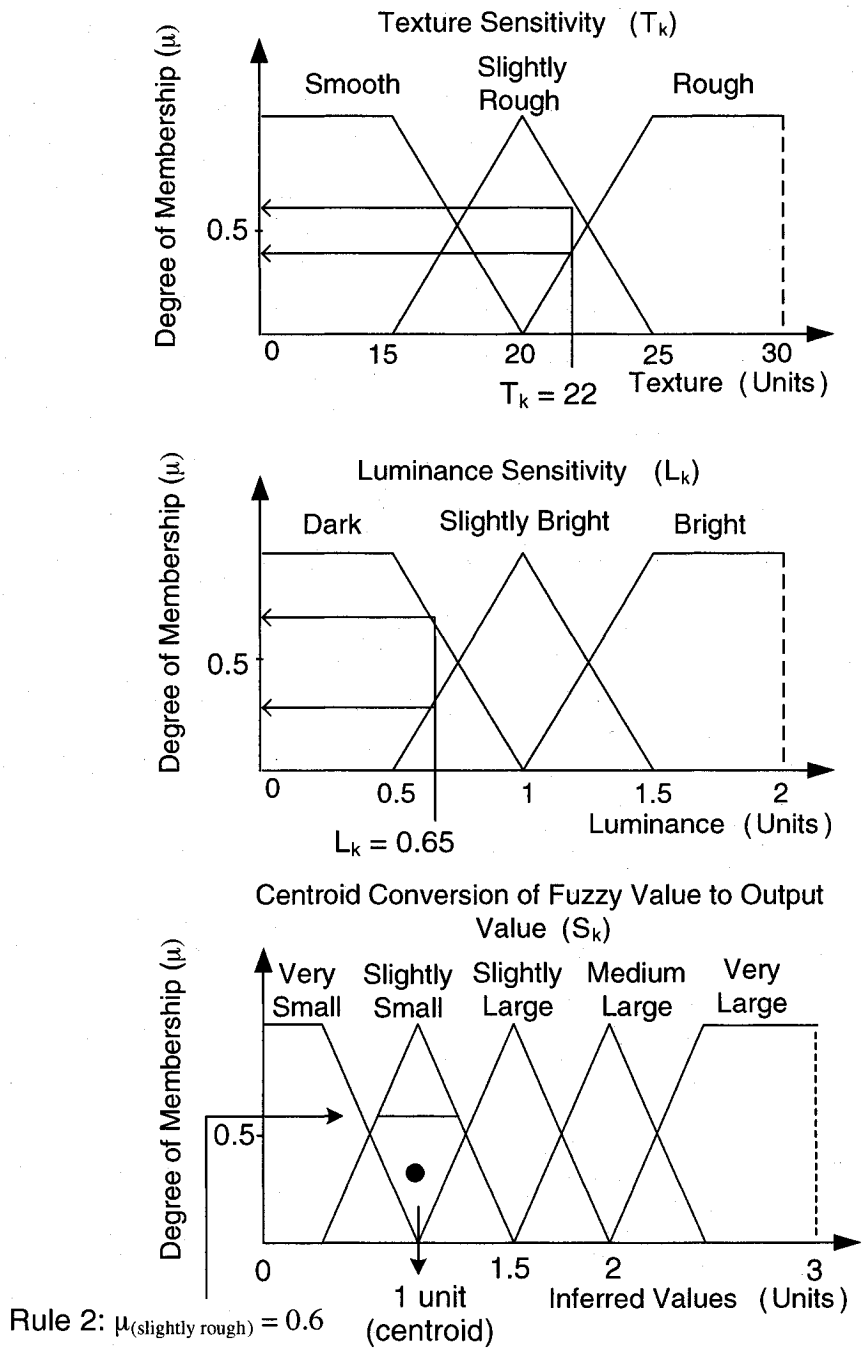


Figure 3.6: An example used to demonstrate the fuzzy inference procedure.

3.4 Computing the Adaptive Watermark Length

The adaptive watermark length is determined similarly to the adaptive watermarking strength. The luminance and texture sensitivity values are evaluated by the DFIS and the resultant inferred values are used to compute the watermark length. This is achieved as in Equ. (3.17), where the watermark length for each block k is computed as follows:

$$l_k = \left\lceil \frac{i_k}{max(i_k)} \times \eta \right\rceil , \tag{3.17}$$

where i_k is the inferred value generated by the DFIS and η is a constant used to set the maximum number of bits that may be embedded into an 8×8 block. In our scheme η is set to 11. In order to insure that the watermark embedding process is achieved in low-frequency components of the original image, η must then be set to a small value which in turn will result in a small predicted embedding region as it will be explained in the following chapter.

3.5 Summary

This chapter presented the HVS and the DFIS model exploited in order to enable the adaptive behavior of the watermarking algorithm. The HVS incorporates three different properties: luminance sensitivity, texture sensitivity as well as frequency sensitivity. The DFIS relies on a statistical method in order to approximate with great accuracy the relationship established between all properties of the human perceptual model. Furthermore, it was determined that the HVS-DFIS strategy can be used to compute the adaptive watermark length with respect to the local characteristics of the cover image. Similarly the adaptive watermarking strength can also be derived. In Chapter 4, we build on what has previously been depicted to provide a concise illustration of the adaptive watermarking algorithm.

Chapter 4

The Proposed Watermarking Scheme

Image watermarking techniques have been significantly studied in the past decade and many methods have been investigated. The proposed watermarking system extends Cox et al.'s [8] spread spectrum watermarking technique to perform adaptive watermark embedding using the aforementioned HVS-DFIS strategy. The goal of this chapter is to mainly introduce the watermark embedder and the watermark detector of the proposed scheme and their relationship to the rest of the system.

Section 4.1 introduces a predictive watermark embedding technique based on a mathematical model that provides an accurate estimate of the embedding regions in which the watermark insertion should be performed. This in turn guaranties a secure and transparent watermark. In Section 4.2, we illustrate the watermark detection process which essentially performs the reverse process of embedding the watermark to extract and identify the inserted message. Finally, in Section 4.3, we demonstrate how the proposed image watermarking scheme can be used to watermark color images.

4.1 The Predictive Watermark Embedding Process

A *predictive watermark embedding* algorithm is introduced that exploits the aforementioned DFIS model in order to insure that the watermark insertion process is adaptively performed in low-frequency (could be extended to mid-frequencies) and significant DCT coefficients.

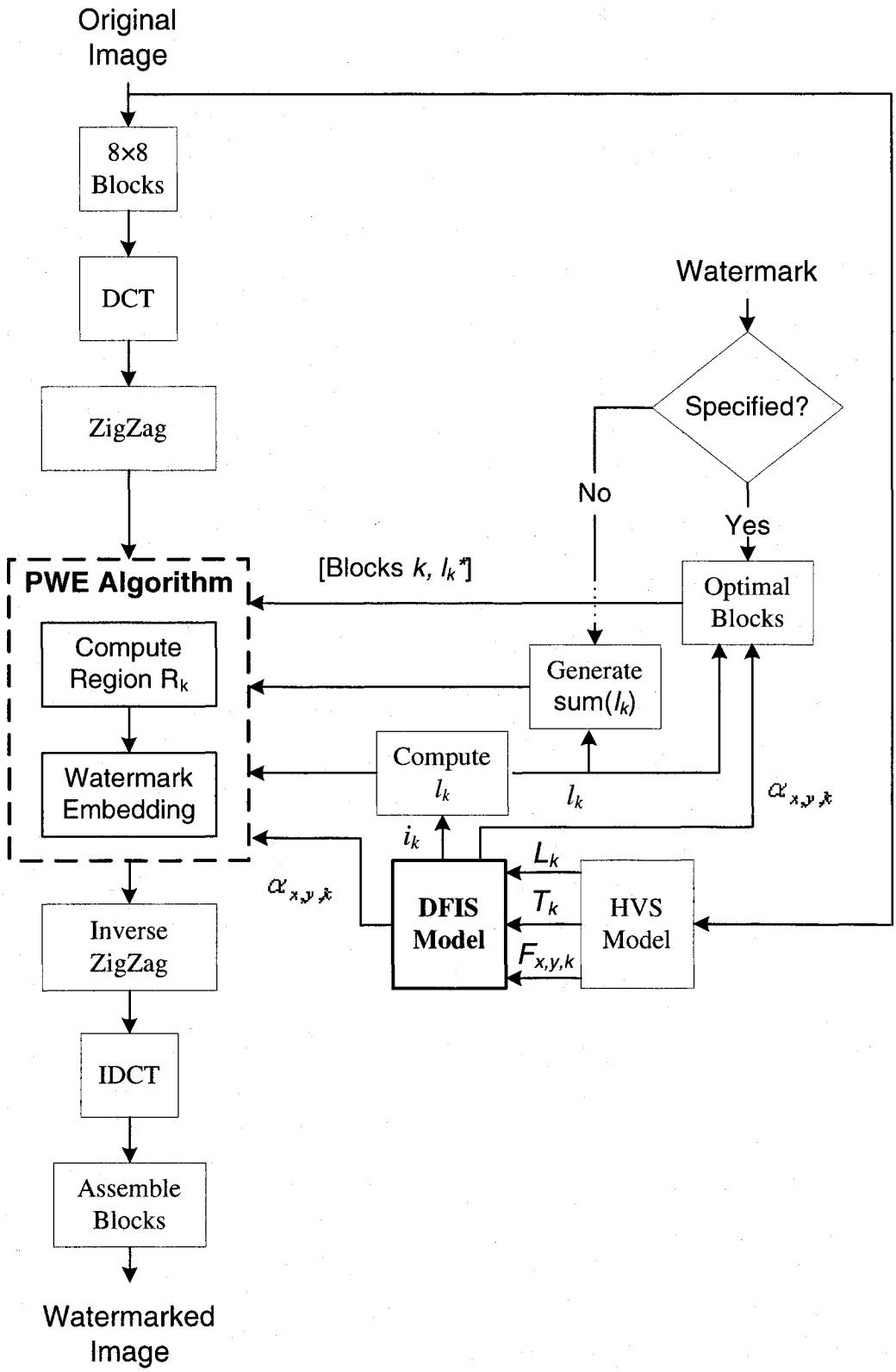


Figure 4.1: The watermark embedding process

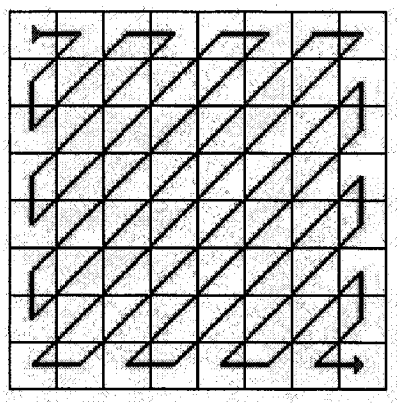


Figure 4.2: The zigzag sequencing technique used to register the DCT coefficients in an ascending frequency order (lower to higher-frequencies).

The motivation behind this approach is to accurately predict the optimum size of the region in which the watermark embedding should be performed while taking into consideration the maximum number of bits that may be inserted in a specific 8×8 block of the cover image. In addition, within each block, the algorithm insures that the watermark sequence is embedded in the selected high magnitude DCT coefficients defined within the aforementioned optimum region. This enables an efficient watermark insertion process and in turn it insures that illegal tampering of the watermarked image does not remove or transform the watermark into another legitimate signature. The watermark embedding process, which encompasses the PWE algorithm is illustrated in Fig. 4.1. The initial step consists of decomposing the original image into non-overlapping 8×8 blocks and subsequently computing the DCT on each block. Then, the DCT coefficients are registered using zigzag sequencing (shown in Fig. 4.2), a technique commonly used in JPEG encoders.

Next, the perceptual analysis by the dynamic FIS is performed and the inferred values i_k, the sub-watermark length l_k and the adaptive weights $\alpha_{x,y,k}$ are generated for each block k. Then, if the user desires to embed a predefined watermark, an *optimal blocks* selection algorithm is performed in order to identify the finest 8×8 blocks of the image in which the watermark insertion should be performed. This selection is based on the per-

ceptual characteristics of each block. The *optimal blocks* module also generates an updated sub-watermark length $l_k{}^*$ to insure that the sum of all $l_k{}^*$ values is equal to the provided watermark length. Conversely, if a predefined watermark is not provided, a watermark with a maximum length (the sum of all l_ks) is generated. Subsequently, the l_k (or $l_k{}^*$) most significant DCT components within the frequency range R_k are selected, where R_k consists of the optimum embedding region within a block k, and it is described as follows:

$$R_k = \{S \mid S = [(0,1)_1, (1,0)_2, (2,0)_3, (1,1)_4, \ldots, (x,y)_{n_k}]\}, \tag{4.1}$$

$$n_k = \eta \cdot f_k \ , \tag{4.2}$$

where n_k is the size of generated embedding region, η is the maximum number of bits that may be embedded in an 8×8 block and it can vary as $1 \leq \eta \leq 15$. In order to compute the embedding region factor f_k, we first determine the average power of the DCT coefficients within the first r lower-frequency components, which are registered using zigzag sequencing. This is described as:

$$P_k = \frac{1}{r} \sum_{x,y} (V_{x,y,k})^2 \ , \tag{4.3}$$

where P_k is the average power of a block k, and $V_{x,y,k}$ is the DCT coefficient at position (x,y) in the k'th block of the cover image. Moreover, the magnitude of r is empirically derived and it is directly dependent on the value of η. In our scheme we set r equal to 20. The embedding region factor f_k is then computed as described below:

$$f_k = \begin{cases} 1, & P_k \geq t_{max}; \\ 1 + \dfrac{(T_{max} - 1)(P_k - t_{min})}{(t_{max} - t_{min})}, & t_{min} \leq P_k < t_{max}; \\ T_{max}, & otherwise. \end{cases} \tag{4.4}$$

where t_{min} and t_{max} are empirically derived threshold values, whereas T_{max} is the maximum factor that respects that following condition $\eta \cdot f_k \leq r$. It is important to realize that for small η, the embedding region can be limited to the low-frequency components, larger values of η however, might slightly extend the embedding range to the mid-frequency components.

Once the adaptive weights $\alpha_{x,y,k}$, the sub-watermark lengths l_k (or $l_k{}^*$) as well as the predictive embedding regions R_k are computed for all 8×8 blocks, the watermark embedding algorithm is then performed to embed the predefined (or generated) watermark. In our proposed scheme it consists of a random number sequence that follows the normal distribution $N(0,1)$. Furthermore, the watermark insertion is based on a spread-spectrum technique introduced in [8] and can be described as:

$$V'_{x,y,k} = V_{x,y,k} \cdot (1 + \alpha_{x,y,k} \cdot w_{x,y,k}), \tag{4.5}$$

where $V_{x,y,k}$ refers to the DCT coefficients of the position (x,y) of the k'th block, and $\alpha_{x,y,k}$ is the selected adaptive strength for the watermark $w_{x,y,k}$. Finally, the IDCT of each block is performed prior to combining all blocks to generate the watermarked image.

4.2 The Watermark Detection Process

The watermark detection process essentially consists of the reverse process of embedding the watermark. The initial step consists of decomposing the watermarked and the original images into non-overlapping 8×8 blocks and subsequently computing the DCT on each block. Then, the DCT coefficients are registered using zigzag sequencing. Subsequently, the regeneration of the DFIS is performed to reproduce the inferred values i_k which are used to compute the watermark length l_k for all blocks. The *optimal blocks* selection is recomputed depending on whether an initial watermark was specified. The inferred values are then multiplied by the frequency sensitivity and a scaling factor β to generate the watermarking strength values which are passed to the watermark detection algorithm. In addition, the

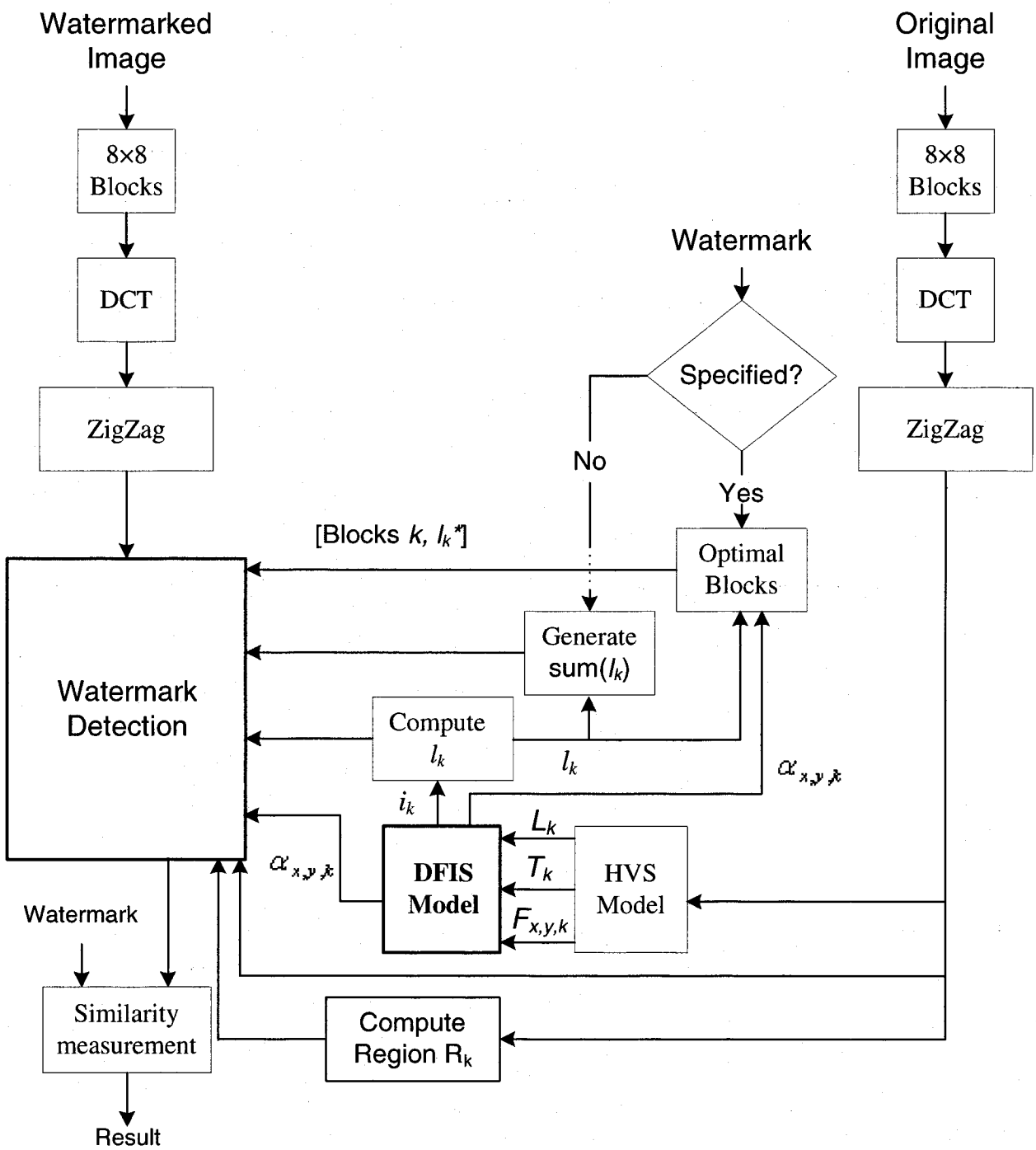


Figure 4.3: The watermark detection process

embedding regions R_k are recomputed from the DCT of the cover image prior to performing the watermark extraction process. The watermark detection is then achieved and it can be described mathematically by the following equation:

$$w'_{x,y,k} = \frac{(V'_{x,y,k} - V_{x,y,k})}{(\alpha_{x,y,k} \cdot V_{x,y,k})} , \tag{4.6}$$

where $V'_{x,y,k}$ is the DCT coefficient at position (x,y) in the k'th block of the watermarked image. Furthermore, from $w'_{x,y,k}$ we can obtain the extracted watermark W' by combining all sub-watermarks as follows:

$$W' = \bigcup_k w'_{x,y,k} , \tag{4.7}$$

where $0 \leq x, y \leq 8$ and $0 \leq k \leq N$, N being the number of non-overlapping 8×8 blocks of the cover image.

The watermark correlation computation is subsequently performed as follows:

$$sim(W', W) = \frac{W' \cdot W}{\sqrt{(W' \cdot W')}} , \tag{4.8}$$

where *sim* is a similarity measurement between the extracted watermark W' and the original watermark W. If the result is larger than a predefined threshold then the extracted watermark is approved and therefore considered as correct.

4.3 Watermarking Color Images

The application of the proposed scheme to color images is rather simple as it is illustrated in Fig. 4.4. First, the image is converted to YIQ, a color space formerly defined by the National Television Systems Committee (NTSC), where I (stands for in-phase) and Q (stands for quadrature) represent the chrominance information, whereas the Y component represents the luminance information, which is essentially the grayscale representation of the image.

Fig. 4.5 shows a color (RGB) version of the Baboon image and its grayscale counterpart (which is the Y component extracted after converting the image from the RGB format to the YIQ color space). Subsequently, the proposed algorithm takes the Y component as an input and generates the watermarked version Y'. The Y' is then combined with the IQ components of the original image and converted back to its original RGB format to finally produce a watermarked color image of Baboon. Fig. 4.6 shows the grayscale watermarked image of Baboon as well as its color (RGB) counterpart. The color image can thereafter be converted to other formats, but it must by converted back to YIQ when the extraction of the watermark is required.

4.4 Summary

In this chapter the proposed watermarking scheme was discussed, in which the HVS-DFIS strategy along with a predictive watermark embedding scheme are exploited to accurately perform the insertion and the detection of the watermark. The predictive watermark embedding algorithm is used to compute the average power of the DCT components in order to predict an accurate size of the regions in which the watermark insertion will be performed in lower-frequencies and high-magnitude DCT coefficients. Furthermore, the watermark detection process was exploited to extract the watermark from the watermarked work and consequently perform a similarity measurement with the original watermark. The proposed adaptive watermarking scheme is primarily design for gray scale images, it can however be used for color images by simply converting the RGB image to YIQ format and subsequently embedding the watermark in the Y component.

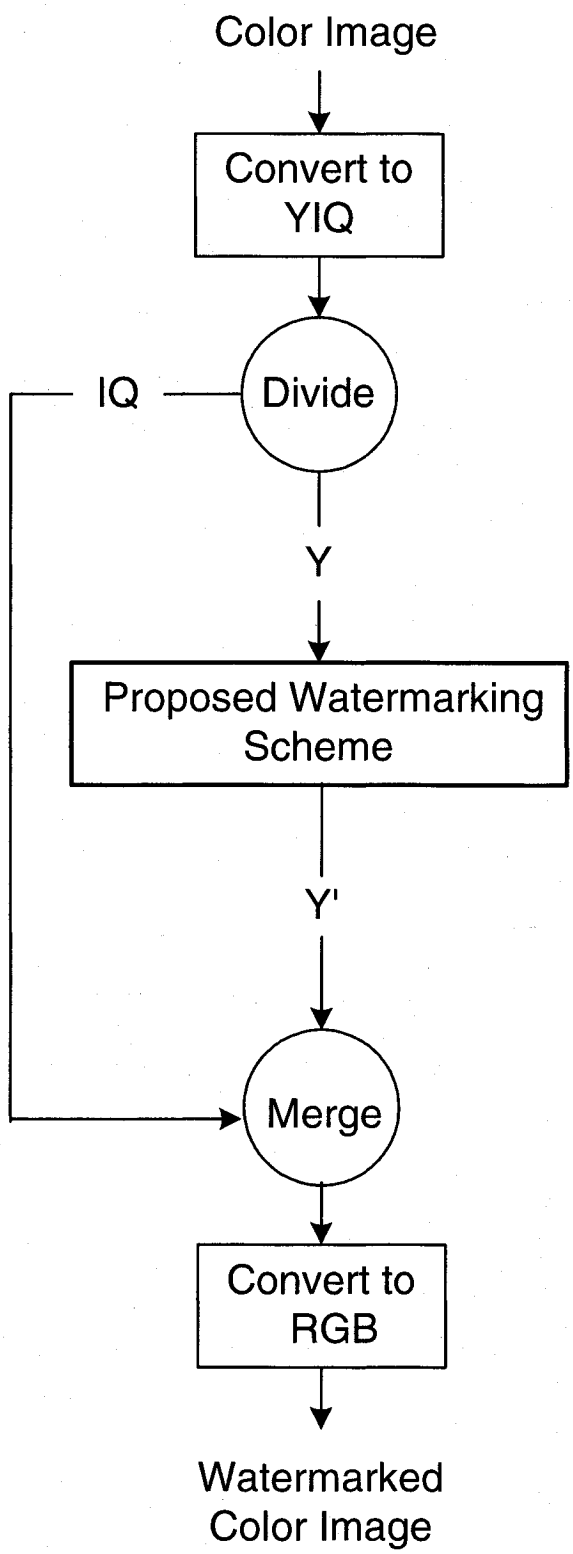


Figure 4.4: The process taken to perform color image watermarking using the proposed scheme.

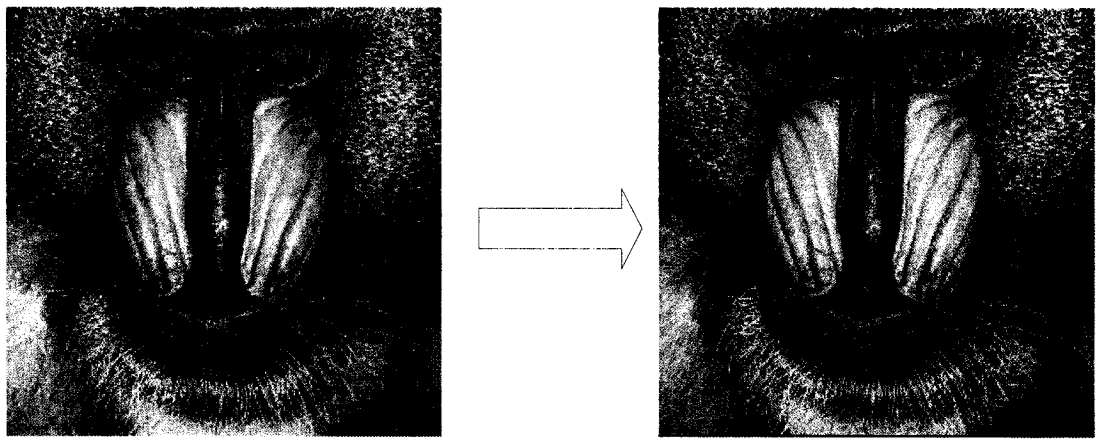


Figure 4.5: The original RGB image of baboon (left) and its grayscale representation (right).

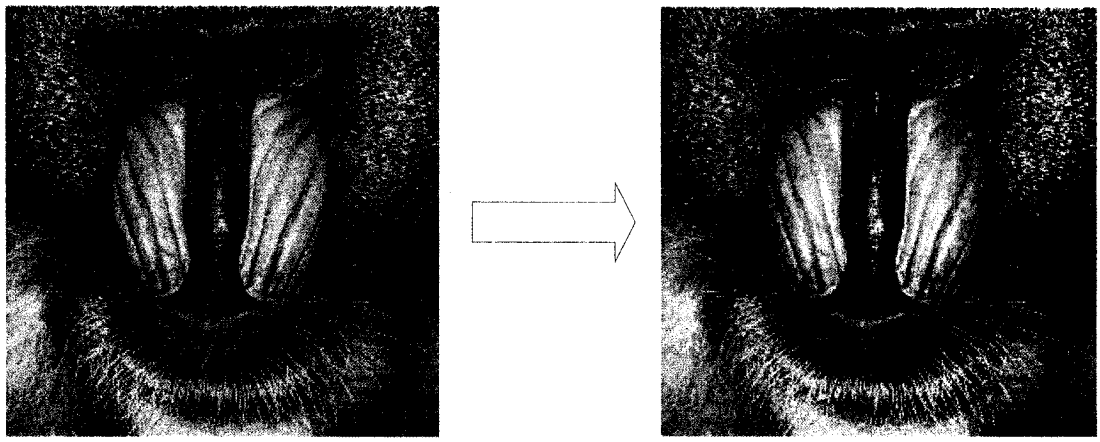


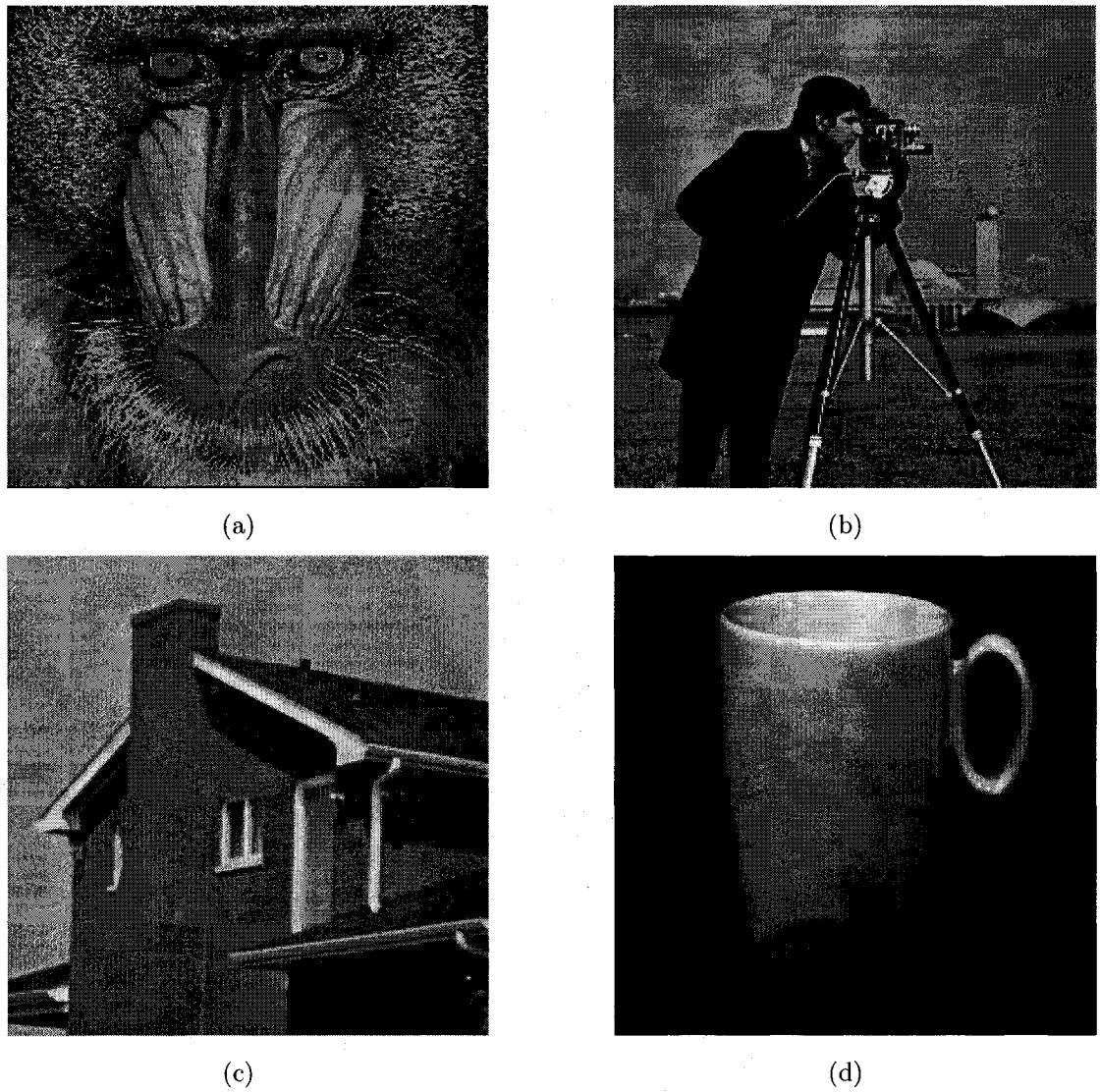
Figure 4.6: The grayscale watermarked image of Baboon (left) as well as its color (RGB) counterpart (right).

Chapter 5

Experimental Results

In this chapter we present the experimental results achieved using 256 × 256 gray scale images of Baboon, Cameraman, House and Cup shown in Fig. 5.1. The Peak Signal to Noise Ratio (PSNR) was measured in order to evaluate the imperceptibility of the watermark as well as the degradation of the watermarked images. Furthermore, several experiments were performed in order to demonstrate the robustness of the algorithm under several signal processing and geometric attacks. As aforementioned, the watermark in our proposed scheme consists of a random number sequence that follows the normal distribution *N(0,1)* [46]. The proposed scheme was also tested using binary watermarks, as it was suggested in [45]. Binary watermarks are however not recommended as they are less robust to attacks based on collusion of several independently watermarked copies of the same image. In addition, we compare our experimental results to Cox et al.'s scheme [8], Huang and Shi's scheme [10], as well as Lou and Yin's scheme [6] described in Chapter 2. In order to adequately compare our results to Huang and Shi's method, we modified their embedding process to be performed as in Equ. (2.2). Furthermore, certain experimental results provided for Lou and Yin's scheme were extracted directly from [6] in order to make the comparison as accurate and fair as possible.

In Section 5.1, the adaptive watermark length and strength are generated and the imperceptibility criterion is evaluated for all test images in Fig. 5.1. Finally, in Section 5.2, the



(a) (b)

(c) (d)

Figure 5.1: Original images of (a) Baboon, (b) Cameraman, (c) House, and (d) Cup.

robustness of the proposed system was also evaluated as the watermarked work was altered using various attacks, including signal processing attacks such as lossy JPEG compression, additive Gaussian noise, scaling, low-pass filtering and collusion, as well as geometric attacks such as cropping and scaling.

Table 5.1: Watermark Lengths for Images of Fig. 5.1.

	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
Baboon	1000	3072	5032	7014
Cameraman	1000	3072	5309	7040
House	1000	3072	3636	5715
Cup	1000	3072	3161	5687

5.1 Adaptiveness and Imperceptibility of Watermark

5.1.1 The Adaptive Watermarking Strength

As aforementioned, the HVS and the DFIS combined were used to take advantage of the perceptual characteristics of the cover image to determine the optimal weights for all DCT coefficients. In consequence, a maximum strength watermark can be embedded while maintaining the perceptual quality of the cover image. The adaptive watermarking strengths of all 8×8 blocks for our scheme, Lou and Yin's Cox, Huang and Shi's scheme and Cox et al.'s scheme are shown in Fig. 5.2(a), Fig. 5.2(b), Fig. 5.2(c), Fig. 5.2(d), respectively. In Cox et al.'s scheme, a constant watermarking strength value $\alpha = 0.1$ was used. In Huang and Shi's scheme, the watermarking strength was assigned one of three possible values α_1, α_2, α_3, that were empirically derived for each test image. In Lou and Yin's scheme and our scheme, adaptive watermarking strength values were used. However, it is well demonstrated that our scheme presents a clearer and a smoother representation of the adaptive watermark weights.

5.1.2 The Adaptive Watermark Length

The watermark length was generated by means of the HVS-DFIS strategy as it was illustrated in the watermark embedding and detection processes. It is achieved in such a manner

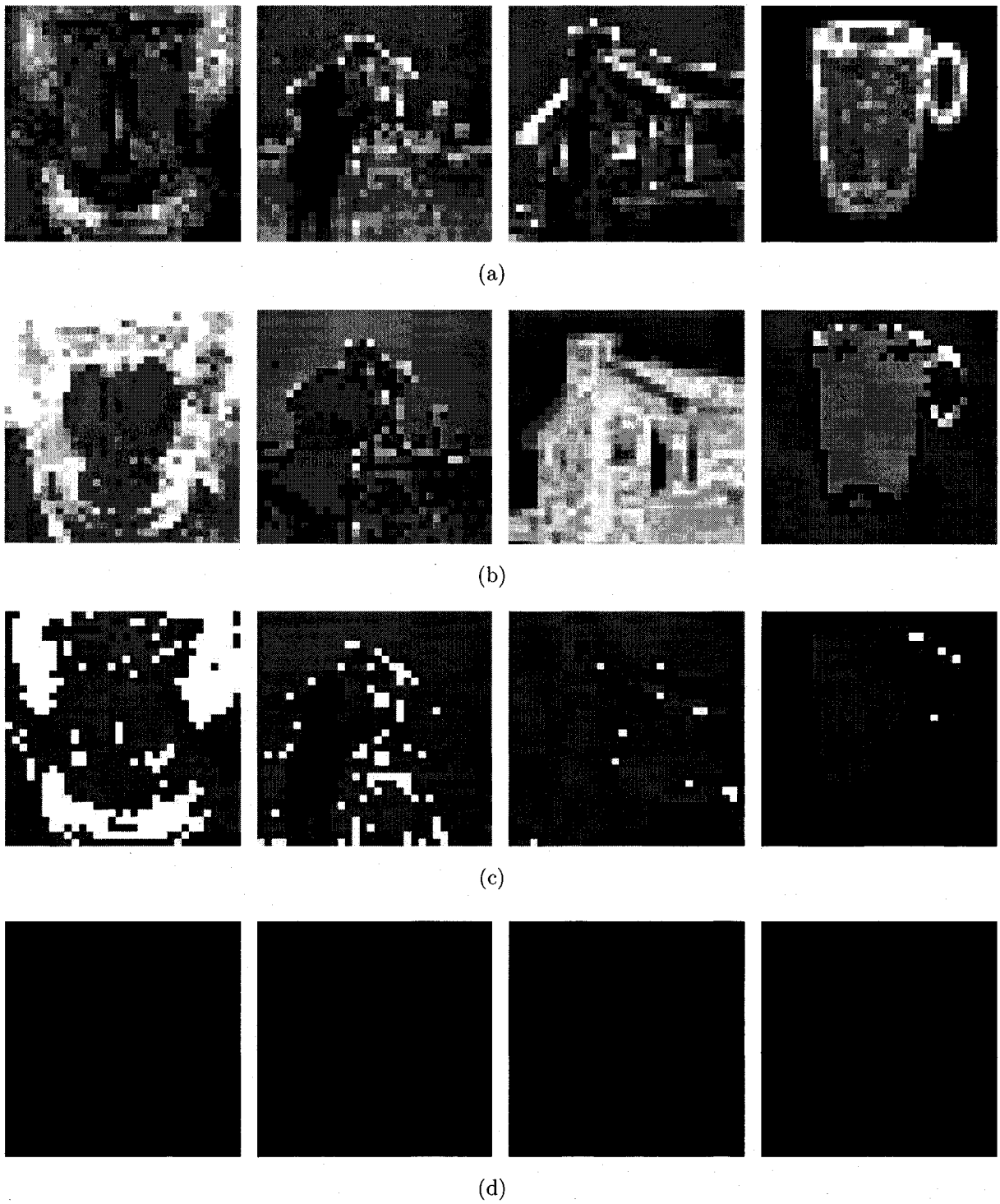


Figure 5.2: Watermark strength values for each 8×8 block (α_k) of all images shown in Fig.5.1 using (a) Our scheme, (b) Lou and Yin's scheme, (c) Huang and Shi's scheme, and (d) Cox et al's scheme.

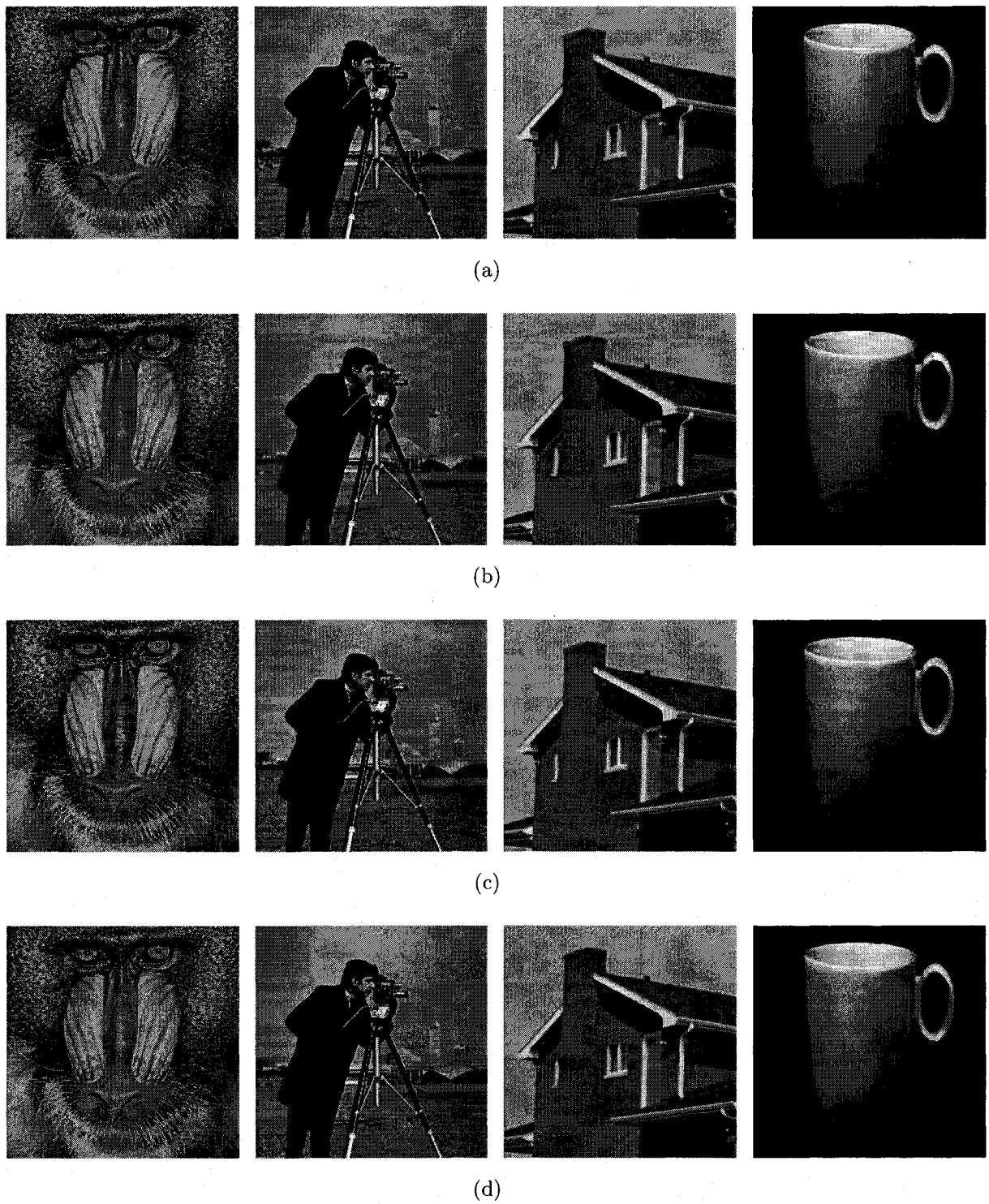


Figure 5.3: Watermarked images of the cover images shown in Fig. 5.1 using (a) Our scheme, (b) Lou and Yin's scheme, (c) Huang and Shi's scheme , and (d) Cox et al's scheme

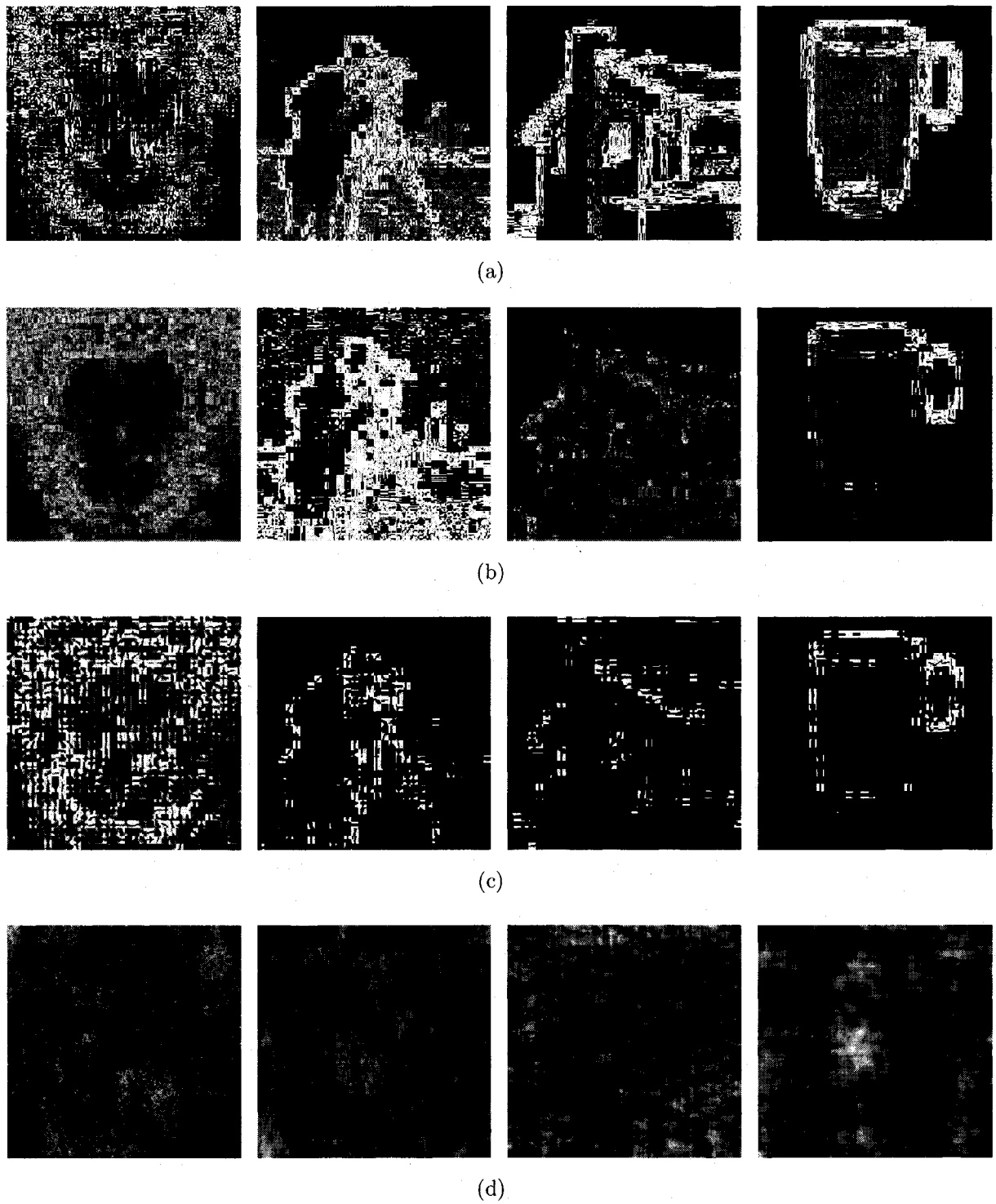
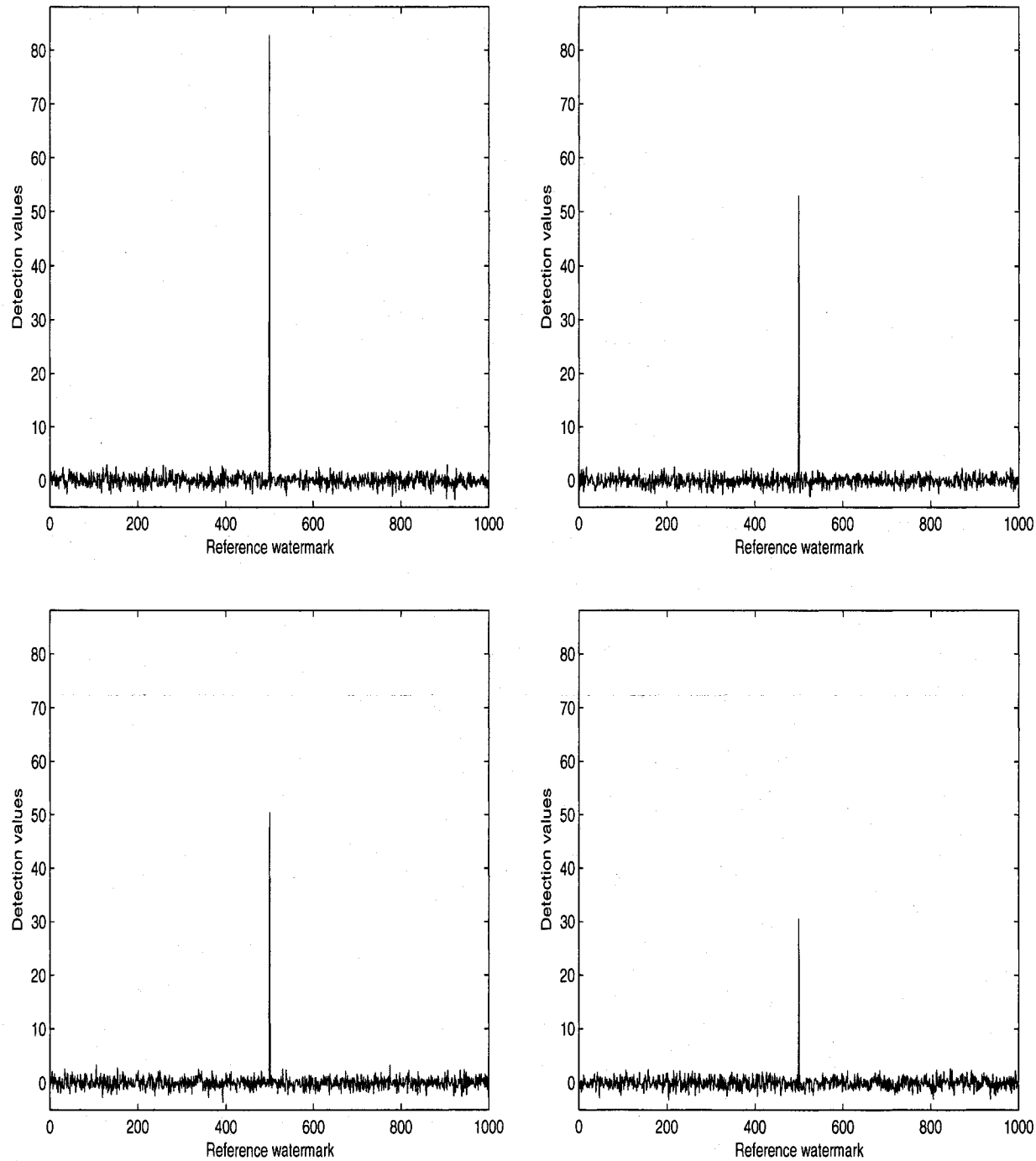


Figure 5.4: The difference images between watermarked images in Fig. 5.3 and the original images in Fig. 5.1 using (a) Our scheme, (b) Lou and Yin's scheme, (c) Huang and Shi's scheme , and (d) Cox et al's scheme .

to generate the longest possible watermark that can be embedded without degrading the quality of the cover image. Moreover, longer watermarks provide more robustness and higher detection values at the expense of imperceptibility. This was discussed in [8], where it was illustrated that in most cases (using the similarity measure presented in Equ. (4.8)), longer watermarks tend to generate higher detection values when the watermark W and the extracted watermark W' are related, without causing higher similarity values when W and W' are unrelated (W' is not the degraded version of W). The watermark lengths that can be used by Cox et al.'s scheme, Huang and Shi's scheme, Lou and Yin's as well as our scheme are illustrated in Table 5.1. Cox et al's scheme and Huang and Shi's scheme use a constant watermark length of 1000 and 3072, respectively. Lou and Yin's, similarly to our scheme, use adaptive watermarks of lengths 5032, 5309, 3636 and 3161. The adaptive watermark lengths in our scheme correspond to 7014, 7040, 5715 and 5687. Lou and Yin's scheme and our scheme demonstrate to nicely model the HVS's properties as the length of the watermarks accurately vary with respect to the image characteristics. The images in Fig. 5.1(a) and 5.1(b) are rough and relatively bright resulting in lengthy watermarks. Conversely, images in Fig. 5.1(c) and 5.1(d) are significantly smooth and uniform resulting in short watermarks. However, the improved image-adaptive nature of our watermarking scheme, results in longer possible watermarks for all test images.

Table 5.2: PSNR Values of Watermarked Images of Fig. 5.3.

	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
Baboon	37.9	38.0	37.6	38.2
Cameraman	39.9	39.4	40.2	40.4
House	39.8	40.3	41.4	41.6
Cup	40.1	39.14	40.4	41.0



(c) (d)

Figure 5.5: The watermark detector response to (a) Our scheme, (b) Lou and Yin's scheme, (c) Huang and Shi's scheme, and (d) Cox et al's scheme, to 1000 randomly generated watermarks, where the 500th watermark is the correct watermark inserted in the Baboon image of Fig.5.1(a).

Table 5.3: Detection Values of Watermarked Images of Fig. 5.3.

	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
Baboon	30.5	50.8	51.8	83.1
Cameraman	32.2	34.9	49.9	64.0
House	31.6	30.3	37.4	60.6
Cup	32.6	20.6	31.8	46.4

5.1.3 Watermark Imperceptibility

In order to examine the imperceptibility constraint, the images in Fig. 5.1 were watermarked using our scheme Fig. 5.3(a), Lou et al.'s scheme Fig. 5.3(b), Huang and Shi's scheme Fig. 5.3(c) and Cox et al.'s scheme Fig. 5.3(d). The Peak Signal-to-Noise Ratios (PSNR) of all watermarked images are illustrated in Table 5.2, and their corresponding detection values for each scheme are also shown in Table 5.3. Fig. 5.5 illustrates the watermark detector response of all four schemes, to 1000 randomly generated watermarks, where the 500th watermark is the correct watermark inserted in the Baboon image of Fig. 5.1(a). The PSNR and detection values demonstrate that our scheme outperforms Cox. et al.'s scheme, Huang and Shi's scheme as well as Lou and Yin's scheme. Moreover, the watermarked images generated by our scheme show no visual distortions, and they are almost identical to the original images. Furthermore, the difference images between the watermarked and original images are illustrated for all four schemes in Fig. 5.4. It can be observed that our scheme accurately models the regions in which the watermark insertion is performed, as it takes full advantage of the image-adaptive HVS-DFIS strategy. The watermark is constrained within the highly nonuniform regions of the image, in order to preserve the imperceptibility criterion. Conversely, Cox et al.'s scheme, Huang and Shi's scheme as well as Lou and Yin's scheme present a watermark that in most cases, is spread all over the cover image, with little restrictions.

5.2 Robustness of Watermark

In this section, the Baboon image shown in Fig. 5.1(a) was used to demonstrate the robustness of the proposed watermarking technique under various attacks. These experiments were also performed on the other three test images, where similar results have been achieved.

Table 5.4: JPEG Compression Attack

Quality Factor	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
100	30.7	15.3	49.7	82.7
90	30.5	12.7	40.6	80.3
80	29.9	11.8	33.7	72.9
70	28.9	10.3	29.2	65.1
60	27.2	9.2	23.3	56.1
50	25.7	11.7	18.7	48.2
40	23.4	9.5	16.2	40.7
30	19.5	8.1	14.3	33.9
20	13.8	7.8	9.5	25.6
10	8.5	7.4	8.1	20.7
5	3.4	5.7	4.3	10.2

5.2.1 JPEG compression attack

Lossy compression algorithms such as JPEG are commonly used for efficient storage and transmission of images over the Internet. It is therefore crucial to examine whether the proposed watermarking scheme can survive JPEG compression attacks. In order to perform this experiment, the watermarked image shown in Fig. 5.1(a) was compressed using different quality factors. The results are presented in Table 5.4. Moreover, in Fig. 5.7 the detection values are plotted against a compressed watermarked image with varying PSNR values. The results clearly demonstrate that our scheme outperforms Cox. et al.'s method, Huang and Shi's method as well as Lou and Yin's method. Furthermore, the detection results are

Figure 5.6: Image of Baboon (Fig.5.1(a)) after a JPEG compression attack with a 5% quality factor.

satisfactory for all images, even when the the watermarked image is considerably degraded when compressed with a quality factor as low as 5% as it is shown in Fig. 5.6.

5.2.2 Scaling Attack

Image scaling is a geometric transformation that can be used to resize a watermarked image. In this particular case, we investigate whether a watermark can survive both, image reduction (subsampling) and image zooming. The watermarked image of Baboon (Fig. 5.1(a)) was scaled by a specific scaling factor and then rescaled to its original size. The watermark was detected with a reasonable detection value even when scaled by half its original size as it is illustrated in Fig. 5.8. Our scheme outperformed Cox et al.'s scheme, Huang and Shi's scheme as well as Lou and Yin's scheme as it is illustrated in Table 5.5.

5.2.3 Additive Gaussian Noise Attack

The watermarking scheme was also tested under additive Gaussian noise pollution, with zero mean and distinct variance values. Fig. 5.9 shows a watermarked image introduced to a Gaussian noise attack with 0.01 variance, which resulted in clearly visible distortions. The

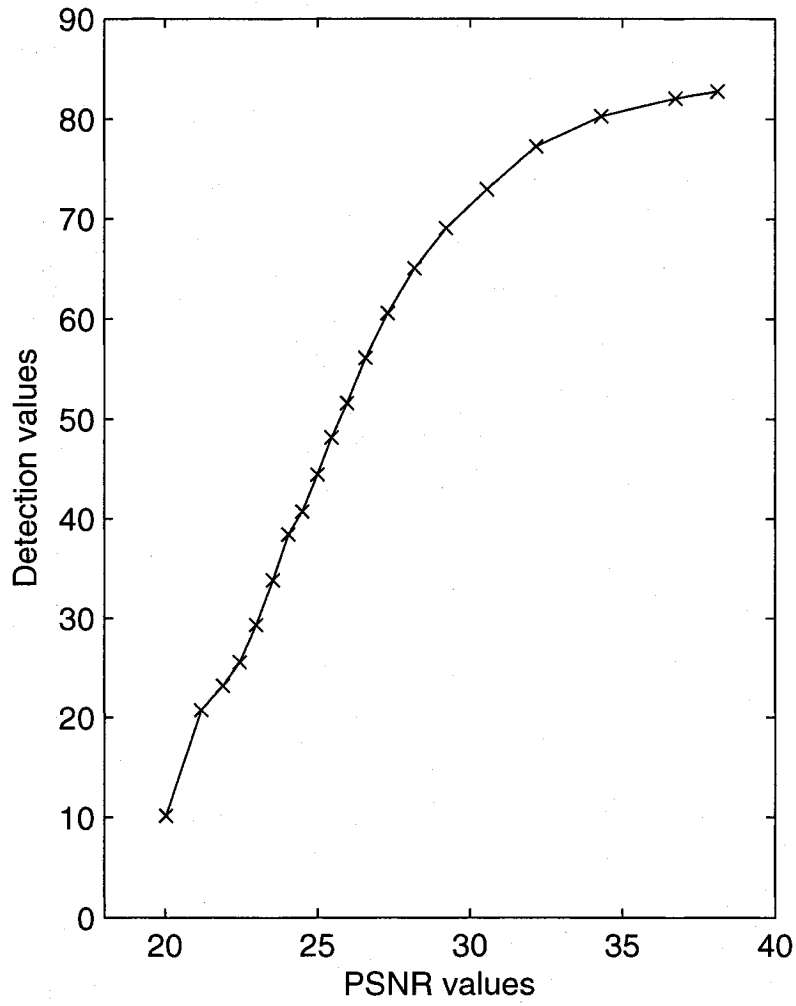
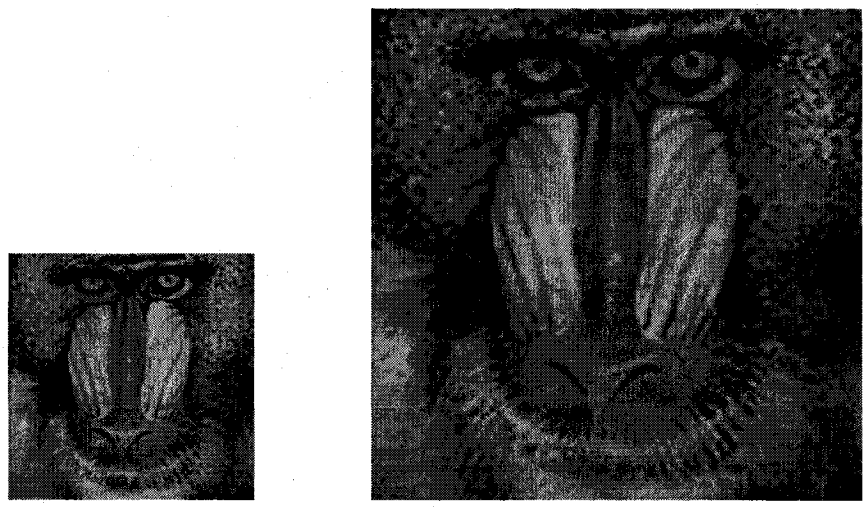


Figure 5.7: Detection values to several JPEG compressed images with different PSNR values.

Table 5.5: Scaling Attack

Scaling Factor	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
2	21.3	2.6	44.7	64.5
1.75	21.5	2.0	43.8	64.5
1.5	21.5	1.9	41.6	64.0
1.25	20.5	4.8	51.1	69.0
0.75	11.9	1.6	30.9	46.9
0.5	7.4	0.7	17.4	19.9



(a) (b)

Figure 5.8: (a) Image of Baboon (Fig.5.1(a)) after a 0.5 scaling attack, (b) Rescaling the image to illustrate the noticeable degradation of the image.

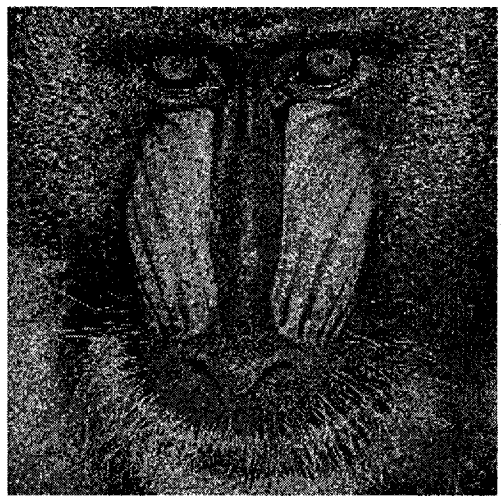


Figure 5.9: Image of Baboon (Fig.5.1(a)) after an Additive Gaussian noise attack.

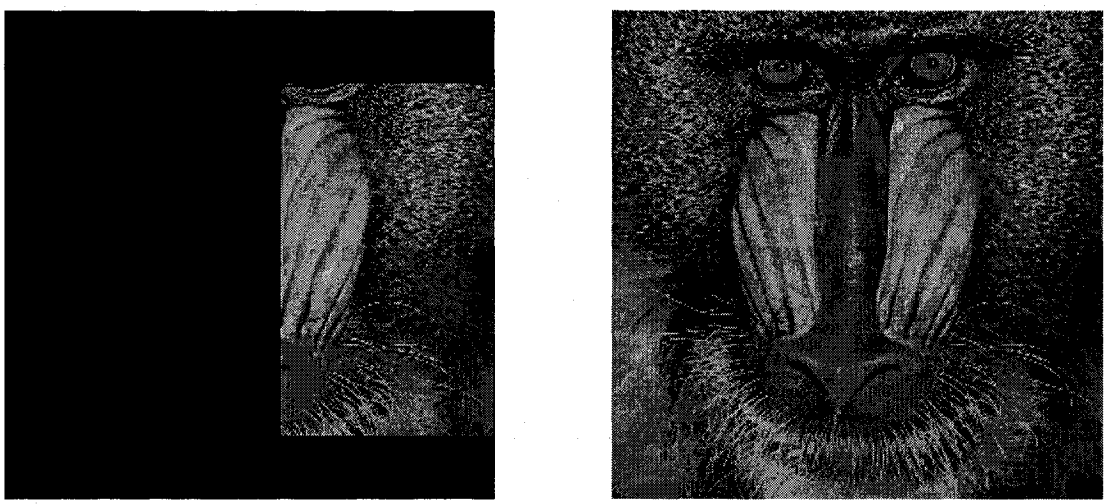
Table 5.6: Additive Gaussian Noise Attack

Variance (Units)	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
0.001	25.0	0.6	16.8	31.1
0.005	15.2	0.3	7.7	16.4
0.01	10.8	0.1	5.5	12.0

Table 5.7: Cropping Attack

Ratio (%)	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
30	24.2	32.0	51.3	68.2
50	20.5	32.3	48.1	57.7
70	16.4	17.8	32.8	46.7

response of the watermark detection for our scheme is 12.0, compared to 10.8, 0.1 and 5.5 for Cox et al.'s scheme, Huang and Shi's scheme, as well as Lou and Yin's scheme, respectively. The results are therefore satisfactory when compared to the other three methods as it is shown in Table 5.6.



(a) (b)

Figure 5.10: (a) Image of Baboon (Fig.5.1(a)) after cropping out 70% of its digital content, (b) Restored version of the cropped image where the missing data portions have been replaced with portions from the original image of Baboon.

5.2.4 Cropping Attack

Image cropping is another geometric attack that may occur to a watermarked image. Fig. 5.10(a) shows a cropped version of the watermarked baboon image in which 70% of its content has

been removed. The image in Fig. 5.10(b) is however used when performing the watermark detection process. It is constructed by replacing the omitted portion of the cropped image with portions from the original unwatermarked image of Fig. 5.1(a). Furthermore, Table 5.7 illustrates the detector response for all four schemes, where the watermarked image is cropped and 30%, 50% and 70% of its content is removed. The detection values clearly indicate that our method outperforms Cox et al.'s scheme, Huang and Shi's scheme, as well as Lou and Yin's scheme.

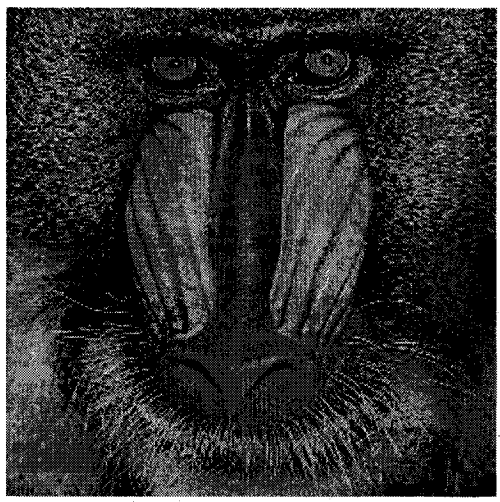


Figure 5.11: Image of Baboon (Fig.5.1(a)) after averaging five watermarked images in order to simulate a collusion attack.

Table 5.8: Collusion Attack

Watermark ID	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
1	14.1	18.6	27.2	36.4
2	13.5	20.4	27.7	37.6
3	15.1	18.8	27.1	35.8
4	14.4	20.3	26.3	37.1
5	14.1	20.2	25.8	36.2

5.2.5 Collusion Attack

This attack was achieved in a similar matter as in [8], where five different watermarked images were generated and averaged to form the image shown in Fig. 5.11. Fig. 5.12 illustrates the detector response of our scheme to 1000 randomly generated watermarks, where the five correct watermarks are set at the following indices: 150, 300, 450, 600 and 750. The response indicates that our scheme is resilient against collusion attacks. Furthermore, Table 5.8 illustrates the detection values for Cox et al.'s scheme, Huang and Shi's scheme, Lou and Yin's scheme as well as our scheme for all five watermarks embedded in the image.

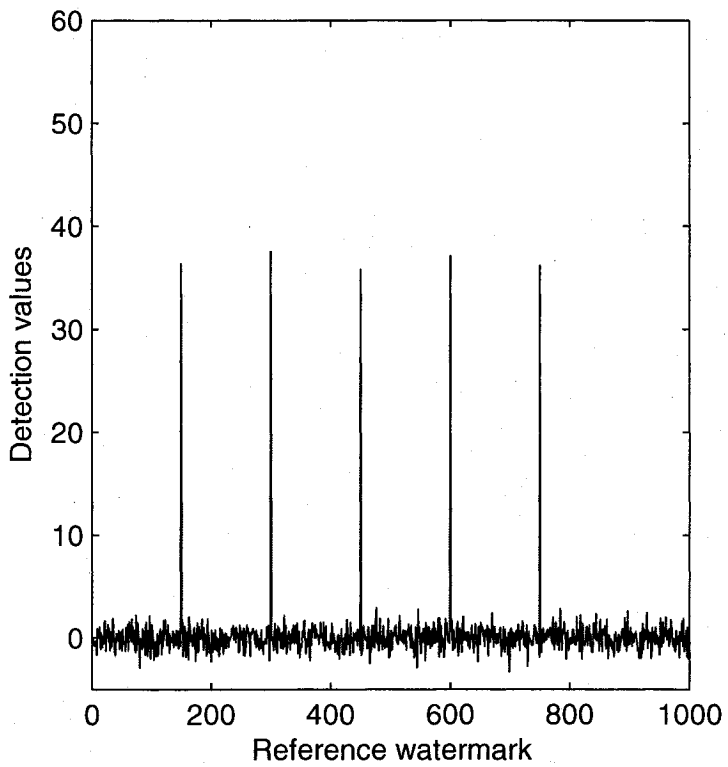


Figure 5.12: The detector response for our scheme, to 1000 randomly generated watermarks, where the five correct watermarks are set at the following indices: 150, 300, 450, 600 and 750.

5.2.6 Low-pass Filtering Attack

The watermarking image of Baboon was also low-pass filtered by means of a mean filter (Fig. 5.13), which essentially consists of a linear filter generally used for smoothing images. Table 5.9 illustrates the detector response of Cox et al.'s scheme, Huang and Shi's scheme, Lou and Yin's scheme as well as our scheme to a low-pass filtering attack.

Table 5.9: Low-Pass Filtering Attack

	Cox et al.'s scheme	Huang and Shi's scheme	Lou and Yin's scheme	Our scheme
Mean filter	5.8	0.2	3.61	10.5

Figure 5.13: Low-pass filtering attack introduced to the original image of Fig.5.1(a)

5.3 An Automated Test-bench

An automated test-bench was built with the aim of generating a robust watermark that meets the desired user-specifications. The test-bench's execution flow is illustrated in Fig. 5.14. The presented flow considers both the classical and the special case. In the former case a watermark with a maximum possible length is generated, whereas in the latter case, a watermark

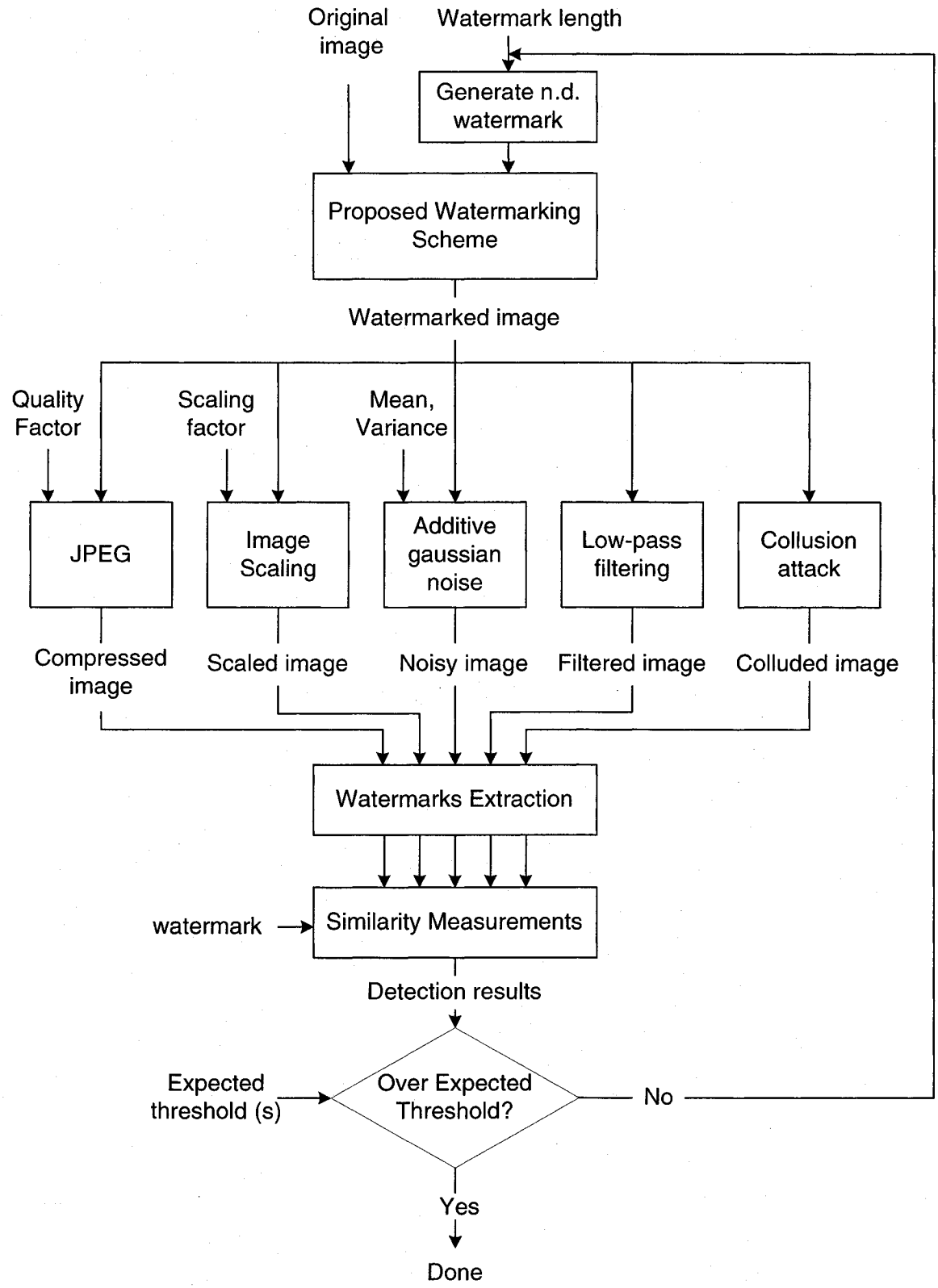


Figure 5.14: The execution flow of the automated test-bench.

with a specific length is considered. First, the proposed watermarking algorithm takes the original image and a normally distributed (n.d.) watermark as inputs. The generated output which corresponds to the watermarked image is then fed to various modules, in which different types of attacks are performed (including lossy compression (JPEG), image scaling, additive Gaussian noise, low-pass filtering as well as collusion attacks). Moreover, the lossy compression module will take on a quality factor as an additional input, whereas the image scaling and the additive Gaussian noise modules take on a scaling factor as well as a mean and variance parameters, respectively. Furthermore, the watermark extraction module then receives the altered watermarked images as inputs and attempts to extract the corresponding watermarks. Then, a similarity process is performed between the extracted watermarks and the original watermark. If the similarity results exceed or are equal to the expected threshold values, then the extracted watermark is approved, otherwise the entire process is repeated. Such an exhaustive testing approach does not however always reach a desired test target. In such a scenario, the system must either decrease the values of the expected detection values, or increase the adaptive watermarking strength by adjusting the scaling factor β (introduced in Section 3.3), at the expense of increasing the embedding distortion.

5.4 Summary

In this chapter the experimental results were presented in order to test the robustness and the imperceptibility of the generated watermark. The imperceptibility criterion was met by obtaining an acceptable PSNR measure of the watermarked images. Furthermore, the robustness of the watermark was evaluated by introducing various attacks to the watermarked images, including signal processing attacks (such as low pas filtering, lossy compression, additive Gaussian noise and collusion) and geometric attacks (such as cropping and scaling). The results proved that the watermark can survive all these attacks while remaining imperceptible. The obtained results are compared with three other popular schemes (Cox et al.'s

scheme [8], Huang and Shi's scheme [10], as well as Lou and Yin's scheme [6]) and demonstrate that our proposed scheme yields better results in terms of watermark imperceptibility and robustness. Finally, an automated test-bench was also developed in order to generate a robust watermark that meets some predefined user-specifications.

Chapter 6

Conclusions and Future Work

The demand for digital watermarking technologies is developing as the distribution of copyright material is becoming more widespread. In this thesis, we proposed an adaptive digital image watermarking algorithm that is based on a HVS model as well as a dynamic fuzzy inference system. The dynamic fuzzy inference system relies on statistical methods to accurately approximate the relationship found between all properties of the human perceptual system. Moreover, the dynamic behavior of the fuzzy inference system is provided by its *dynamic membership function engine* module as it can accurately adapt a membership function for any nonlinear input/output mapping. This strategy was used in order to determine the adaptive watermarking strength as well as the maximum possible watermark length that can be inserted in a cover image without introducing visual degradation. It was observed that the watermarking strength values were accurately determined even when the characteristics of the cover image are quite uniform. Furthermore, a *predictive watermark embedding* technique is used, which relies on the average power of the DCT coefficients in order to provide an accurate estimate of the embedding regions in which the watermark insertion should be performed. This approach is proved to restrict the watermark embedding to significant DCT coefficients and lower-frequency components. The application of the proposed method to color images also proved to be feasible. Moreover, robustness of the system to color images is suspected to be comparable to grayscale images, however, it remains to be

investigated. The experimental results demonstrated that the proposed scheme can embed an imperceptible watermark without degrading the watermarked image. Furthermore, the embedded watermark is very robust against signal processing attacks including JPEG compression, additive Gaussian noise, low-pass filtering, and collusion attacks, as well as geometric attacks such as image scaling and cropping. An important limitation of this scheme however, is that any geometric transformations (such as scaling, translation, rotation and cropping) performed on the watermarked image must be inverted prior to the watermark detection process. In addition, an automated test-bench was developed that relies on an exhaustive testing scheme to generate a watermark that meets the desired user-specifications. The test-bench was implemented in several independent modules, it can therefore be easily extendable by other image watermarking applications.

The computational complexity of the undertaken system was not taken into account since its primary application is assumed to be copyright protection. However, the proposed algorithm is not recommended for real-time applications as it relies on a defuzzification procedure that requires a considerable amount of computational effort. It would however be interesting to investiage whether it is feasible to incorporate the adaptive nature of the proposed fuzzy system into computationally efficient fuzzy inference systems, such as the Sugeno fuzzy model [60, 61] and the Tsukamoto [62] fuzzy model.

The future work is to enhance this technique by introducing a blind watermarking strategy. Furthermore, with minor modification such as incorporating a temporal masking effect into the visual model, this adaptive watermarking scheme could be extended to perform video watermarking. Moreover, the DFIS strategy can easily be associated with human auditory systems, to refine a perceptual model for audio when performing audio watermarking. Finally, it would be interesting to further extend the exploited visual model by introducing other properties (such as entropy masking) and consequently evaluate the performance of the dynamic fuzzy inference system under such conditions.

Bibliography

[1] I.J. Cox, M. L. Miller and J.A. Bloom, "Digital watermarking," *Morgan Kaufmann Publishers Inc.*, 2001.

[2] M. Yeung and F. Mintzer. "An invisible Watermarking Technique for Image Verification," *Proceedings of the IEEE International Conference on Image Processing*, vol. 1, pp.680-683, 1997.

[3] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," *Proceedings of the IEEE International Conference on Image Processing*, vol. 11, pp. 86-90, 1994.

[4] W. Bender, D. Gruhl, N. Morimoto and Aiguo Lu, "Techniques for data hiding," *IBM Systems Journal*, vol.35, pp.313-336, 1996.

[5] C. Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking," Independent Study, 2002.

[6] D.C. Lou and T.L. Yin, "Adaptive digital watermarking using fuzzy logic techniques," *Optical Engineering*, Vol. 41, pp.2675-2687, 2002.

[7] K. Wi and K. Xie, "Adaptive image watermarking scheme based on HVS and fuzzy clustering theory," *Proceedings of the IEEE International Conference on Neural Networks and Signal Processing*, Vol. 2, pp.1493-1496, 2003.

[8] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, Vol. 6, pp. 1673-1687, 1997.

[9] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," *Proceedings of the IEEE International Conference on Image Processing*, pp. 243-246, Sept. 1996.

[10] J. Huang and Y. Q. Shi, "Adaptive image watermarking scheme based on visual masking," *IEE Electronics Letter*, Vol.34, pp.748-750, 1998.

[11] V. Capellini, M. Barni, F. Bartolini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal Processing*, Vol. 66, pp.357372, May 1998.

[12] R. H. M. A. Juan and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector Performance analysis and a new structure," *IEEE Transactions on Image Processing*, Vol. 9, pp. 5568, Jan. 2000.

[13] M. Ramkumar, A. N. Akansu, and A. A. Alatan, "A robust data hiding scheme for images using DFT image processing," *Proceedings of the IEEE International Conference on Image Processing*, Vol. 2 , pp. 211-215, Oct. 1999.

[14] J.J.K.O. Ruanaidh, W.J. Dowling, F.M. Boland, "Phase watermarking of digital images, " *Proceedings of the IEEE International Conference on Image Processing*, Vol. 3, pp. 239-242, Sept. 1996.

[15] T. J. Chuang and J. C. Lin, "A new multiresolution approach to still image encryption," *Pattern recognition and Image Analysis*, Vol. 9, pp. 431-436, 1999.

[16] E. Muharemagic and B. Furht, "A Survey of Multimedia Watermarking Techniques, " *a chapter in Multimedia Security Handbook*, CRC Press, 2005.

[17] H. Lohscheller, "A Subjectively Adapted Image Communication System," *IEEE Transactions on Communications*, Vol. 32, pp.1316-1322, 1984.

[18] G. Wallace, "The JPEG Still Picture Compression Standard", *IEEE Transactions on Consumer Electronics*, Vol. 38, pp.1-17, 1992.

[19] P. Moulin, J. A. OSullivan, "Information-theoretic analysis of information hiding," *IEEE Transactions on Information Theory*, Vol. 49, pp. 563-593, March. 2003.

[20] B. Furht, E. Muharemagic, "Multimedia Security: Watermarking Techniques," IEC Comprehensive Report on Information Security, *International Engineering Consortium*, 2003.

[21] H. Lesley Ellen, "Canadian Copyright Law: Second Edition," *McGraw-Hill Ryerson*, 1995.

[22] http://www.digimarc.com/about/release.asp?newsID=158. Last accessed: November 2005.

[23] D. Green, and J. Swets, "Signal Detection Theory and Psychophysics," *New York: John Wiley and Sons, Inc.*, 1966.

[24] Recommendation ITU-R BT.500-10.ITU, "Methodology for Subjective Assessment of the Quality of Television Pictures," *Radiocommunication Assembly*,2000.

[25] M. Kutter and F. Hartung, "Introduction to Watermarking Techniques," in: S. Katzenbeisser, F. Petitcolas (Eds.), Proceeding of Information Hiding Techniques for Steganography and Digital Watermarking, *Artech House* , 2000.

[26] A.B. Watson, "DCTune: A technique for visual optimization of DCT quantization matrices for individual images," *Society for Information Display Digest of Technical Papers, XXIV*, pp. 946-949, 1993.

[27] Z. Wang, A.C. Bovik, "A Universal Image Quality Index," *IEEE Signal Processing Letters*, Vol. 9, pp. 81-84, 2001.

[28] N. Jayant and J. Johnston, "Signal Compression Based on Models of Human Perception," *Proceedings of the IEEE*, Vol. 81, pp. 1385-1422, 1993.

[29] B. Girod, "What's wrong with mean-squared error?," *Digital images and human vision, MIT Press*, 1993.

[30] F.W. Campbell and J.J. Kulikowski, "Orientation Selectivity of the Human Visual System," *Journal of Physiology*, pp.437-445, 1966.

[31] F.W. Campbell, J.J. Kulikowski and J. Levinson, "The effect of orientation on the visual resolution of gratings, " *Journal of Physiology*, pp.427-436, 1966.

[32] D. Storck, "A new approach to integrity of digital images," *Proceedings of IFIP Conference on Mobile Communication* , pp. 309-316, 1996.

[33] T. Terano, K. Asai, and M. Sugeno, "Fuzzy Systems Theory and its Applications," *Academic Press*, 1992.

[34] B. Kosko, "Fuzzy Thinking: The New Science of Fuzzy Logic." *New York Hyperion*, 1993.

[35] C. C. Lee, "Fuzzy logic in control systems: Fuzzy logic controller, part I," *IEEE Transactions on Systems, Man and Cybernetics*, Vol.SMC-20, pp.404-418, 1990.

[36] D. G. Schwartz, G. J. Klir, H. W. Lewis, and Y. Ezawa, "Applications of fuzzy sets and approximate reasoning," *Proceedings of the IEEE (special issue on consumer electronics)*, vol. 82, pp. 482-498, 1994.

[37] T. Terano, K. Asai, and M. Sugeno, "Fuzzy Systems Theory and Its Applications," *New York Academic*, 1992.

[38] J. Yen, R. Langari, and L. Zadeh, "Industrial Applications of Fuzzy Logic and Intelligent Systems," *New York: IEEE Press*, 1995.

[39] J.-S.R. Jang, C.T. Sun, and E. Mizutani, "Neuro-fuzzy and soft computing," *Prentice Hall*, 1997.

[40] L. X. Wang, "Back-propagation of fuzzy systems as nonlinear dynamic system identifiers," *IEEE International Conference on Fuzzy Systems*, pp. 1409-1418, 1992.

[41] L. Wang, J.M. Mendel , "Generating fuzzy rules from numerical data, with applications." *IEEE Transactions on Systems, Man and Cybernetics*, Vol. SMC-22, pp. 1416-1427, 1992.

[42] J.3. R. Jang, "Self-learning fuzzy controllers based on temporal back-propagation," *IEEE Transactions on Neural Networks*, vol. 3, pp. 714-723, Sept. 1992.

[43] S. Horikawa, T. Furahashi, and Y. Uchikawa, "On fuzzy modeling using fuzzy neural networks with back-propagation algorithm," *IEEE Transactions on Neural Networks*, vol. 3, pp. 801-806, Sept. 1992.

[44] L.A. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning," *Information Sciences*, Vol. 8, pp. 199-249, and vol. 9, pp. 43-80, 1975.

[45] N. Sakr, J. Zhao, and V. Groza, "Adaptive Watermarking based on a Dynamic Fuzzy Inference System," *Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp.950-953, May 2005.

[46] N. Sakr, J. Zhao, and V. Groza, "A Dynamic Fuzzy Logic Approach to Adaptive HVS-based Watermarking," *IEEE International Workshop on Haptic Audio Visual Environments and their Applications Ottawa*, pp. 121-126, October 2005.

[47] P. Moulin, A. Ivanovic, "The zero-rate spread-spectrum watermarking game," *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, pp. 1098-1117, April 2003

[48] Y. Jitsumatsu, Y.Hattori, T.A. Khan, T. Kohda, "Bit error rate in digital watermarking systems using spread spectrum techniques," *Proceedings of 2004 IEEE Eighth International Symposium on Spread Spectrum Techniques and Applications*, pp.890-893, 30 Sept. 2004.

[49] H. Malik, S. Khokhar, A. Rashid , "Robust audio watermarking using frequency selective spread spectrum theory," *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004. Proceedings.* , Vol.5, pp.385-388, May 2004.

[50] D. Kirovski, H.S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Transactions on Signal Processing*, Vol.51, pp.1020- 1033, Apr. 2003.

[51] H. Demirel, S. Sener, M. Gokmen, "Adaptive spread spectrum video watermarking," *Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference*, pp. 288-291, April 2004.

[52] P. Trammanontikul, T. Amornraksa, "Spread spectrum based spatial watermarking using partial embedding and reduced dynamic range detection," *Proceedings of IEEE International Symposium on Communications and Information Technology*, Vol.1, pp. 324-329, Oct. 2004.

[53] C.I. Podilchuk, Z. Wenjun, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, Vol.16, pp.525-539, May 1998.

[54] S. Suthaharan, S.W. Kim, H.K. Lee, S. Sathananthan, "Perceptually tuned robust watermarking scheme for digital images," *Pattern Recognition Letters*, pp.145-149, Feb. 2000.

[55] N.S. Jayant, J.D. Johnson, and R. Safranek, "Signal compression based on models of human perception," *Proceedings of IEEE*, Vol. 81, pp. 1385-1422, 1993.

[56] A. Lotfi and A.C. Tsoi, "Learning fuzzy inference systems using an adaptive membership function scheme," *IEEE Transactions on Systems, Man, and Cybernetic*, Vol. 6, pp. 326-331, 1996.

[57] R.R. Yager and D.P. Filev, "Essentials of Fuzzy Modeling and Control," *John Wiley*, 1994.

[58] E.H. Mamdani, and S. Assilian,"An experiment in linguistic synthesis with a fuzzy logic controller," *International Journal of Man-Machine Studies*, Vol. 7, pp. 1-13, 1974.

[59] NIST/SEMATECH. e-Handbook of Statistical Methods. http://www.itl.nist.gov/div898/handbook/. Last accessed: Oct. 2005.

[60] M. Sugeno and G.T. Kang, "Structure identification of fuzzy model," *Fuzzy Sets and Systems*, pp.15-33,1988.

[61] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," *IEEE Transactions on Systems, Man, and Cybernetics*, pp.116-132,1985.

[62] Y. Tsukamoto, "An approach to fuzzy reasoning method," *Advances in fuzzy set theory and applications*, pp.137-149, 1979.