Intelligent Perceptual Shaping of a Digital Watermark

by

Asifullah Khan
(May 2006)

A thesis submitted for the degree of Doctor of Philosophy to the Ghulam Ishaq Khan Institute of Engineering Sciences & Technology.

Faculty of Computer Science and Engineering
Ghulam Ishaq Khan Institute of Engineering Sciences and Technology,
Topi, Pakistan.


بسم الله الرحمن الرحيم

Dedicated to my parents
& my Wife

Acknowledgements

I would like to bow my head before Allah Almighty, the Most Gracious, and the Most Merciful, whose benediction bestowed upon me talented teachers, provided me sufficient opportunity, and enabled me to undertake and execute this research work.

This dissertation describes research undertaken at the Faculty of Computer Science and Engineering (FCSE), Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Topi, between **August** 2001 and **May** 2006, under the supervision of Prof. Dr. Anwar Majid Mirza, to whom I am indebted for suggesting the subject and for his encouragement, guidance and support throughout the research program. His advice, discussion, and effective comments were always a source of motivation.

I am also thankful to Dr. Sajid Qamar, and Dr. Syed Asif Gilani, who not only managed and administrated my research activities, but also guided and encouraged my innovative ideas and gave me fully moral support at every stage of my research work.

I would not have reached this stage but for the prayers, love and moral support of my mother and father, my wife Mrs. Shagufta Naz. I would like to thank my brothers, sisters, and all other well-wishers. I would also like to pay tribute to my friends Mr. Abdul Majid, Asmatullah, Shuja Amir Khan and Imran Usman.

I appreciate the help of Mr. Mohajir shah, Abdul latif, Fayaz Khan, Abdul Ghani, and other faculty staff for their cooperation. I would like to thank everyone at the FCSE for day-to-day support, advice, and patience. Obviously there are many other friends and colleagues, too numerous to list, who have helped with the progress of the work.

I am also extremely thankful to Dr. Javaid Bashir, Dr. Nasir Khan, and other colleagues, who not only allowed me to do my research work in

GIKI, but also appreciated my innovative ideas and give me fully moral support.

I acknowledge the enabling role of the Higher Education Commission of Pakistan and appreciate their financial support through its Indigenous PhD Scheme.

Table of Contents:

List of Figures:

List of Tables:

Abbreviations	Description
x	image matrix in spatial domain
$\mathbf{X}$	image matrix in DCT domain
$\mathbf{y}$	watermarked image matrix in spatial domain
$\mathbf{Y}$	watermarked image matrix in DCT domain
$\mathbf{w}$	watermark
$\mathbf{S}$	Spread Spectrum Square matrix
$\mathbf{b}$	expanded message Vector
$\boldsymbol{\alpha}$	perceptual mask for an image obtained using WPM
$\mathbf{X}_0, \mathbf{Y}_0$	Vectors representing some selected coefficients of the original and watermark images in DCT domain respectively
l_1, l_2	indices inside a DCT block
i, j	indices of a general matrix
A	information related to the conceivable attack
$SSIM_{es}$	SSIM measure at certain level of Estimated Robustness
BCR	Bit Correct Ratio
N_b	number of 8x8 DCT block in a Cover Image
N_d	number of selected coefficient inside an 8x8 block
$[\mathbf{k}]$	2-D discrete indices in DCT-domain
$GPSS$	Genetic Perceptual Shaping Scheme
$GPSF$	Genetic Perceptual Shaping Function
WPM	Watson's Perceptual Model

Abstract

Embedding of a digital watermark in a digital media is proving to be a workable solution for many of the recent problems like copyright protections and content authentication. However, the embedding of a digital watermark in a digital media is not without constraints. This requires perceptual shaping of a watermark in context of Human Visual System (HVS). The goal of this thesis is to develop a new watermarking scheme based on intelligent shaping of a digital watermark using GP. To achieve this goal, the research focuses on making efficient tradeoffs between two of the most important, but contradicting properties of a watermarking system; robustness and imperceptibility.

This thesis makes the following contributions: (1) An analysis of the importance of perceptual shaping of a watermark in making a trade off between robustness and imperceptibility is performed, (2) intelligent search technique, like GP, is used to exploit the characteristics of HVS in evolving superior perceptual shaping functions, (3) the concept of bonus fitness has been proposed to implement multi-objective fitness function, in the GP simulation. This helps in simultaneously handling the estimated robustness and imperceptibility requirements during embedding stage, and actual robustness during decoding stage, (4) we realize that perceptual shaping of a watermark is not only important for making a superior trade off, but could also be used to tailor the watermark in accordance to an anticipated attack, (5) watermarking systems are becoming more and more sophisticated, as such this thesis, using intelligent search technique like GP, points towards the solution strategy of many complex issues in watermarking that are difficult to be computed analytically. A series of empirical investigations are performed to analyze the performance of the genetically evolved perceptual shaping functions (GPSFs) using standard benchmark, which shows the effectiveness of our approach.

Publications Produced

Following are the publications produced during PhD research.

1. A. Khan and Anwar M. Mirza, "Genetic Perceptual Shaping: Utilizing Cover Image and Conceivable Attack Information Using Genetic Programming", International Journal of Information Fusion, Elsevier Science, 2006 (in press).

2. A. Khan, Anwar M. Mirza and A. Majid, "Intelligent Perceptual Shaping of a Digital Watermark: Exploiting Characteristics of Human Visual System," International Journal of Knowledge-Based Intelligent Engineering Systems, Vol. 9, 2005, pp. 1-11.

3. A. Khan, A. M. Mirza, A, Majid, "Optimizing Perceptual Shaping of a Digital Watermark Using Genetic Programming," Iranian Journal of Electrical and Computer Engineering (IJECE), vol. 3, pp. 144-150, 2004.

4. A. Khan, A. Majid, and Anwar M. Mirza, "Combination and Optimization of Classifiers in Gender Classification Using Genetic Programming," International Journal of Knowledge-Based Intelligent Engineering Systems, vol. 8, pp. 1-11, 2004.

5. A. Khan, A Novel Approach to Decoding: Exploiting Anticipated Attack Information Using Genetic Programming, International Journal of Knowledge-Based Intelligent Engineering Systems, 2006, (in press).

6. A. Majid, A. Khan and Anwar M. Mirza, "Combining Support Vector Machines Using Genetic Programming," International Journal of Hybrid Intelligent Systems, vol. 3, No. 2, pp-109-125, 2006.

7. A. Khan**,** Anwar M. Mirza and I. Usman, "Cascade Attack-resistant Perceptual Shaping of a digital Watermark", submitted in International journal of Information Fusion, Elsevier Science, 2006.

8. A. Majid, A. Khan and Anwar M. Mirza "Intelligent Combination of Kernels Information for Improved Classification", accepted in the Proc. of International conference on machine learning and its applications ICMLA'05, Los Angeles, California, USA, 2005.

9. A. Majid, A. Khan, and Anwar M. Mirza, "Improving Performance of Nearest Neighborhood Classifier Using Genetic Programming," in the Proc. of International conference on machine learning and its applications ICMLA'04, Louisville, KY, USA, 16-18 Dec. 2004.

10. A. Majid, A. Khan, and Anwar M. Mirza, “Gender Classification using Cosine Discrete Transformation: A Comparison of Different Classifiers”, Proceedings of the International Multi-topic (INMIC 2003), IEEE Conference, Dec. 2003.

11. A. Khan, S. A. Husain, A. M. Mirza, Asmatullah. “Optimizing ROC curves using Genetic Programming”,. In Procs. of TECHCOM Karachi, 2003.

12. Asmatullah, A.M. Mirza, A. Khan**,** “Blind Image Restoration Using Back Propagator”, Procs. of the International Multi-topic (INMIC 2003), IEEE Conference, 8,9 December Islamabad.

13. A. Majid, A. Khan and Anwar M. Mirza, “Combination of Nearest Neighborhood Classifiers Using Genetic Programming” in the International IEEE Conference (INMIC2005), Dec. Karachi, Pakistan.

Chapter 1

Intelligent Perceptual Shaping of a Digital Watermark

Digital watermarking has become a matter of more concern over the past few years as the urge to find solutions to the many problems related to the widespread usage of digital media is being sought. These issues, like copyright protection, are becoming hard to protect because the illicit attempts to override these by the adversaries, are also becoming ingenious. As such, two important realizations need to be considered. Firstly, intelligent search techniques are needed to find solutions to the complex issues concerning widespread usage of the digital media, which are difficult to be handled analytically. Secondly, there are very few restrictions on the adversaries, i.e. they are free to develop sophisticated attacks regularly. Therefore, there must be some adaptive technique to counteract these new attacks effectively by modifying the watermarking scheme.

The field of watermarking started with paper watermarks in 1282 in Italy. Thin wire patterns were added to paper moulds for generating marks [1]. However, not until eighteen century did paper watermarks become popular. They were primarily used for making trademarks, and as anti-counterfeiting measures on money and other documents. In 1996 Cox et al. [1], introduced the concept of spread spectrum based modulation of a watermark signal to provide robustness regarding the anti jamming property of spread spectrum modulation. This work brought about a major enhancement in coping with the diverse types of watermarking applications. After a year, Piva et al. [4], proposed the idea of blind watermarking, whereby the use of original cover image is not needed for detecting the watermark signal. Many researchers, then started exploiting these two concepts of spread spectrum based embedding and blind detection to develop novel watermarking approaches. Their detailed discussion can be found in [1, 2]. The third major development in watermarking originated through the work of Chen et al., whom introduced the concept of quantization index modulation based embedding of a watermark signal to implement host interference rejection [2]. This prompted the development of several structured coding based watermarking approaches, whose detail could be found in [1, 2]. Recent major advancement to the approaches of watermarking came through the work of Miller et al., who proposed the idea of informed embedding and coding based watermarking approach [1]. They argued

that since the cover image is available at the embedding stage so why should not it be exploited to encode the message and embed the resultant watermark in such a way that improves the effectiveness of the scheme.

Watermarking can be divided into two broad categories; robust watermarking and fragile watermarking. In robust watermarking, as its name implies, the watermark is supposed to be resistant to intentional and/or unintentional attacks. Here, the integrity of the watermark itself has to be withheld. On the other hand, fragile watermarking refers to the situation, where the watermark is used in verifying the integrity of its associated cover work. Its main application is content authentication, where any possible alteration to the content should be conveyed by the watermark. Watermarking has a wide variety of applications that ranges from owners identification to authentication encompassing the two broad categories of watermarking. Watermarking could be applied to different data, e.g. text, digital images, printed documents, audio signals, and digital videos etc. The present work is concerned with the robust watermarking of digital images.

Watermarking is an interesting field having intriguing affect of providing challenging problems, such as making a tradeoff between robustness and imperceptibility, or breaking of an already existing robust watermarking scheme through novel malicious attacks, or perhaps counterfeiting an intentional attack by proposing novel watermarking schemes. The motivation of this work came from studying and analyzing the importance of perceptual shaping of a watermark related to the first example of the above challenging problems that the field of watermarking encompasses.

Genetic Programming is a simple and effective technique that has recently found increasing applications such as automatic programming, combinatorial optimization and model induction. The focus of this thesis is to use GP for effectively finding a solution to the two important issues of a watermarking system, as discussed above; automatic development of the perceptual shaping module of the watermarking system and adaptation with respect to a specific attack.

Before being embedded, a watermark is usually shaped according to the content of the cover image. The model that exploits the sensitivities/insensitivities of Human visual System (HVS) to embed high power watermark at places not clearly discernable, is called perceptual model. Perceptual model are cover image independent, shaping the watermark according to the content of the cover image. Perceptual models thus play an important role by ensuring imperceptibility of a watermark. However, these models are complex and sub-optimal, as it is very difficult to model HVS. Therefore, global search mechanisms like GP must be used to further exploit the dependencies on the characteristics

of HVS. Using multi-objective fitness function concept, GP is able to develop such perceptual shaping functions that not only ensure imperceptibility, but also can offer high resistance against an anticipated attack.

1.1 Research Perspective

This thesis focuses on the understanding of perceptual shaping of a watermark, the ways it can be benefited from, and the development of perceptual shaping functions appropriate for a specific application. Specifically, some key contributions of perceptual shaping other than mere hiding a watermark are uncovered. Theoretically, modelling HVS has been difficult; therefore, the majority of perceptual modelling has been performed empirically. The approach taken in this thesis is also based on considering the optimization of perceptual shaping function by treating the tradeoff it makes between robustness and imperceptibility, as an optimization problem. Thus, the approach taken is based on the careful design and analysis of experimental studies.

1.2 Contributions

This thesis contributes in the following domains:

1) A study of perceptual shaping of a watermark demonstrates the complexity in making a tradeoff between robustness and imperceptibility.

2) Exploitation of the characteristics of HVS using intelligent search techniques, such as GP, to evolve superior perceptual shaping functions, especially, demonstrating the development of perceptual shaping functions tuned for a specific application of watermark.

3) An analysis of the watermark power-based estimated robustness measure shows that the estimated robustness may not closely represent the actual robustness at the decoding stage.

4) Proposing an idea of bonus fitness in GP-based simulation to incorporate, simultaneously, estimated robustness and imperceptibility requirements at embedding stage, and actual robustness at the decoding stage.

5) Realization and practical demonstration of the important fact that perceptual shaping of a watermark is not only important for just hiding the watermark, but it can also be used to spread the watermark in

such a way that it becomes highly resistant to a specific conceivable attack. In addition, such application-specific perceptual shaping functions are developed that are resistant against a battery of conceivable attacks.

6) Accentuating the need of using intelligent techniques, techniques that are able to obtain solutions to the watermarking issues that are becoming complicated with each new day. This consideration is important because the watermarking applications are increasing rapidly and becoming entangled and complex. Secondly, the technologies at the disposal of adversaries are also becoming advanced.

1.3 Structure of the thesis

Chapter 2 introduces the basics of watermarking; its properties, applications, domains in which it has been applied mostly. It discusses a data hiding approach that has been frequently used in this work as a test case to analyze the robustness versus imperceptibility tradeoff. Detail discussion about the perceptual shaping of a watermark has been given. Utilization of intelligent techniques, like GP, in watermarking has also been discussed. Chapter 2, in fact is a preamble to the rest of the chapters.

Chapter 3 is the first among the four chapters that describe the contributions of this thesis. Development of GPSF for the full frame Discrete Cosine Transform (DCT) domain based watermarking is discussed. An experimental comparison of the GPSF-based watermarking scheme in terms of the tradeoff is made with that of the scheme proposed by Piva et al., [4].

Chapter 4 develops GPSF for block-based DCT domain watermarking systems. First, the GPSF developed are compared with that of Watson's Perceptual Model (WPM), which has been regularly used in image compression. The method of developing improved perceptual shaping functions from the existing ones, such as WPM, is described next. The improvement that has been achieved both in imperceptibility and actual robustness, is discussed and analyzed.

Chapter 5 explores the realization of the fact that whether a perceptual shaping, at the embedding phase, could be used to thwart the threat from a conceivable attack. Results suggest that such strategy against conceivable attack could be highly effective. The performance of evolved GPSFs is analyzed with the help of standard benchmark attacks. During the evolution phase, the performance against the specific attack is introduced using the concept of bonus fitness.

Chapter 6 explores the role of perceptual shaping against a battery of conceivable attacks. It introduces those scenarios/applications, where the watermark has to deal with a set of attacks. Experimental results indicate that such application specific perceptual shaping functions could be very effective.

Chapter 7 presents conclusions in the context of results and obtained throughout the whole work. A recommendation for future research follows next.

Chapter 2

Basics of Digital Watermarking and Machine Learning

2.1 Digital Watermarking

In recent years, digital data is obtained and transmitted easily. This ease has instigated the wide appearance, transmission, and storage of digital data. The technologies that have supported this flooding of digital data are internet, World Wide Web (www), CD- ROM, and DVD. Although the widespread use of digital data has brought a lot of ease in different aspects, nonetheless, it is not without its side effects. These side effects are best presented by asking a question: with the digital data being so widely used, how are we going to address the issues like privacy, copyright infringement, authentication, and security? Three different technologies; information hiding, steganography and watermarking, are mostly used to address issues like these. These three technologies often use similar technical approaches and are closely related [1]. However, they do have some philosophical differences that affect their design towards a problem. Watermarking is defined as the practice of imperceptibly altering a work to embed a message about that work, whereas steganography represents the art of concealed communication. Here, the very existence of a message being kept secret. On the other hand, data hiding is a more general term and encompasses a wide range of problems that are either related to making information imperceptible or secret. A detailed discussion about the differences in these concepts can be found in [1, 2].

2.1.1 WM Applications:

Watermarking has a wide range of applications. Generally, a watermarking scheme is designed in view of its application, as the application poses certain requirements to be fulfilled [2]. Watermarking has found a large number of applications recently due to its advantages over the possible alternative technologies. Details of these advantages can be found in the 2nd chapter of [1]. Fragile and robust watermarking schemes usually have different applications. A few examples of watermarking applications consist of owner identification, tempering detection, copyright control, broadcast monitoring, transaction tracking and device control etc.

2.1.2 Imperceptibility:

Watermarking systems have some requirements that needs considerable attention. The most important of these is the imperceptibility requirement (also known as fidelity). A watermarking system is of very little use, if it distorts the cover image to the extent of being useless. Theoretically, the watermark should be invisible to a human eye, even on the highest quality equipment.

Although visible watermarks are usually more robust, for most of the applications it is advantageous for the embedded mark to be indiscernible to the human eye or ear. To date, researchers have attempted to conceal the watermark in such a way that it is not possible to be noticed. However, this constraint contradicts with other requirements such as tamper resistance and robustness.

2.1.3 Robustness:

A watermarked image could suffer different attacks before the watermark is retrieved, where; the attack is defined as any processing of the watermarked image that can damage the watermark [1, 3]. Resistance against attacks is thus, a fundamental issue while designing a watermarking system. With the exception of fragile watermarking systems, almost all watermarking systems need to be resistant against any intentional or unintentional processing of the watermarked image. This attribute of a watermarking system is usually called robustness. These attacks and their countermeasures are studied in the context of the watermark applications, as different applications are mostly concerned with a different set of conceivable attacks [1]. Therefore, while designing a watermarking system, its intended application and thus the corresponding set of conceivable attacks are of prime importance.

Digital music, images and video signals, normally include many types of distortions. Especially, in the digital image case, these include lossy compression, filtering, resizing, contrast enhancement, cropping, rotation etc. For the watermarking system to be practical enough, the watermark is supposed to be detectable even after such distortions. It is a general conclusion [1] that robustness against signal distortion could be achieved efficiently, if the watermark is placed in perceptually significant parts of the signal. This fact is related to the behavior of lossy compression algorithms, which work by dumping perceptually irrelevant data. The imperceptibility requirement of a watermark, however, seeks to encode information in extra bits that compression expects to remove. Thus, ideal watermarking and compression systems are usually at odds.

On the other hand, in case of malicious attacks, an attacker

intentionally tries to disable the watermark, often through a geometric distortion or through the addition of noise. In case of image watermarking, the resistance to geometric alterations, such as, rotation, resizing, translation, and cropping is still an open area of research. Yet, such operations are common and a proper solution needs to be developed so that watermarking techniques are productively applied for copyright protection.

2.1.4 Robustness versus Imperceptibility:

There is an intrinsic relation between the two most important, but contradicting properties of a watermarking system; robustness and imperceptibility. If we try to improve the watermark imperceptibility, robustness decreases and vice versa. Consequently, one needs to make a tradeoff according to the application domain. For this purpose, different methods, both in spatial as well as transformed domain, have been used to tailor a watermark according to the cover image [5-7, 15]. These watermarking systems are known to be image adaptive. On the other hand, most of the earlier approaches are not image adaptive and use a global watermarking strength for all the selected coefficients [4].

2.1.4.1 Watermark Robustness and Imperceptibility Measures

The imperceptibility of a watermark is generally measured in terms of weighted Peak Signal to Noise Ratio (wPSNR) [15], Watermark to Document Ratio (WDR) (40) and Structural Similarity Index Measure (SSIM) (52) . SSIM measure uses the hypotheses that HVS is highly adopted for extracting structural information. It is argued that natural image signals are highly structured, as the nearby pixel exhibit strong dependencies. These dependencies provide information about the structure of the object in an image, which are overlooked by the error-based measures. To estimate robustness during GP simulation, we use watermark power. We represent watermark power by mean squared strength (MSS) given as:

$$MSS = \frac{1}{N_b N_d} \sum_{u_1=1}^{N_b} \sum_{u_2=1}^{N_d} \alpha(u_1, u_2)^2 \qquad (2.1)$$

where, N_b is the total number of 8×8 blocks in the cover image, and N_d is the number of bandpass (low and mid frequency) DCT coefficients, and α is the perceptual mask.

We have used watermark power as an estimate of robustness, because in the testing and comparison phase of best evolved GPSF (section 5.3), the underlying watermarking technique is the same for both WPM and GPSF based perceptual shaping schemes. Hence, we assume that the MSS will provide a suitable measure of the estimated robustness at the embedding stage of the GP simulation.

2.1.5 Attacks: Categories and their Countermeasures

A watermarked data can be attacked in a variety of different ways. However, each application usually has to deal with a specific sequence of distortions. Cox et al. [1] and Barni et al. [29] have discussed in detail the types and levels of robustness that might be required for a particular watermarking application. They have discussed some of the attacks as well as their countermeasures. Keeping in view the expected distortions, several strategies are implemented to make a watermark system reliable. Few examples include; redundant embedding, selection of perceptually significant coefficients, spread spectrum modulation, and inverting distortion in the detection phase.
Voloshynovsky et al. (58,60) have classified attacks into four basic categories: removal and interference attacks, geometrical attacks, cryptographic attacks and protocol attacks. Intentional tempering, as opposed to the common signal processing attacks are difficult to be risisted. However, watermark attacks as well as their countermeasures are complex and still a topic of research. Therefore, in evaluating the potential of a watermarking technique to meet the robustness requirements, many assumptions are made especially about the attacker. For example, does the attacker know the watermarking algorithm, does he possess a detector that he can modify, what tools are available to him etc. Once the watermarking system is specified publicly, an attacker usually has more freedom as compared to a watermarker because the attacker is free to develop extra and more intricate attacks, while the watermarker can no longer amend it [1].

2.1.6 WM Domains:

Typical watermarking schemes are based on transform-domain techniques (DCT, DFT, Wavelets etc) [5, 6, 9, 13, 14] as well as spatial-domain methods [2, 15]. Watermarking in spatial-domain is straightforward and easy as compared to watermarking in transform-domain. Spatial-domain watermarking are also the first watermarking schemes that were investigated by researchers. On the other hand, transform-domain watermarking techniques have the convenience of

allowing us more direct understanding of the content of cover data. This ease in understanding the content is exploited in many ways. For example, perceptual models are used to make sure that the alterations are not easily visible. Watermarking based on transform-domain has thus become a widely used approach and is mostly encountered in literature. Different transform-domain techniques have their pros and cons and are mostly selected to exploit their specific features for a certain application. In the following section, we discuss the watermarking approach proposed by Hernandez et al. [5] that has been mostly used in our work. To explain this approach, let us denote the 2-D discrete indices in DCT domain by $[\mathbf{k}]$.

2.1.6.1 Block-based DCT Domain Watermarking Approach

We have used the spread spectrum based watermarking technique proposed by Hernandez et al. [5] to test the performance of evolved GPSF. This watermarking technique is oblivious as well as image adaptive, embedding message into the low and mid frequency coefficients of 8×8 DCT blocks of a cover image. They have shown that the statistical modeling of DCT coefficients using generalized Gaussian distribution, enable us to construct better detector/decoder structures than the simple Gaussian correlation receiver that is mostly used. This is because Gaussian distribution does not suitably model the DCT coefficients. Therefore, in order to model them appropriately, [5] and [6] have used generalized Gaussian and alpha-stable distribution respectively.

2.1.6.1.1 Watermark Generation and Embedding

Let us represent an image in the spatial domain as a discrete 2-D sequence $\mathbf{x}$ and its DCT transform as $\mathbf{X}$. The watermark that is being added to $\mathbf{X}$, generating watermarked DCT image $\mathbf{Y}$ is viewed as a 2-D DCT signal $\mathbf{W}$. Let M be a message, which is mapped to a codeword vector (figure 2.1). At the decoding stage, we have to retrieve this message M.

The codeword vector is then expanded to generate $\mathbf{b}$, with each element $b_i \ (i = 1.....N)$ repeated over a selected set of DCT coefficients. This redundancy bolsters robustness. The resulting signal $\mathbf{b}$ is further direct sequence spread spectrum (DSSS) modulated. The DSSS modulation is performed using 2-D pseudo random sequence (PRS) denoted by $\mathbf{S}$. The PRS behaves as spread sequence taking values ±1 and has zero mean. Next, to produce the watermark $\mathbf{W}$, the resultant signal is shaped according to the cover image. For this purpose, it is multiplied with perceptual mask $\boldsymbol{\alpha}$ (obtained by applying the perceptual model to the cover image in DCT domain) as follows:

$$\mathbf{W} = \boldsymbol{\alpha} \cdot \mathbf{S} \cdot \mathbf{b} \tag{2.2}$$

Adding this watermark to the original image, coefficient by coefficient as follows thus performs the embedding:

$$\mathbf{Y} = \mathbf{X} + \mathbf{W} \tag{2.3}$$

Here the watermark $\mathbf{W}$ is our desired signal, while the cover image $\mathbf{X}$ acts as an additive noise.

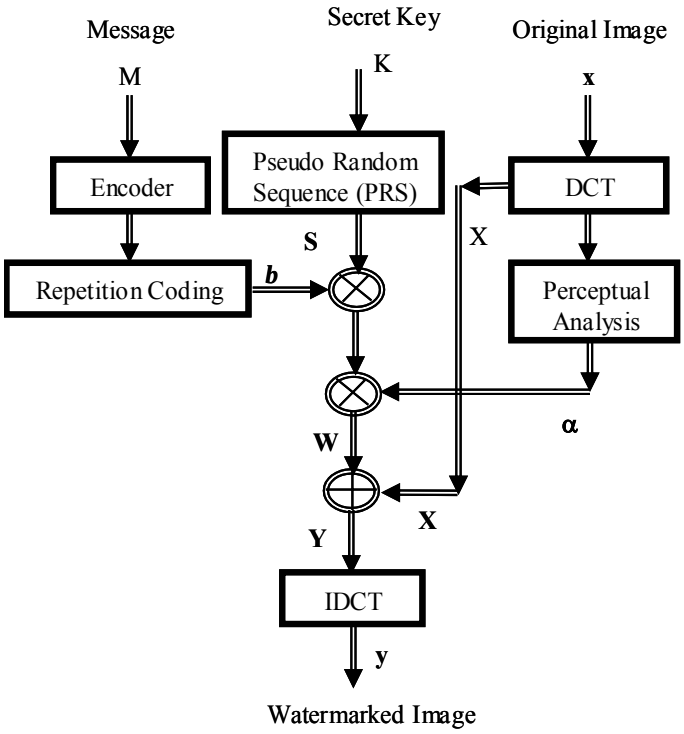

Figure 2.1 Hernandez's watermark embedding technique

2.1.6.1.2 Information Decoding

Hernandez et al. [5] have assumed that, the pdf of the original coefficients remains the same even after embedding. Based on this idea, they have obtained expressions for maximum likelihood (ML) decoder structures. The zero mean generalized Gaussian pdf is given as follows:

$$f_x(x) = A\, e^{-|\beta x|^c} \tag{2.4}$$

where both A and β are expressed as a function of the unknown parameters c and standard deviation σ :

$$\beta = \frac{1}{\sigma}\left(\frac{\Gamma(3/c)}{\Gamma(1/c)}\right)^{1/2} \quad , \quad A = \frac{\beta c}{2\,\Gamma(1/c)}$$

with the Γ denoting gamma function.

The unknown parameters c and σ should be estimated from the received image at the decoding stage. For this purpose, we follow [5] as discussed below.

Generalized Gaussian Parameter Estimation: The variance for each DCT coefficient of 8×8 block can be estimated using the estimator:

$$\hat{\sigma}^2(l_1,l_2) = \hat{\sigma}_Y^2(l_1,l_2) - \frac{1}{N_b}\sum_{\boldsymbol{k}} \alpha_{l_1,l_2}^2[\boldsymbol{k}] \tag{2.5}$$

Where $\alpha_{l_1,l_2}[\boldsymbol{k}] = \alpha[8k_1+l_1, 8k_2+l_2]$ is the 2-D sequence of PSF values corresponding to the (i,j) DCT coefficient and l_1,l_2 represent indices inside a block.

$$\hat{\sigma}_y{}^2(l_1,l_2) = \frac{1}{N_b}\sum_{\boldsymbol{k}} X_{l_1,l_2}^2[\boldsymbol{k}] - \left(\frac{1}{N_b}\sum_{\boldsymbol{k}} X_{l_1,l_2}[\boldsymbol{k}]\right)^2 \tag{2.6}$$

On the other hand, parameter c is a crucial parameter that dictates the shape of distribution. It should be carefully estimated for each image. Sometimes, an image independent value of c (0.5 or 0.8) can suffice [5]. In the present work, as in [5], the value of parameter c of the generalized Gaussian pdf for each (i,j) DCT sequence is estimated using the ML estimator. It is obtained by maximizing the log-likelihood function given as:

$$L(i,j) = -\frac{N_b}{c}\ln\left(\frac{1}{N_b}\sum_{\boldsymbol{k}}\left|X[\boldsymbol{k}]\right|^c\right) + N_b(\ln c - \ln\Gamma(1/c)) - \frac{N_b}{c}(\ln c + 1) \tag{2.7}$$

Generalized Gaussian based ML decoder: The Presence of a watermark is first verified through a process called watermark detection. Once, the watermark is detected, the message is then retrieved using the watermark decoder. Since our primary concern is to compare perceptual shaping functions in terms of decoding performance and not the detection performance. Therefore, before going into the decoding stage, we assume that the image is watermarked. Let us suppose there are L possible messages. In the verification process, our job is to obtain an estimate of the hidden message M from the marked image (figure2.2). We know that, in cases where there is less or no knowledge of the priory probabilities of the classes/hypotheses, priori probabilities are selected that make the classes equally likely. Hence if we assume that the messages are equiprobable, then it's fair to consider maximum likelihood (ML) test. The estimated message should satisfy:

$$\ln \frac{f(Y/\boldsymbol{b}_l)}{f(Y/\boldsymbol{b}_m)} > 0 \quad , \quad \forall \ m \neq l \tag{2.8}$$

Where $\boldsymbol{b}_l$ represents the code vector corresponding to the message being embedded while, $\boldsymbol{b}_m$ represents the code vectors corresponding to all other possible messages.

Hernandez et al. [5] have assumed that the sequences that are generated by considering each (i,j) DCT coefficient of all 8x8 blocks behave like generalized Gaussian and are statistically independent. Let us denote these 2-D sequences by $Q_{i,j}[\boldsymbol{k}]$, obtained as follows:

$$Q_{l_1,l_2}[k_1,k_2] \triangleq X[8k_1+l_1\ ,8k_2+l_2] \quad , \quad l_1,l_2 \in \{\ 0,\cdots,\ 7\ \} \tag{2.9}$$

The ML is then easily proved [5] to be equivalent to finding index $l \in \{1,2,\cdots\cdots,\mathrm{L}\}$ that obey

$$\sum_{\boldsymbol{k}} \frac{\left|Y[\boldsymbol{k}]-W_m[\boldsymbol{k}]\right|^{c[\boldsymbol{k}]} - \left|Y[\boldsymbol{k}]-W_l[\boldsymbol{k}]\right|^{c[\boldsymbol{k}]}}{\sigma[\boldsymbol{k}]^{c[\boldsymbol{k}]}} > 0 \quad , \quad \forall \ m \neq l \tag{2.10}$$

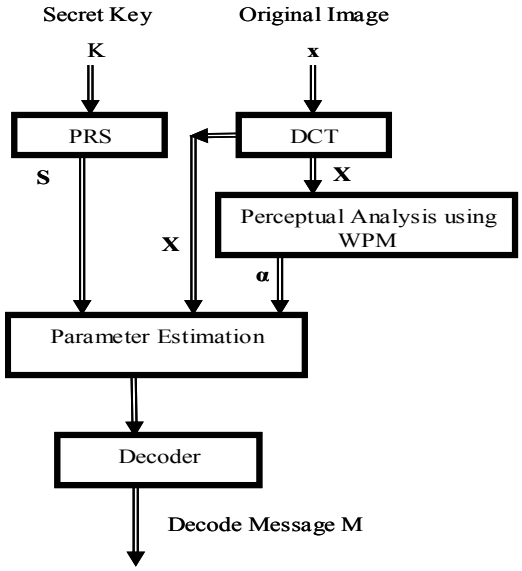

Figure 2.2 Hernandez's watermark decoding technique

We should remember that our bit could be +1 or −1 only i.e. a bipolar signal. If now G_i sample vector denote all the DCT coefficients of different 8×8 blocks that correspond to a single bit *i*, then one can prove [5] that the sufficient statistics of this sample vector is given by:

$$r_i \triangleq \sum_{\boldsymbol{k}\in G_i} \frac{\left|Y[\boldsymbol{k}]+\alpha[\boldsymbol{k}]S[\boldsymbol{k}]\right|^{c[\boldsymbol{k}]} - \left|Y[\boldsymbol{k}]-\alpha[\boldsymbol{k}]S[\boldsymbol{k}]\right|^{c[\boldsymbol{k}]}}{\sigma[\boldsymbol{k}]^{c[\boldsymbol{k}]}} \tag{2.11}$$

For bipolar signal i.e. $\boldsymbol{b} \in [-1,1]$, the estimated bits could be:

$$\hat{b}_i = \operatorname{sgn}(r_i) \qquad \forall \ i \in \{1,2,\cdots,N\} \tag{2.12}$$

2.2 Perceptual Shaping of a Digital Watermark

Development of an adaptive watermarking scheme to tailor a watermark requires the understanding of the cover image in the context of human visual system (HVS). In spatial-domain, this understanding means knowing the distribution of smooth and textured areas in a cover image. In transform-domain, it means knowing the distribution of low, mid and high frequency components of the cover image. Thus, in order to hide the watermark, the watermark is tailored/shaped using perceptual models that exploit sensitivities/insensitivities of HVS. The better a perceptual model is, the better is the perceptual shaping and hence imperceptibility of the watermark. Perceptual model can be viewed as a perceptual shaping function (PSF), providing maximum allowed alteration to a pixel value (or DCT coefficient) that is not observed by a human observer.

These perceptual models are able to learn the content of a cover image by exploiting the sensitivities/insensitivities of an HVS. They take advantage of frequency sensitivity models that are based on viewing conditions as well as the cover image dependent, luminance sensitivity and contrast masking effects. Frequency sensitivity describes the HVS sensitivity to sine wave gratings at different spatial frequencies and depends only on the surrounding conditions. Luminance sensitivity on the other hand, is a measure of the effect of detectability threshold of a signal on a constant background. It depends on the average luminance value of the background as well as on the signal's luminance level. In block-based DCT case, the DC coefficient of each block dictates the luminance sensitivity for that block. The third important property of HVS that is exploited for hiding a watermark is the contrast masking. It represents the detectability of one signal in presence of another signal. This masking (hiding) effect increases when the masking signal and the signal to be masked have same spatial frequency, orientation and location. In block-based DCT, the AC coefficients dictate this behavior. In our present investigations, we have compared the developed GPSF with that of WPM.

In watermarking schemes based on DCT-domain techniques, mostly Watson's perceptual model [16, 18] is used to shape the watermark. Watson's perceptual model is based on Ahumada's work [17] and has been used in DCT-based JPEG compression. Podilchuk et al. [7], using Watson's perceptual model, have attempted to exploit HVS for watermark shaping in DCT domain. They propose image adaptive watermarking and use the concept of Just Noticeable Difference (JND) as a measure of subsequent distortion being caused by the watermark embedding. Hernandez et al. [5] and Briassouli et al. [6] have applied the same idea in spread spectrum-like DCT domain watermarking. Rather than comparing magnitude of DCT coefficients with JND, they directly use the Watson's perceptual model as a perceptual shaping function. Cox et al. [19] have also used the Watson's perceptual model for perceptually shaping the watermark in their informed coding and embedding-based watermarking technique. Watson's perceptual model, although widely used in DCT domain-based watermarking, is not the optimal perceptual model [1]. Firstly, the model is built on empirical studies and is not based on extensive search methods. Secondly, it neglects certain effects like spatial masking in frequency domain [5].

2.2.1 Watson's Perceptual Model (WPM)

Consider an image matrix $\mathbf{x}$ in spatial domain. The image is transformed to matrix $\mathbf{X}$ by applying 8x8 block DCT. According to the WPM, we define the visibility threshold $T(i,j)$ for every (i,j) DCT coefficient of 8x8 block as follows:

$$\log T(i,j) = \log\left(\frac{T_{\min}\,(f_{i,o}^2 + f_{o,j}^2)^2}{(f_{i,o}^2 + f_{o,j}^2)^2 - 4(1-r)\,f_{i,o}^2 f_{o,j}^2}\right) + u\left(\log\sqrt{(f_{i,o}^2 + f_{o,j}^2)} - \log f_{\min}\right)^2 \quad (2.13)$$

where $f_{i,o}$ and $f_{o,j}$ denotes the vertical and horizontal frequencies (cycles/degree) of the DCT basis functions respectively. $T_{\min}$ is the minimum value of $T(i,j)$ corresponding to the minimum frequency $f_{\min}$. The rest of the parameters are also set empirically [16-17]. The effect of luminance sensitivity is considered by correcting this threshold corresponding to average luminance of each block:

$$T'(i,j) = T(i,j)\left(\frac{X_{o,o}}{\overline{X}_{o,o}}\right)^{a_T} \quad (2.14)$$

where $X_{o,o}$ is the DC coefficient of each block and $\overline{X}_{o,o}$ represents the average screen luminance =1024 (for an 8-bit image). The effect of contrast masking is incorporated by the following relation:

$$T^*(i,j) = \max\left[\,T'(i,j)\;,\; \left|T'(i,j)\right|^{1-\omega} X(i,j)^{\omega}\,\right] \quad (2.15)$$

where $X(i,j)$ is AC DCT coefficient of each block and ω has been empirically set to a value of 0.7. These allowed alterations represent the perceptual mask denoted by $\boldsymbol{\alpha}$.

Watson's perceptual model although, fair enough to give us imperceptible alterations, is not an optimum PSF. This is because some effects like spatial masking in frequency domain are ignored as well as many of the constants are set empirically. Based on this, we have tried to evolve genetically an effective perceptual shaping function.

2.3 Evolutionary Algorithms: Computational Intelligence-based Approaches

Evolutionary Algorithms (EAs), inspired by natural selection and genetics, is a field of Computational Intelligence. Like other meta-heuristic methods, EAs implement a search strategy supplemented by an objective function and operators. Following are the basic types of EAs:

1. Genetic Algorithms
2. Evolutionary Programming
3. Genetic Programming
4. Evolutionary Strategies

The distinction in these approaches is largely due to the way they implement the search strategy of EAs.

2.3.1 Genetic Programming: The Basics

The term genetic programming (GP) has been introduced independently by Koza and Garis in 1990. Since then it has received widespread applications in research academia. It is a category of evolutionary algorithms, which are inspired by the mechanism of natural selection.

GP will converge over successive generations towards the global (or near global) optimum. Why this simple operation should generate rapid, valuable, and robust techniques is largely because Evolutionary Algorithms combine direction and chance in the search in an effective and efficient manner. Since population implicitly contain much more information than simply the individual fitness scores, Evolutionary Algorithms combine the good information hidden in a solution with good information from another solution to produce new solutions with good information inherited from both parents, hopefully leading towards optimality.

The ability of the algorithm to explore and exploit simultaneously, a growing amount of theoretical validation, and successful application to real-world problems supports the conclusion that Evolutionary Algorithms are a powerful, robust optimization technique.

2.3.1.1 The Primitives of GP

The terminals to an individual GP tree act like inputs to a program (more like an independent variable of a function) and may be constants or variables. On the other hand, non-terminal nodes are called functions. These functions process a value that is given as an argument. Functions are usually composed of statements and operators and are mostly application specific. Together these two primitives: terminals and functions make up a GP tree, representing an individual solution.

Functions and terminals in GP simulation should be powerful enough to represent an individual solution to the problem. Most trivial functions being used are *PLUS, MINUS, DIVISION, AND, TIMES* and *EXP* etc. [24, 28, 30].

2.3.1.2 Structure of GP Program

In GP simulation, an individual candidate solution of a population is represented through a data structure, mostly by a tree. At the beginning of GP simulation, these individual structures are randomly constructed from the GP primitives. During the process of generating offspring from the selected parents, the genetic operators are applied on these data structures.

2.3.1.3 Strategies for Initializing GP Population

The initial population of a GP simulation is formed by randomly generating trees. This randomness is achieved through different ways and has a profound effect on the behaviour of the subsequent simulation. Three most important strategies are:

- The Full method
- The Ramped Half - and - Half method
- The Grow method

2.3.1.4 Genetic Operators

To produce a new generation, mainly three operators: replication, mutation and crossover are used in GP (figure 2.3). Replication is mere copying an individual into the next generation without any change. In

mutation, a small part of an individual's genome (genetic representation) is changed. This small random change often brings diversity in the solution space and helps to avoid trapping in local minima/maxima. On the other hand, crossover creates an offspring by exchanging genetic material, usually between two individual parents. In fact, crossover tries to mimic recombination and sexual reproduction. It mainly helps converging onto an optimal solution.

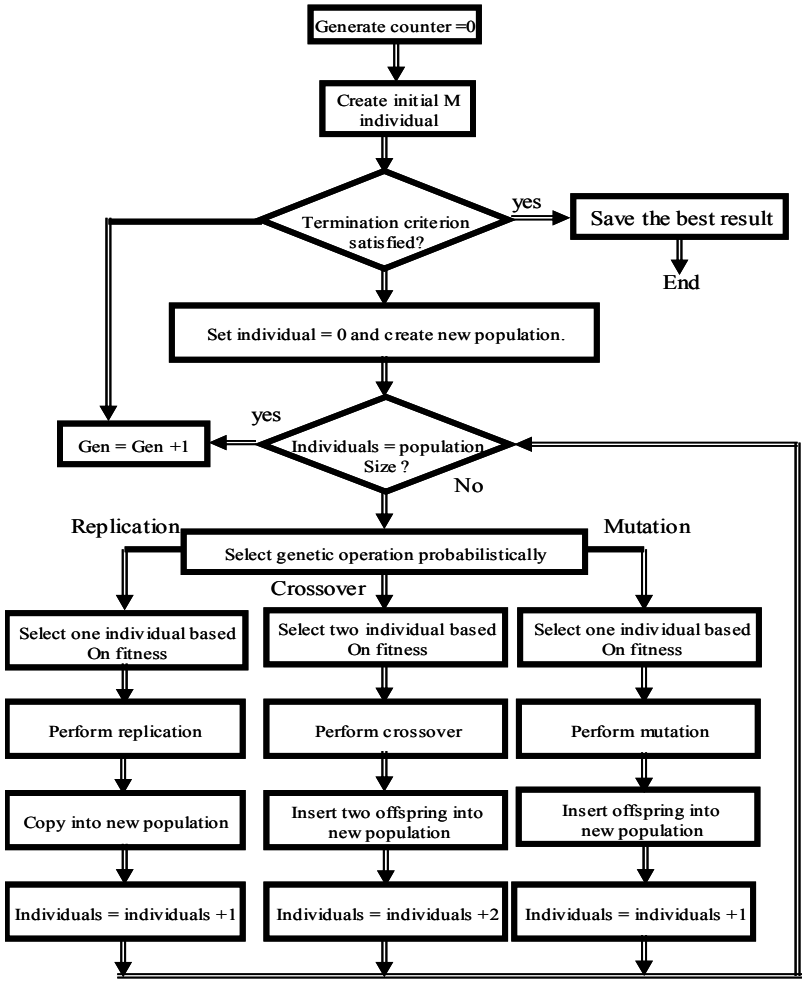

Figure 2.3 GP search mechanism

2.3.1.5 Fitness Criteria and Selection Strategies

In a generation, every candidate solution is evaluated and scored using the fitness function, is application dependent. The survival of fittest is implemented by retaining the best individuals. The rest are deleted and replaced by the offspring of the best individuals. Together (the retained ones and the offspring) make a new generation. Some offspring may have high score than their parents in the previous generation.

The whole process is repeated for the subsequent generations. With the scoring and selection procedure in place, each new generation has, on average, a slightly higher score than the previous one. In this way the solution space is refined generation by generation and thus converges to the optimal/near optimal solution. For a detailed study, one may refer to [24, 28, 30].

The user according to the application defines the fitness function. The better an individual is performing at this function; the better its survival is and thus better is its chances of producing children for the next generation.

2.3.1.6 Control Parameters:

There are certain parameters that affect the basic operation of the GP simulation. They comprise of population size, the maximum number of generations, and the number of individuals chosen for the next generation, and so on. These parameters do not affect the GP simulation directly, but their values can affect global properties like the number of generations needed before a solution is found.

2.3.1.7 Termination Criterion:

There must be a way for the GP simulation to end. This happens when the generation count reaches maximum number of generations, or when a program surpasses a threshold fitness level.

2.4 Machine Learning: The Basic Concept

Machine learning is the study of computer algorithms that improve automatically through experience. It is a process that starts with the specification of the learning domain and ends with testing. Machine learning systems are applied to the learning domain, where the researcher identifies features of the domain that are useful for the prediction of accurate useful results.

The selection of features, however does not completely define the whole process. The learning process occurs by training, where the ML systems attempts to learn from examples. Finally the quality of learning is appraised by testing the ability of the best solution of the ML system to predict outputs from a test set. The test set must contain different examples than those of train test. The ability of ML system to test set is often called generalization.

2.4.1 GP as a Machine Learning System

GP includes a population of computer programs that improve automatically as they experience the data on which they are trained. As

such, GP is a type of machine learning system (24). It has already changed the view on a variety of problems that machine learning has successfully handled and has mostly exceeded the performance of other machine learning systems(27). According to the terminology used in machine learning, the fitness cases in GP are referred as training cases. The corresponding learning on the training set means that the GP system must learn a computer program that is able to predict the outputs of the training set from the inputs. The best-evolved computer program of the GP simulation is then tested on the test set. Thus GP systems use a learning algorithms based on an analogy with natural evolution which in case Multilayer feed forward neural networks, analogy with biological nervous systems is considered.

2.4.2 Watermarking using Machine Learning Techniques

Recently machine learning techniques are applied in the field of watermarking. Most of them are related to the detection of a hidden message i.e. classifying watermarked and unwatermarked works. Lyu et al [20] have used high order statistics as features and Support Vector Machine (SVM) as classifier for detecting hidden messages in an image. Fu et al [21], have proposed optimal watermark detection by exploiting the generalization capabilities of SVM. Yu et al [22], have used neural networks in watermarking for enhancing robustness against some of the common attacks.

On the other hand, Pereira et al [23] have used Linear Programming to optimally embed a watermark in transform-domain, subject to a linear set of constraints in spatial-domain. Huang et al [8] use Genetic Algorithms at the embedding stage. They propose optimal embedding positions in a block-based DCT domain watermarking. The use of machine learning techniques has thus proven its worth in the field of watermarking. Following the same concept of exploiting machine learning capabilities for improvement of watermarking schemes, we have been employing GP for developing optimal perceptual shaping functions –perceptual shaping functions that make an optimal tradeoff between robustness and imperceptibility [9-11]

2.5 Genetic Perceptual Shaping Scheme (GPSS):

We first give a brief description of our proposed technique of intelligent perceptual shaping of a watermark using GP. The rest of the chapters of this thesis will explain in detail the different approaches that we have taken for intelligently shaping a watermark. The basic architecture of our proposed scheme for developing a PSF is shown in

figure 2.4. Three different modules supplement each other in a cyclic fashion. Using the robustness versus imperceptibility tradeoff as an optimization problem, GP module produces a PSF. The watermark generated by the watermarking scheme is shaped by this PSF. The imperceptibility of this shaped watermark is then used as a scoring criterion in the GP module. In this way, the GP module evaluates the performance of its several generated PSF. In a separate stage, the best-evolved GPSF is compared with the Watson's perceptual model.

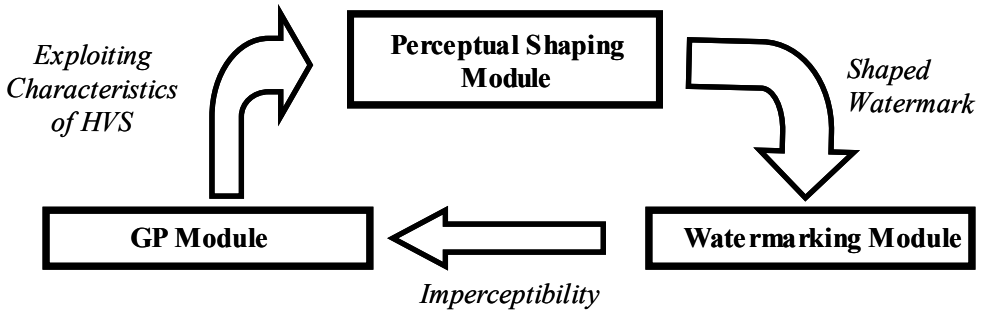

Figure 2.4 Basic architecture of GPSS

Chapter 3

Perceptual Shaping of Full Frame DCT Domain-based Watermark

A watermark is generally embedded in the selected coefficients of the transformed image using a carefully chosen watermarking strength. Choice of a good watermarking strength, to perceptually shape the watermark according to the cover image is crucial to make a tradeoff between the two conflicting properties, namely, robustness and imperceptibility of the watermark. Traditionally, a constant watermarking strength obtained from spatial activity masking and heuristics has been used for all the selected coefficients during embedding. In this Chapter, we present an innovative scheme of perceptually shaping watermark to the cover images. We consider this tradeoff as an optimization problem and investigate an evolutionary optimization technique to find optimal/near-optimal perceptual shaping function for full frame DCT domain-based watermarking system. First, we describe the full frame DCT domain-based watermarking scheme proposed by Piva et al. [4]. We have used this scheme to develop GPSF.

3.1 Introduction

In digital watermarking, using the overall information about the image characteristics, the watermark is generally embedded in the whole image with the same strength without considering the local distribution of the cover image content. This embedding usually leads to unwanted visible objects, especially in regions, which are more sensitive to noise (smooth regions). In order to decrease these deformations, the watermarking strength should be decreased. However in doing so, robustness is lost. Therefore one needs to perceptually shape the watermark, providing a suitable watermarking strength for each of the selected DCT coefficients.

Generally, watermarking in frequency domain has been used [4, 31, 32, 33], as it allows the direct understanding of the contents of the image. Consequently, the characteristics of HVS can be taken into account more easily when one needs to decide the strength and position of the watermark to be added to the image. Boland et al. [34] have employed frequency domain transformation on block by block basis, while Barni et al. [31] and Cox et al. [32], have employed transformation to the image as a whole. Recently Cox et al. [19] and Hernandez et al. [5]

have used Watson's perceptual model [16] to perceptually shape the watermark according to the cover image before embedding. But their watermarking scheme is based on 8x8 block-based *DCT* domain watermarking. On the other hand, rather than optimizing perceptual shaping, Huang et al. [2,8,35] use Genetic Algorithms to find the optimal embedding positions in a block-based *DCT* domain watermarking schemes to improve marked image quality. In the present work, we are concentrating on the optimization of perceptual shaping of a watermark in the whole *DCT* domain watermarking system as used in [4].

DCT domain watermarking techniques are important due to the extensive use of the *DCT* in many image and video compression standards. The *DCT* based watermarking techniques provide good resistance against many attacks, except geometrical attacks like rotation. In this work, nonetheless keeping high invisibility of the watermark, we have improved watermark resistance by embedding a watermark of high overall strength.

3.2 Full Frame DCT-domain Watermarking Scheme

Digital watermarking is a process of embedding information (or signature) directly into a multi media data by making small modifications. These small modifications however should not affect the visibility of the image largely. Similarly, these small modifications should be able to survive intentional and unintentional attacks (i.e. should have robustness). Robustness is difficult to achieve, since both security levels and operational requirements are usually application dependent. In this work we are focusing on image watermarking which means that image should be able to survive common image preprocessing techniques and forgery attacks. In order to achieve invisibility, Cox et al. [32] proposed to use a pseudo-random sequence of real numbers as the watermark. These sequences should be numerous and easily retrievable. Following his idea we are using a pseudo-random sequence of real numbers as the watermark. This whole process can be viewed as a communication task with the watermark acting like a signal and the cover image acting just like a channel. The intentional attacks and unintentional image processing can thus be considered just like the noise, which the signal should be immune to. Lastly, the scheme should have the ability to detect or extract the signal from the corrupted image.

Based on the need of original cover image during the detection stage, there are mainly two types of watermarking techniques [3]: one, which requires the original image [32] and the other that does not [2]. We have followed the later approach, which is also called a blind detection scheme. In the following, we explain the various steps taken in the full frame DCT-domain watermarking scheme proposed by Piva et al. [4].

3.2.1 Watermark Embedding and Detection Processes

Let $\mathbf{x}$ denote an original image of size $M \times N$ then it's DCT transformed image $\mathbf{X}$ is given by:

$$X(u,v) = \frac{2}{\sqrt{MN}} a(u)a(v) \times \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I(m,n) \cos\left[\frac{(2m+1)u\pi}{2M}\right] \cos\left[\frac{(2n+1)v\pi}{2N}\right] \quad (3.1)$$

where

$$a(u) = \begin{cases} \sqrt{1/M} & for \quad u = 0 \\ \sqrt{2/M} & \quad\quad u = 1,2,\cdots,M-1 \end{cases} \quad (3.2)$$

and

$$a(v) = \begin{cases} \sqrt{1/N} & for \quad v = 0 \\ \sqrt{2/N} & \quad\quad v = 1,2,\cdots,N-1 \end{cases} \quad (3.3)$$

In order to select coefficients for embedding, a zigzag scanning of the transformed image in DCT domain is done [4]. It is equivalent to sorting according to importance, since the perturbation in the low frequency components is generally more perceivable to human eyes than high frequency components. The first L coefficients are left intact and the watermark is added to the next G coefficients. Suppose the first L+G DCT coefficients are:

$$\mathbf{X_0} = \{X_1, X_2, \cdots, X_L, X_{L+1}, \cdots, X_{L+G}\} \quad (3.4)$$

And the pseudo-random watermark is given by:

$$\mathbf{S} = \{S_1, S_2, \cdots, S_G\} \quad (3.5)$$

The new coefficients after embedding are:

$$Y_{L+i} = X_{L+i} + \alpha |X_{L+i}| S_i \quad (3.6)$$

where α is the watermarking strength and i runs from 1 to G. These new coefficients are re-inserted into the zigzag scan. Watermark embedded image in spatial domain is then obtained by taking the inverse of modified DCT coefficients.

In the detection process, Piva et al. [4] have used the reverse process for a given corrupted image. First the $M \times N$ DCT coefficients matrix is computed. It is then re-ordered by the zigzag scan. The L+1 to L+G

coefficients are selected to form a vector $\hat{\mathbf{Y}}$ as follows:

$$\hat{\mathbf{Y}}_{\boldsymbol{0}} = \left\{\hat{Y}_L, \hat{Y}_{L+1}, \cdots, \hat{Y}_{L+G}\right\} \tag{3.7}$$

The correlation Z of $\hat{\mathbf{Y}}$ and any mark $\mathbf{S}_{\circ}$ is calculated as:

$$Z = \frac{1}{G}\hat{\mathbf{Y}} \cdot \mathbf{S}_{\circ} = \frac{1}{G}\sum_{i=1}^{G} \hat{Y}_{L+i} \cdot S_{0i} \tag{3.8}$$

By comparing the correlation Z to a pre-defined threshold, they determine whether watermark exists or not.

3.2.2 Perceptual Shaping of a Watermark generated in Full-frame DCT domain

In order to perceptually shape a watermark according to the cover image, one has to exploit the sensitivity/insensitivity of *HVS*. But *HVS* is a complex system that is mainly composed of three parts: a receiver with a pre-processing stage (the eye and the retina), a transmission channel (the optic nerve), and a processing channel (the visual cortex). Efforts to understand and model *HVS* have partly remained fruitless due to the lack of our knowledge about the way that a stimulus is processed through the huge neural network of our brain. Different techniques have been used to exploit its properties and thus hide (mask) a signal into another signal. For example, edges in images can mask signals of much greater amplitude than regions having nearly constant intensity [36]. This fact is exploited by spatial masking. But spatial masking is relatively limited and is concentrated in a location only few pixels close to the edge. This makes it difficult for use in watermarking schemes. However, it is observed that regions in an image that are not smooth and have sharply changing luminance are able to mask other signals significantly. This phenomenon is called noise masking and is difficult to be modeled [37].

The concept of entropy masking has also been used, which states that masking is a function of the degree to which knowledge about a mask is uncertain [37]. The noisier a region is, the greater the entropy is. Nadenau et al. [38] gave the concept of similarity masking, which states that *HVS* is more sensitive to a distortion that does not look like its surroundings. Another technique, which is based on the subjective visual quality measurement, is called spatial activity [39]. The use of spatial activity relies on the fact that noise visibility decreases in areas with sharp luminosity variations, thus offering easy embedding of noise in these areas. Spatial activity $A_{m,n}$ around a pixel position (m,n) is defined as the sum of local variations of surrounding pixels.

Piva et al. [4] made use of the spatial activity to exploit the distinctiveness of the *HVS* to embed a watermark of high energy content in an image at low cost of visibility. In his method the original image $\mathbf{X}$ and the watermarked image $\mathbf{Y}$ are added pixel by pixel according to the local

weighting factor $\beta_{m,n}$ thus obtaining new watermark image $\mathbf{Y}'$

$$Y'_{m,n} = X_{m,n}(1-\beta_{m,n}) + \beta_{m,n}Y_{m,n} = X_{m,n} + \beta_{m,n}(Y_{m,n} - X_{m,n}) \quad (3.9)$$

The weighting factor $\beta_{m,n}$ was used to take into account the characteristics of *HVS*. In highly textured regions, where noise sensitivity is low i.e. $\beta_{m,n} \approx 1$ and $Y'_{m,n} \approx Y_{m,n}$. Whereas in uniform regions, where noise sensitivity is high $\beta_{m,n} \approx 0$ and $Y'_{m,n} \approx X_{m,n}$. For each pixel intestines**,** $\beta_{m,n}$ was computed by obtaining variance of 9×9 non-overlapping blocks of the image. The average watermarking strength $\bar{\alpha}$ was thus obtained using $\beta_{m,n}$

3.3 Proposed Technique for Optimizing Perceptual Shaping of Watermark

In this work, GP is used to insure invisibility of watermark by optimizing perceptual shaping according to HVS. That human visual system is sensitive to local changes in variance of an image. A human observer can easily observe noise in smooth regions, but not in highly textured regions [29, 40]. These local changes in variance can be traced by using spatial activity masking [39]. Spatial activity masking thus helps us to select those areas whose visibility will be less affected with watermark embedding. GP is then used to evolve such a perceptual shaping function that embeds high strength watermark in high variance areas and low strength watermark in low variance areas. For this purpose, change in local variance of the marked image with respect to the original cover image is used as the fitness function in *GP* simulation.

It is difficult to simultaneously optimize robustness and perceptual invisibility. Therefore, we keep the mean squared strength (*MSS*) that represents a measure of robustness, in a suitable range and try to evolve such *PSF* that ensures maximum invisibility of the watermark $\boldsymbol{x}$. This *PSF* is allowed to have values in range of [0, 1], as the alteration to a *DCT* coefficient should be a fraction of its value. However, it is constrained to have *MSS* greater than certain application dependent lower bound.

$$MSS = \frac{1}{G}\sum_{i=1}^{G}\alpha_i^{\,2} \quad (3.10)$$

where *G* is the total number of selected DCT coefficient.

Since the evolved watermarking strength is no more a constant

rather a distribution, therefore we can configure an interesting modification to the conventional watermarking scheme proposed by Piva et al. [4]. Conventionally, the marked image $\mathbf{Y}$ is given by:

$$\mathbf{Y} = \mathbf{X} + f(\mathbf{X},\mathbf{S}) \tag{3.11}$$

The function $f(\mathbf{X},\mathbf{S})$ dictates the embedding process and depends only on the original image and the pseudo-random mark. Generally it is given by:

$$f(\mathbf{X},\mathbf{S}) = \mathbf{X}\cdot\mathbf{S} \tag{3.12}$$

A certain constant strength of this is added to the original image. Now, since we are not using constant watermarking strength for the image; rather we use perceptual mask obtained from GPSF (denoted by $\boldsymbol{\alpha}$). Consequently, in our case this function also depends on the GPSF and the marked image $\mathbf{Y}$ is given by:

$$\mathbf{Y} = \mathbf{X} + f(\mathbf{X},\mathbf{S},\boldsymbol{\alpha}) \tag{3.13}$$

with

$$f(\mathbf{X},\mathbf{S}) = \mathbf{X}\cdot\mathbf{S}\cdot\boldsymbol{\alpha} \tag{3.14}$$

To shape the watermark according to the cover image, the PSF should depend on the value of the *DCT* coefficient to be altered. But a question arises here, that using the same PSF for the marked image, how one should expect the same perceptual shaping to be obtained at the detection stage. Here we assume that the *DCT* coefficients during the embedding process are not heavily altered due to constraint on the image fidelity [5]. The experimental results shown in section 3.5 validate this assumption.

If α_i denote the watermarking strength for a particular coefficient of the selected coefficients, then for our proposed scheme, equation 3.6 and 3.8, which are used for embedding and detection respectively are modified as:

$$Y_{L+i} = X_{L+i} + \alpha_i \left| X_{L+i} \right| S_i \tag{3.15}$$

$$Z = \frac{1}{G}\sum_{i=1}^{G} \hat{Y}_{L+i}\cdot S_{0i}\cdot\alpha_i \tag{3.16}$$

3.4 Implementation Details

To represent a possible solution with a *GP* tree, one needs to define suitable functions, terminals and fitness criteria according to the optimization problem [41]. We have used a variant of Kuhlmann et al. *GP* C++ code [42] for evolving PSF. *Matlab* [43] has been used for the

manipulation of the images including taking DCT of the cover image and the subsequent selection of the DCT coefficients. The selected coefficient array (SCA) is passed on to the GP C++ environment, where each PSF of the population is used for embedding in the SCA. The modified SCA is then sent back to the *Matlab* environment and its fitness is computed based on its perceptual invisibility. This fitness of the individual PSF is again sent to GP C++ environment, where it dictates the mating probability for the creation of next generation. Typically, for a population size of 300 and 30 generations, the GP simulation takes about 4-5 hours on a Pentium IV – 2.0 GHz machine

The best PSF of the last generation is copied and is used for watermark embedding in *Matlab* environment (figure 3.1). Its perceptual invisibility is checked using mean squared error (MSE) and signal to noise ratio (SNR) given by (3.17) and (3.18). Interfacing of *Matlab* to VC++ has been used to coordinate among the different steps of the simulation. We have used Intel Pentium IV machine with a processing speed of 2.0 GHz for our simulation studies.

$$MSE = \frac{1}{M \times N} \sum_{m} \sum_{n} [x(m,n) - y(m,n)]^2 \qquad (3.17)$$

$$SNR = 10 \log_{10} \left(\frac{\sum_{m} \sum_{n} [x(m,n)]^2}{\sum_{m} \sum_{n} [x(m,n) - y(m,n)]^2} \right) \qquad (3.18)$$

3.4.1 GP Configuration:

Four binary floating arithmetic operators $(+, -, *, protected\ division)$, if less than $(IFLT)$, if greater than $(IFGT)$, EXP and ABS are used as conventional functions in the GP tree. Nearly 200 constants between -1 and +1 are used as constant terminals (see table 3.1). Since for every DCT coefficient of SCA, GP has to decide the watermarking strength, therefore the current DCT coefficient value and its index i in SCA are set as the variable terminals in a GP tree.

3.4.1.1 GP Fitness Criteria:

Fitness of each PSF individual is computed based on perceptual invisibility using spatial activity masking. For this purpose first we obtain the marked image in spatial domain using inverse DCT of modified image. We then compute the variance of 8×8 non-overlapping blocks of the image.

Table 3.1 GP Parameter setting for evolving GPSF for full-frame DCT-domain watermarking

Objective:	To evolve an optimal/near-optimal perceptual shaping function (PSF)
Function Set:	+, -, *, protected division, IFGT, IFLT, EXP and ABS
Terminal Set:	Current DCT coefficient of SCA, index of SCA
Fitness :	$\frac{64}{M * N} \sum_m \sum_n (BVM - BVM_0)$
Selection:	Generational
Population Size:	300
Initial Tree Depth Limit:	6
Initial population:	Ramped half and half
Reproduction Prb:	20%
Mate Selection Prb:	80%
Operators:	90% crossover, and 10% mutation
Termination:	Generation 30

These blocks are replaced by their respective variances, which gives us a Block Variance Matrix (BVM) of size $M \times N/8 \times 8$. Difference between this BVM and that of the original image (BVM_0) is obtained. The mean of this difference is then used as the fitness of each PSF. The lesser the value of mean is, the higher is the perceptual invisibility and better the individual PSF has performed.

3.5 Results and Discussion

A. Embedding and Detection:

In order to check the robustness of our proposed watermarking technique, we first use standard Lena image as a cover image. The marked image is shown in figure 3.2. The image is marked using $L = 25000$ and $G = 16000$ (equation 3.4), while block size for evaluating spatial activity masking is kept equal to 8×8. About 1000 randomly generated watermarks are checked for correlation with the marked image. The response to the correct watermark ($seed = 379$) is much larger than the responses to the others (see figure 3.3). The correlation value is compared to a suitable threshold value. The correlation crossing this threshold is considered to be representing the seed of the mark with which embedding is performed. Figure 3.4 shows the correlation when evolved PSF is not used in detection phase (equation 3.8), whereas figure 3.3 shows the same when PSF is used in the detection phase .

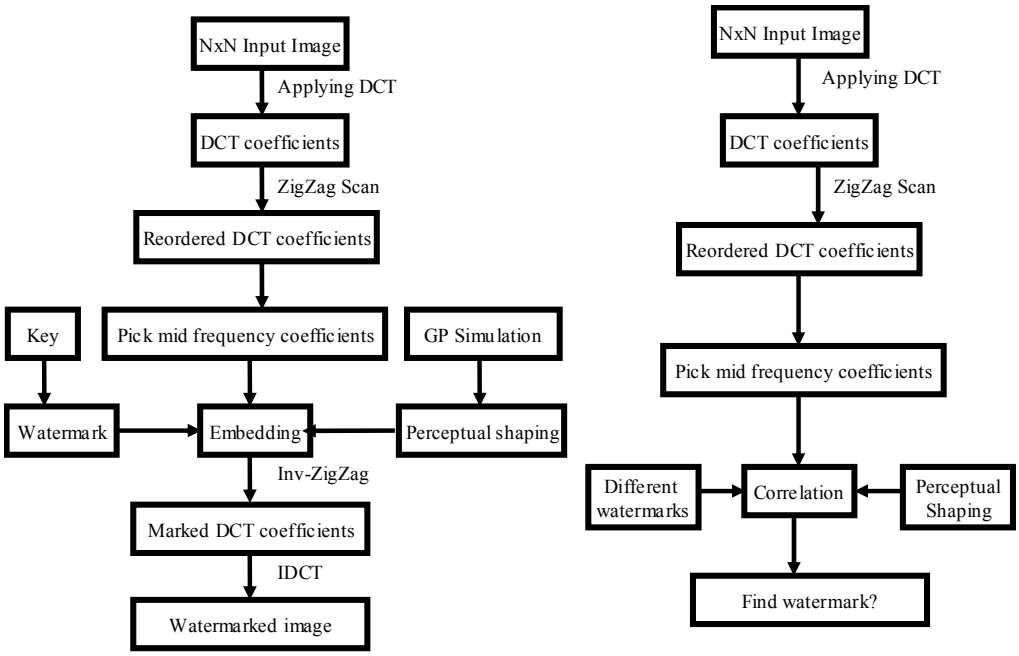

Figure 3.1 Full-frame DCT-domain watermark embedding (a) and detection (b) scheme

Figure 3.2 Watermarked Lena image

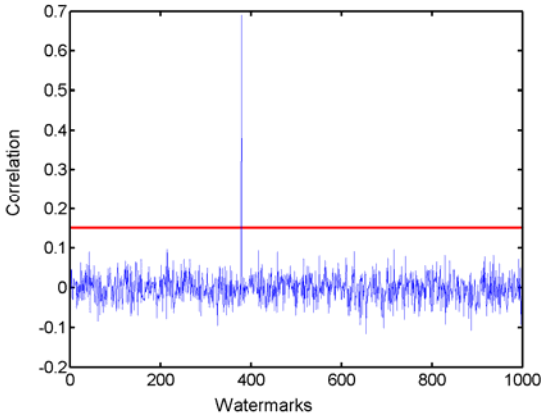

Figure 3.3 Watermark detection using GPSF

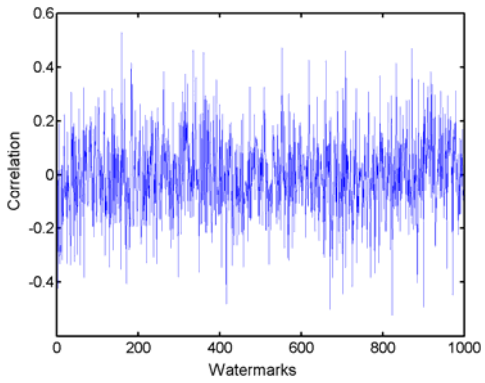

Figure 3.4 Watermark detection without using GPSF

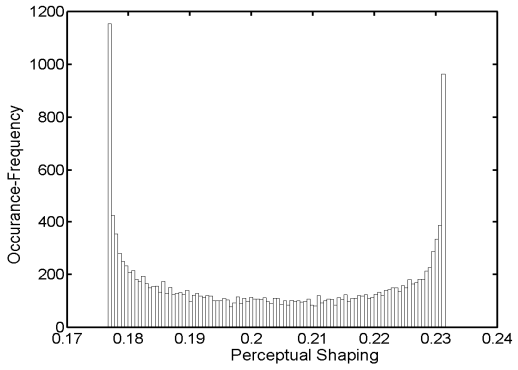

Figure 3.5 Histogram of GP

3.5.1 Genetic Perceptual Shaping

Figure 3.5 show the histogram of the *GP* evolved *PSF*. It is obtained for Lena image of size 512×512 with $L = 25000$ and $G = 16000$. Using the evolved *PSF*, suitable *SNR* values are obtained for different standard images with *MSS* approximately equal to 0.0417. The important property of this *PSF* is that it is cover-image independent and thus makes the watermarking scheme an image adaptive one. This fact can be observed from table 3.2, where we have used the same GPSF for different standard images. It provides high image quality measures while still offers effective resistance against Gaussian noise and *JPEG* compression. The best-evolved GPSF using *GP* simulation is given as:

$$\alpha = divide(minus(cos(sin(cos(sin(0.62621)))),0.58698),cos(cos(cos(cos(DCTcoef))))) \quad 3.19$$

where *DCTcoef* is the *DCT* coefficient being altered.

Table 3.2 Performance of the evolved GPSF for different images

Standard Images	Mean squared strength (MSS)	SNR	MSE	Max. Gauss. Noise	Max. JPEG Comp.
Lena	0.0417	44.45	0.6287	7,000	6%
Mandrill	0.0417	36.28	3.884	30,000	4%
Jaguar	0.0418	38.24	2.847	25,000	6%
Boat	0.0417	40.94	1.530	10,000	8%
Couple	0.0418	39.59	1.840	15,000	8%

3.5.2 Survival against Attacks

Figure 3.6 and table 3.3 confirm the robustness of our watermarking technique against some of the hostile attacks. These are compared to the results obtained by simulating Piva's approach [4,33]. It can be observed that our method has an edge over Piva's method in survival against attacks like *JPEG* compression of 8% quality, Gaussian noise of variance=14,000 and combined *JPEG* and Gaussian. The response to the correct watermark can still be detected, although the image degradation is quite heavy. However like Piva's, our method is not robust against translation and rotation attacks. For this purpose, one will need to use transforms that are invariant to these types of geometric attack [44] and then use *GP* to evolve *PSF* for such domains.

Table 3.3 summarizes the performance of our watermarking approach against different attacks. Our watermarking scheme survives low-pass filtering and median filtering up to window size of 5×5. Similarly it survives image resize up to 50%, *JPEG* compression up to 7% quality,

Gaussian noise up to 17000 variance and combined Gaussian and *JPEG* compression up to 5000 variance and 25% quality respectively. As expected, with increase in Gaussian noise the threshold increases while *SNR* decreases.

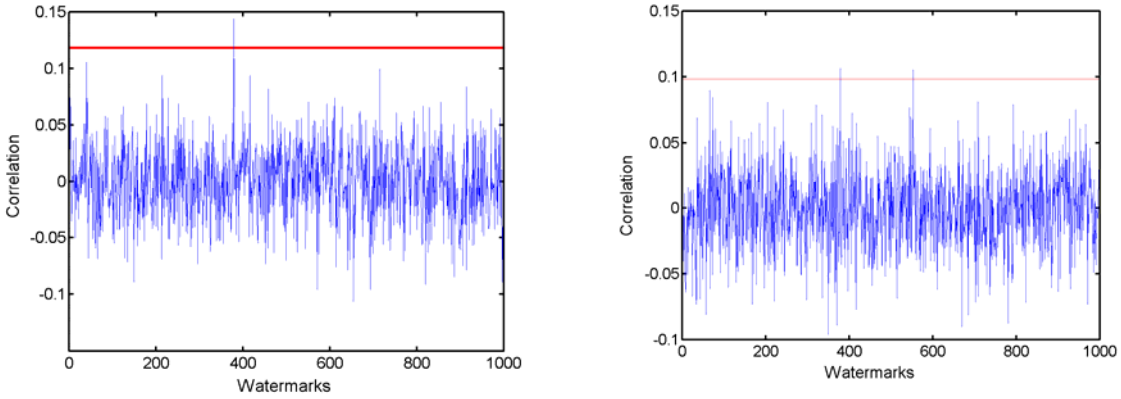

Figure 3.6 (a) Detector response after JPEG attack using GPSS
(b) Detector response after JPEG attack using Piva's approach

Table 3.3 Performance comparisons against different attacks

Attack Name	Attack Value	MSE	SNR	T	Z
JPEG Comp.	100%	1.100	40.59	0.120	0.68
	75%	15.08	29.22	0.120	0.665
	50%	23.65	27.26	0.122	0.545
	25%	36.95	25.32	0.125	0.330
	10%	72.62	22.39	0.128	0.198
Gauss. Noise	500	499	14.19	0.190	0.750
	1000	1002	11.32	0.240	0.774
	5000	5014	05.46	0.455	0.875
	10000	10014	03.54	0.650	0.955
	15000	15046	02.64	0.790	0.998
Median Filter	2x2 window	86.33	21.61	0.110	0.454
	3x3 window	27.87	26.52	0.093	0.431
	4x4 window	102.45	20.84	0.077	0.198
	5x5 window	68.73	22.57	0.061	0.132
	6x6 window	135.44	19.61	0.060	0.132
Lowpass Filter	2x2 window	81.47	21.86	0.105	0.455
	3x3 window	49.37	24.01	0.075	0.381
	4x4 window	112.37	20.41	0.044	0.175
	5x5 window	114.65	20.30	0.032	0.065
	6x6 window	166.67	18.65	0.015	0.011
Combine Weiner, jpeg Comp. & G. Noise	J=75,N=500	109.01	20.76	0.135	0.436
	J=50,N=1000	185.0	18.54	0.164	0.490
	J=50,N=5000	842.0	12.12	0.295	0.531
	J=50,N=10000	1612	9.56	0.390	0.565
	J=25,N=5000	752.0	12.59	0.295	0.492
	J=25,N=9000	1402	10.08	0.398	0.388
Highpass Filter	3x3 window	42.34	24.81	0.172	0.410
Image Resize	75%	--	--	0.121	0.468
	50%	--	--	0.072	0.164
	40%	--	--	0.083	0.050

3.6 Conclusions

We have considered the robustness versus imperceptibly as an optimization problem. Using this idea, a GPSF is evolved that effectively shapes the watermark according to the cover image. Unlike the heuristic techniques used in [4] that search for a constant watermarking strength for each new cover image, the GPSF is image adaptive and selects a suitable watermarking strength for each *DCT* coefficient. The optimal/near-optimal shaping of the watermark obtained using the evolved GPSF increases its resistance against most of the non-geometric attacks. As a result of our simulations, the best evolved GPSF has been obtained. Its expression is quite general and can be used in any full frame *DCT* domain-based watermarking technique.

Chapter 4

Perceptual Shaping of Block-based DCT-domain Watermarking Scheme

The most widely used transformation, both in image compression and watermarking is the block-based DCT transformation. In this chapter, as opposed to the previous chapter, we will concentrate on intelligent perceptual shaping of block-based DCT domain watermarks. The performance of the GPSF is compared with that of WPM. This will help in establishing the fact that intelligent perceptual shaping of a watermark could be applied to a broad category of watermarking techniques.

The proposed technique exploits the characteristics of human visual system using GP. We employ a tradeoff between watermark robustness and imperceptibility, as an optimization criterion in the GP search. The resultant GPSF is a combination of frequency, luminance sensitivity and contrast masking, enabling us to shape the watermark according to the cover image.

4.1 Introduction

Typical watermarking schemes are based on transform-domain techniques (DCT, wavelets etc) [4, 5, 6, 7, 8] as well as spatial-domain methods [15, 47]. Transform-domain techniques have the convenience of allowing us the direct understanding of the content of the cover data.

Development of an adaptive watermarking scheme to tailor a watermark requires the understanding of the cover image in the context of HVS. Recent survey by Cox et al. [46], foresee optimal perceptual shaping of a watermark as a fruitful new area of research. The better a perceptual model is, the better is the perceptual shaping and hence imperceptibility of the watermark.

In watermarking schemes based on DCT-domain techniques, mostly WPM [16, 48] is used to shape the watermark. WPM is based on Ahumada's work [17] and has been used in DCT-based JPEG compression. Podilchuk et al. [7, 49], using WPM, have attempted to exploit HVS for watermark shaping in DCT domain. Hernandez et al. [5] and Briassouli et al. [6] have applied the same idea in spread spectrum-

like DCT domain watermarking. Cox et al. [19] have also used WPM for perceptually shaping the watermark in their informed coding and embedding based watermarking technique. WPM, although widely used in DCT domain-based watermarking, is not the optimal perceptual model [1]. Firstly, the model is built on empirical studies and is not based on extensive search methods. Secondly, it neglects certain effects, like spatial masking in frequency domain [5].

As regards spatial-domain based watermarking schemes, Delaigle et al. [47], have used both masking and texture discrimination to embed high strength watermark. On the other hand, Voloshynovskiy et al. [15] have used the idea of noise visibility function to shape the watermark in the spatial-domain. They use a non-stationary Gaussian stochastic model to model noise and thus differentiate between smooth and noisy regions in a cover image. Recently Kutter et al. [50] have presented a perceptual model that takes into account the sensitivity and masking behaviour of HVS, by means of a local isotropic contrast measure and a masking model. On the other hand, Lambrecht et al. [51] have proposed a perceptual model that is based on Gabor filters.

Although, both in transform and spatial-domain based watermarking schemes, a number of efforts have been made to appropriately shape a watermark according to the cover image. However, very few attempts have been made to consider the watermark shaping as an optimization problem. Huang et al. [2, 8] have used Genetic Algorithm to choose optimal embedding positions in a block of a block-based DCT domain watermarking system. However, they have not considered the optimization of perceptual model itself to improve the marked image quality. Cox et al. [1] have used Lagrange optimization for optimally embedding an already shaped watermark. Pereira et al. [23], using Linear Programming, optimally embed a watermark in transform-domain, subject to a linear set of constraints in spatial-domain. We address these issues through the following contributions:

1. We concentrate on the optimization of the perceptual shaping function itself and propose a technique for developing GPSF.

2. We consider the perceptual shaping function as a function and the characteristics of HVS as independent variables. The GP search mechanism is then used to strive for optimal dependency of the perceptual shaping function on the characteristics of HVS.

4.2 Proposed Technique for Developing a GPSF

Figure 2.4 shows the basic architecture of our proposed scheme for developing perceptual shaping functions. Three different modules

supplement each other in a cyclic fashion. Robustness versus imperceptibility trade-off is considered as an optimization problem. We first explain the overall working of the basic architecture. Details of the individual modules are given in section 4.2.1.

The GP module produces a population of GPSF. Each GPSF is presented to the perceptual shaping module, where it is applied on the cover image in DCT-domain, generating a perceptual mask. The watermark is shaped using the perceptual mask and its imperceptibility is then used as a scoring criterion in the GP module. In this way, the GP module evaluates the performance of its several generated GPSFs. In a separate stage, the best-evolved GPSF is compared with that of the WPM.

4.2.1 Evolution of Perceptual shaping functions

4.2.1.1 The GP Module

The GP settings for evolving GPSF are as under:

GP Function Set: Function set in GP is a collection of functions available to the GP system. In our GP simulations, we have used simple functions, including four binary floating arithmetic operators (+, -, *, and protected division), *LOG, EXP, SIN* and *COS*.

GP Terminals: To develop initial population of GPSF, we consider GPSF as watermark shaping function and the characteristics of HVS as independent variables. By doing this, in essence, we are letting GP exploit the search space representing different possible forms of dependencies of the watermark shaping function on the characteristics of HVS. Therefore, visibility threshold $T(i,j)$, DC and AC DCT coefficients of 8x8 block are provided as variable terminals (figure 4.1). Random constants in the range [-1,1] are used as constant terminals.

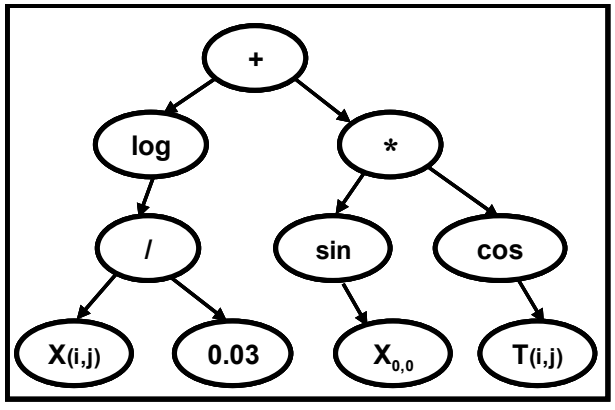

Figure 4.1 An example GP tree for exploiting characteristics of HVS

Fitness Function: A fitness function in GP is supposed to grade each individual of the population. It is designed to provide feedback about how well an individual of the GP population is performing at the given task. Figure 2.2 depicts the idea of using fitness function as feedback. Every perceptual shaping function of a GP population is evaluated in terms of structuring the watermark. The evaluation is based on how well is the SSIM measure at a certain level of *estimated robustness* (MSS).

$$Fitness = SSIM_{E.R} \tag{4.1}$$

Thus, each individual perceptual shaping function of a GP population is scored using equation 4.1 as a fitness function. The greater the fitness is, the better the individual has performed.

Termination Criterion: The GP simulation is ceased when one of the following conditions is encountered:

1. The fitness score exceeds 0.99 with MSS ≥ 20.0.
2. The number of generations reaches the predefined maximum number of generations.

4.2.1.2 Perceptual Shaping Module

A perceptual model exploits the characteristics of HVS to tailor a watermark according to the cover image. This enables us to embed a large energy watermark at low cost of resultant distortion to the cover image. The perceptual shaping module receives the individual GPSF provided by the GP module as an input. Each GPSF is operated on the cover image in DCT-domain. Corresponding to the selected DCT coefficient of a block, the GPSF returns a value. The magnitude of this value represents the perceptual strength of the alteration made to that coefficient. The functional dependency of the perceptual shaping function on the characteristics of HVS can be represented as follows:

$$\alpha(k_1, k_2) = f\left(T(i,j),\ X_{0,0},\ X(i,j)\right) \tag{4.2}$$

where the first variable, T is the visibility threshold representing frequency sensitivity of HVS. $X_{0,0}$ is the DC DCT coefficient, while $X(i,j)$ is the AC DCT coefficient of the current block. They represent the luminance sensitivity and contrast masking characteristics of HVS respectively.

Operating the GPSF on all of the DCT coefficients, we obtain the perceptual mask for the current cover image. The product of the spread-spectrum sequence and expanded message bits is multiplied with this

perceptual mask to obtain the watermark. The 2-D watermark signal $\mathbf{W}$ (see figure 4.2) is given as:

$$\mathbf{W} = \boldsymbol{\alpha} \cdot \mathbf{S} \cdot \mathbf{b} \tag{4.3}$$

where $\mathbf{S}$ is a pseudo random sequence and $\mathbf{b}$ is the repetition-based expanded code vector, corresponding to the message to be embedded. The embedding is performed by adding this watermark to the original image in transformed domain:

$$\mathbf{Y} = \mathbf{X} + \mathbf{W} \tag{4.4}$$

Here the watermark $\mathbf{W}$ is our desired signal, while the cover image $\mathbf{X}$ acts as an additive noise. As we are developing GPSF, therefore, equation 4.3 will be modified as follows:

$$\mathbf{W} = \boldsymbol{\alpha}_G \cdot \mathbf{S} \cdot \mathbf{b} \tag{4.5}$$

where $\boldsymbol{\alpha}_G$, representing perceptual mask corresponding to GPSF, incorporates the dependencies from visibility threshold $T(i,j)$, AC and DC coefficients.

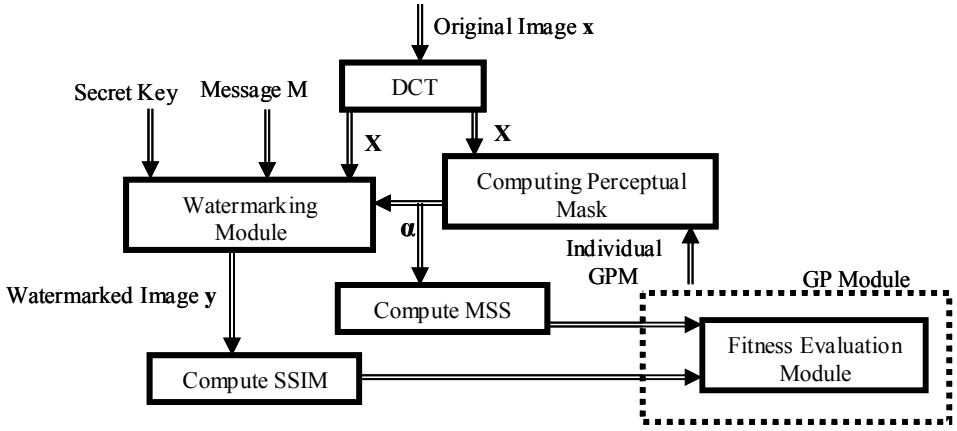

Figure 4.2 Detailed structure of GPSS for exploiting characteristics of HVS

4.2.1.3 Watermarking Module

In order to evaluate the performance of each individual GPSF of the GP population, the watermarking module implements the spread spectrum based watermarking technique proposed by Hernandez et al. [5] (figure 2.1). This watermarking technique is oblivious and embeds message into the low and mid frequency coefficients of 8×8 DCT blocks of a cover image. The employed watermarking scheme performs the statistical modelling of DCT coefficients using generalized Gaussian distribution. This fact helps in constructing better detector/decoder structures than the simple Gaussian correlation receiver that is mostly

used. One of the reasons for using this watermarking scheme is that the DCT is applied in blocks of 8x8 pixels, in a manner similar to that used in JPEG algorithm. Hence, it is easy to use and compare WPM with that of the GPSF. Secondly, this watermarking scheme has strong theoretical foundations [5]. The embedding in DCT-domain is performed using equation 4.4.

The watermarking module of our proposed technique provides the imperceptibility of the resultant watermark as a feedback to the GP module. The structure of how different sub-modules work within the proposed model is shown in figure 4.2.

4.2.3 Testing Performance of the Best-evolved GPSF

In order to assess the performance of the best-evolved GPSF, its expression is saved at the end of the GP simulation. The best-evolved GPSF is then compared with that of WPM in terms of watermark shaping. Where by, the watermark shaping ability is assessed by computing watermark imperceptibility as well as robustness measures. Figure 4.3 shows the details of the testing method for the evolved GPSF using watermarking approach of [5]. In this testing phase, besides using the watermarking approach proposed in [5], we also use an algorithm similar to the E_PERC_SHAPE algorithm of Cox et al. [1] as well. We compare both perceptual shaping functions on the E_PERC_SHAPE algorithm, to see whether the GP search mechanism has a bias towards Hernandez's watermarking algorithm used during evolution stage. We also evaluate the message retrieval performance in terms of Bit Correct Ratio[2]:

$$BCR(\mathbf{M},\mathbf{M}') = \frac{\sum_{i=1}^{L_m} \overline{(m_i \oplus m_i')}}{L_m} \tag{4.6}$$

where $\mathbf{M}$ represents the original, while $\mathbf{M}'$ represents the decoded message, L_m is the length of the message and $\oplus$ represents exclusive-OR operation. It should be noted that $(1-BCR)$ represents bit incorrect ratio.

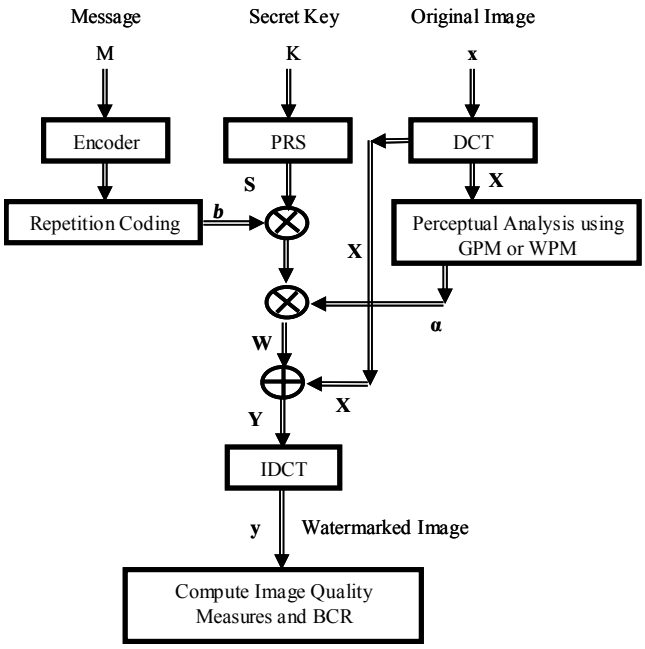

Figure 4.3 Details of the testing method for the evolved GPSF

4.3 Implementation Details

We have used MATLAB environment for our experimental studies. To employ GP, we use GPLAB toolbox [53-54]. The GP parameter settings are shown in table 4.1, while the remaining parameters are used as default in the software.

Lena image of size 256x256 is used as a cover image with $N_d = 22$ (7 to 29 in zigzag order) during the GP simulation. Message size is kept equal to 64 bits. Following [12, 13], the parameters of WPM are set as $r = 0.7$, $T_{\min} = 1.1548$, $u = 1.728$, $f_{\min} = 3.68$ cycles/degree and a_T = 0.649. To estimate the value of parameter c for generalized Gaussian Distribution-based modeling of each (i,j) DCT sequence [5], we have considered its range [0.02, 2.0] with grid step of 0.02. The watermark power, represented by MSS, is constrained to lie above a certain lower bound (e.g. 20.0) for all the individuals.

In the testing phase, all images except Baboon and Boat are of size 256x256. For each of the test image, grid search with a step of 0.01 is applied to find the watermark strength needed to produce a resultant image of same SSIM measure. In order to develop GPSF, keeping population size equal to 300 and no. of generations 30, the GP simulation consumes about half an hour on a Pentium IV machine (2.0 GHz speed and 256 Mb RAM). In the testing phase, the watermarking scheme using the best-evolved GPSF spends about 30 sec to watermark Lena image.

Table 4.1 GP Parameter setting for evolving GPSF for block-based DCT-domain watermarking

Objective:	To evolve optimal /near-optimal Perceptual model
Function Set:	+, -, *, protected division, *SIN, COS,* and *LOG*
Terminal Set:	Constants: *random constants in range* of [-1, 1] Variables : $X_{0,0}/1024, abs(X(i,j))$ *and* $T(i,j)$
Fitness :	*SSIM*
Selection:	Generational
Population Size:	260
Initial max.Tree Depth	6
Initial population:	Ramped half and half
Operator prob. type	Variable
Sampling	Tournament
Expected no. of offspring	rank89
Survival mechanism	Keep best
Real max level	28
Termination:	Generation 30

4.4 Results and Discussion

4.4.1 Perceptual Shaping Using GPSF

In figure 4.4, watermarking strength corresponding to each bandpass DCT coefficient of block-based DCT is shown. These strengths are produced by the GPSF for Lena image. It is observed that instead of keeping same strength for each DCT coefficient; it provides suitable imperceptible alterations according to the spatial content of that block. This fact indicates that GPSF is able to exploit HVS for shaping the watermark according to any cover image. In other words, GPSF makes the watermarking technique adaptive with respect to the cover image. The resultant watermark is shown in figure 4.5.

4.4.2 Imperceptibility of the resultant watermark

In figure 4.8, we have shown the difference image, obtained by subtracting the original image (figure 4.6) from the watermarked image (figure 4.7) in spatial domain. The pixel intensity of the difference image is amplified ten times for illustration purpose. Although, DCT domain is used for embedding, still GPSF is able to learn the spatial distribution of the Lena image, as most of the strong embedding is performed in highly textured areas.

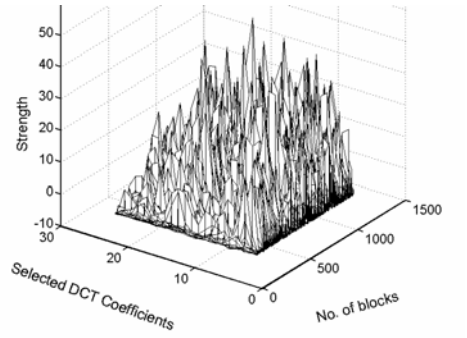

Figure 4.4 Watermarking strength distributions

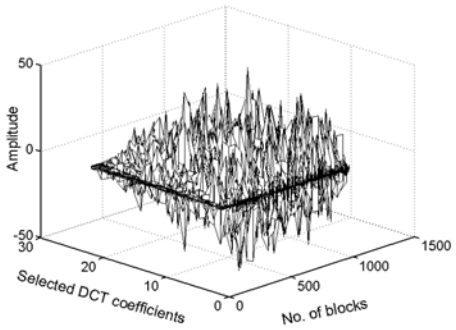

Figure 4.5 Watermark distribution

Figure 4.6 Original Image

Figure 4.7 Watermarked Lena Image using the evolved GPSF for block DCT-domain

Figure 4.8 Difference Image

Table 4.2 compares both perceptual shaping functions in terms of the marked image quality, *estimated robustness* and BCR performance for 10 different standard images. Both perceptual shaping functions are multiplied with some scaling factor to achieve a desired Value of SSIM that represents watermark imperceptibility. Columns 3 of table 4.2 and table 4.3 represents watermark strength, while column 4 represents mean squared strength giving a measure of the watermark power. On the other hand, columns 5-9 show watermarked image quality in terms of different measures. These different image quality measures are used here due to two reasons. Firstly, it would be easier for other researchers to verify our results. Secondly, because of the complexity in modeling HVS, there is no generic and widely accepted image quality measure reported so far [52]. Therefore, we use these different measures; however, most of our watermark imperceptibility analysis is based on the most recently reported SSIM measure.

It is observed that in case of GPSF, keeping same distortion of the resultant image as in WPM case, the watermark being embedded is of high power. Specifically, by looking at the MSS values (column 4 of table 4.2), GPSF is able to embed watermark of approximately double power, as compared to that of WPM. This improvement in terms of high power embedding can be observed for all of the test images and in both watermarking approaches (see table 4.3 as well). Consequently, the watermark shaping ability of the evolved GPSF is superior to that of WPM.

4.4.3 Message Retrieval Performance

Last column of table 4.2 shows the message retrieval performance of both the perceptual shaping functions at equal image distortion for different test images. Table 4.4, on the other hand, illustrates the comparison of both perceptual shaping functions in terms of BCR performance, when the message size is varied. It shows the bit extraction power of both shaping functions, when the capacity of a watermark is increased. We have multiplied both perceptual models by a scaling factor to produce watermarked image having $SSIM \geq 0.981$. With increase in message size, GPSF produces high (1-BCR) than that of WPM. This could be mainly because equal watermark power may not result in the same practical robustness for two different perceptual shaping schemes. In other words the *estimated robustness* measure MSS does not always reflect actual robustness.

Table 4.2 Perceptual shaping comparisons for different images using Hernandez's watermarking scheme

Test Images	Perceptual Model	Watermark strength	Watermark power	Watermarked image quality measures					Decoding performance
		Scaling Factor	MSS	MSE	WDR	PSNR	wPSNR	SSIM	BCR
Lena	WPM	0.3660	13.3571	4.59020	-35.819	41.5125	44.5196	0.9809	1.0
	GPSF	0.3910	27.224	9.3570	-32.726	38.4192	42.7858	0.9810	1.0
Trees	WPM	0.413	28.692	9.85670	-33.0527	38.1935	43.2628	0.9810	1.0
	GPSF	0.326	52.1633	17.9278	-30.455	35.590	41.703	0.9810	1.0
Baboon (232x248)	WPM	0.504	46.876	16.0850	-29.2547	36.066	44.947	0.9810	1.0
	GPSF	0.357	68.6184	23.5636	-27.596	34.408	44.023	0.9810	1.0
Couple	WPM	0.440	30.869	10.5910	-31.957	37.881	42.796	0.9809	1.0
	GPSF	0.335	46.064	15.7770	-30.2267	36.1504	41.849	0.9809	1.0
Boat (232x248)	WPM	0.402	22.979	7.8730	-33.775	39.1691	43.488	0.9809	1.0
	GPSF	0.331	42.9183	14.7246	-31.0567	36.4504	41.968	0.9809	0.984
Airplane	WPM	0.244	6.1794	2.1210	-42.596	44.865	46.240	0.9809	1.0
	GPSF	0.417	27.153	9.3220	-36.166	38.435	41.4217	0.9810	1.0
Watch	WPM	0.259	9.286	3.187	40.748	43.097	45.577	0.9809	1.0
	GPSF	0.467	53.987	18.5227	-33.4538	40.3724	42.569	0.9809	1.0
Fruits	WPM	0.331	14.3347	4.926	-37.769	41.206	44.081	0.9810	1.0
	GPSF	0.381	41.854	14.367	-33.1207	36.557	41.307	0.9810	1.0
House	WPM	0.314	8.9053	3.0543	-38.3856	43.3814	45.254	0.981	1.0
	GPSF	0.359	20.8086	7.127	-34.7056	39.6014	42.464	0.9810	0.984
Chemical Plant	WPM	0.473	28.246	9.7046	-31.1713	28.261	42.7097	0.9809	1.0
	GPSF	0.358	39.538	13.588	-29.709	36.799	42.0516	0.9809	1.0

Table 4.3 Perceptual shaping comparisons for different images using Cox's E_PERC_SHAPE watermarking scheme

Test Images	Perceptual Model	Watermark strength	Watermark power	Watermarked image quality measures				
		Scaling Factor	MSS	MSE	WDR	PSNR	wPSNR	SSIM
Lena	WPM	0.245	37.8116	3.5026	-37.0258	42.687	44.6156	0.9803
	GPSF	.53	139.763	11.0403	-32.0416	37.701	40.8717	0.9805
Trees	WPM	0.35	67.671	5.956	-35.27	40.381	43.912	0.9803
	GPSF	0.61	316.5	22.979	-29.408	34.5174	39.788	0.9809
Baboon (232x248)	WPM	0.47	118.77	10.23	-31.332	38.031	44.734	0.9808
	GPSF	1.0	322.188	23.205	-27.781	34.475	42.442	0.9810
Couple	WPM	0.37	82.586	7.21	-33.66	39.552	43.312	0.9806
	GPSF	0.71	238.243	19.43	-29.36	35.246	40.152	0.9808
Boat (232x248)	WPM	0.3	49.86	4.516	-36.282	41.583	44.283	0.981
	GPSF	0.68	15.66	16.62	-30.63	35.924	40.26	0.9806
Airplane	WPM	0.15	18.094	1.85	-43.213	45.46	46.076	0.9803
	GPSF	0.63	104.32	9.2	-36.246	38.493	41.389	0.9806
Watch	WPM	0.15	21.492	2.123	-42.535	44.862	45.993	0.9809
	GPSF	0.56	224.62	21.12	-22.56	34.884	38.198	0.9807
Fruits	WPM	0.225	35.034	3.262	-39.584	42.996	44.568	0.9802
	GPSF	0.63	57.248	12.133	-33.881	37.291	44.550	0.9807
House	WPM	0.205	24.436	2.364	-39.526	44.393	45.584	0.9808
	GPSF	0.57	155.29	12.344	-32.354	37.212	40.459	0.9807
Chemical Plant	WPM	0.4	78.486	6.919	-32.678	39.73	43.127	0.981
	GPSF	0.77	277.883	22.391	-27.583	34.63	39.728	0.9809

With an increase in message size, the watermarked image quality remains the same for both perceptual shaping functions. This is because, only the number of repetitions of a bit in different blocks decreases with increase in message size. The BCR performance can be increased by using advance channel coding like low-density parity check code [40] in concatenation to the simple repetitive coding that we have used. Since in this work we are concentrating on the perceptual shaping of the watermark, therefore we use repetitive coding only.

4.4.4 Best-evolved GPSF

Expression of the best GPSF in normal notation is:

$$\alpha(k_1, k_2) = ((|X(i,j)| - (SIN(X_{0,0}/1024)/v(i,j))) - \log(T(i,j) - 0.583018), \quad i, j \in \{0, \ldots, 7\} \tag{4.7}$$

where $v(i,j) = (T(i,j) - 1.4023) \cdot ((T(i,j) - 0.10025/|X(i,j)|)$

Table 4.4 Imperceptibility versus message retrieval performance

Message Size	SSIM		(1-BCR)	
	WPM	GPSF	WPM	GPSF
64	0.981	0.981	0.0	0.0
128	0.981	0.981	0.00	0.0313
256	0.981	0.981	0.0117	0.0430
512	0.981	0.981	0.0371	0.0898
1000	0.981	0.981	0.051	0.1510

Figure 4.9 shows the accuracy versus complexity plot of GP simulation. It is observed that as generations pass by, improvement in fitness of the best individual is achieved at cost of its complexity. That is, with increase in fitness of the best perceptual shaping function of a generation, its genome's total number of nodes as well as its average tree depth increases.

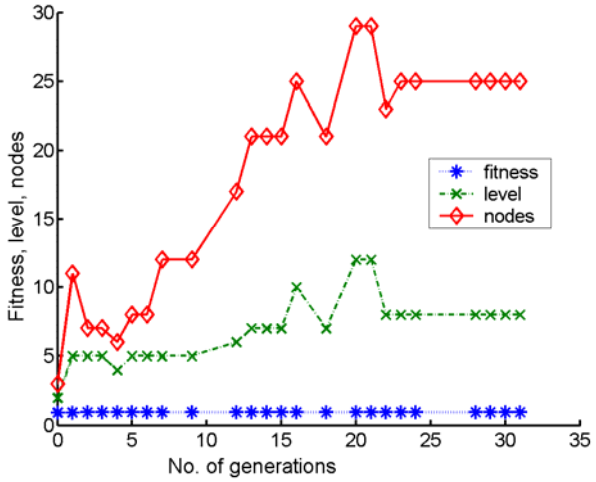

Figure 4.9 Accuracy versus Complexity plot of GP simulation

4.5. Conclusions

We have considered the robustness versus imperceptibility tradeoff in a watermarking system as an optimization problem to obtain optimal/near–optimal GPSF. The developed GPSF is image independent and can be used for any cover image. It is a combination of frequency and luminance sensitivity as well as contrast masking. It offers superior performance to that of Watson's perceptual model in terms of watermarked imperceptibility but not in terms of message decoding. Our analysis shows that high power embedding does not always reflect high practical robustness. Developing GPSF by employing GP needs considerable execution time (approximately half an hour). However, once the best GPSF is developed, then employing GPSF for watermark shaping is quite straightforward and easy to implement. Even in the development phase, using fast and parallel processing based implementations of GP [24, 55, 56], it is possible to use GP-based watermarking to real business applications. The concept of Pareto optimization [25], if applied for simultaneously improving robustness, imperceptibility as well as capacity of a watermark, may further improve the proposed method. The proposed technique can be applied in other watermarking domains, like FFT, Wavelet and Spatial as well. Currently work is in progress to enhance the proposed technique for developing GPSF, by exploiting information about the conceivable attacks as well.

Chapter 5

Exploiting Attack information during Watermark Shaping

Survival of a watermark mostly depends on the type and strength of the subsequent distortions faced by the watermarked image. There is no generic watermarking scheme that could resist all sorts of attacks. However, most of the watermarking applications are concerned only with a specific set of attacks. As such, knowledge about the conceivable attack could be utilized before hand at the encoding, embedding or detection/decoding stage thwarting the subsequent reduction in message retrieval performance. In this chapter, we introduce a new idea of utilizing conceivable attack information during watermark shaping. In essence, this chapter introduces a generic scheme of intelligently developing specific attack-resistant perceptual shaping functions.

5.1 Introduction

Watermarks are rendered undetectable with an attack, where the attack is defined as any processing of the watermarked data that might damage the watermark [1, 3]. Thus watermarking can be viewed as a reliable mode of communication to transfer important information (i.e. a watermark) embedded in a signal (e.g. a cover image) safely through a hostile environment [57]. Attacks can be intentional such as watermark estimation using Wiener filtering or unintentional such as JPEG compression. An extensive list of attacks appears in [1, 58-62].

Due to the nature of diverse types of attacks, there is no generic watermarking scheme that could resist all sorts of attacks. However, it can be assumed that many applications are not concerned with all conceivable attacks, but with specific attacks that might occur before decoding [1]. Investigators have addressed this problem in various ways. One way is to develop watermarking approaches suitable for the anticipated attack [63]. For example, in case of rotational attack, alteration in the phase, rather than the amplitude of the Fourier component, is performed to embed a watermark [64]. Another possibility is to achieve robustness against the probable processing of the watermarked image, by restructuring the watermark. In this scenario, robustness is often achieved at the expense of imperceptibility, computational cost, data payload, or even robustness to some other processing.

To defend attacks, efforts have been made to increase robustness at low cost of imperceptibility. For instance Jonathan et al. [3] have taken a theoretical approach to answer the complex question of "how should a watermark be structured to maximize its robustness". They have proposed that the watermark power spectrum should be proportional to that of the original signal. Liang et al. [65] propose robust watermarking using robust coefficients for embedding. Huang et al. [2, 8], on the other hand, have used Genetic Algorithms for the selection of coefficients to be altered for watermark embedding. However, these efforts concentrate on tailoring just the choice of specific coefficients, not the whole watermark, to a cover image and intended attack. In fact, they are not using perceptual shaping functions; rather a fixed strength of the alteration is used for each selected DCT coefficient.

Perceptual models [23-26], as those of Watson's, which have been frequently used in image compression are used to compute the strength of the alteration for each selected coefficient. These perceptual models make a tradeoff between robustness and imperceptibility according to the cover image. However, they do not take into consideration the watermark application and thus the intended attacks. For instance, when the watermarked image is expected to be JPEG compressed, it is judicious to structure the watermark in view of the JPEG compression. Pertinent examples exist in literature [66], where appropriate watermarking approaches as well embedding domains have been studied to achieve robustness against JPEG compression.

One way to restructure a watermark in view of the anticipated attack is to keep high watermark strength for those selected coefficients that are less affected by the attack. However, firstly this requirement needs to consider limitations imposed by imperceptibility. Secondly, this requirement vary for different types of attacks. Consequently, our aim in this work is to propose and study an automatic system that can restructure the watermark in accordance to the cover image and intended attack. Specifically, to develop a system capable of generating suitable perceptual shaping functions, which are image independent and intended attack-resistant.

We address these requirements through the following contributions:

1. We consider the perceptual shaping of a watermark to be vital, not only for imperceptibility enhancements, but we realize it to be a method of structuring the watermark in accordance to the anticipated attack.

2. We introduce the concept of developing complex and appropriate perceptual shaping functions from the existing ones. Specifically, we consider Watson's perceptual model, characteristics of

the HVS and information about the distortion caused by the anticipated attack, as independent variables and genetically search for application-specific perceptual shaping functions.

The idea used is analogous to combining classifiers for developing complex, but appropriate classifier for a certain application of pattern recognition [67]. We call this technique as Genetic Perceptual Shaping Scheme (GPSS) and the genetically developed perceptual shaping functions as Genetic Perceptual Shaping Function (GPSF).

5.2 Proposed Technique for Developing a GPSF

The basic architecture of our proposed scheme for developing GPSF is shown in figure 5.1. Five modules work in a cyclic fashion. We first explain the overall working of the basic architecture. Details of the individual modules are given in section 5.2.1.

The GP module produces a population of GPSF. Each GPSF is presented to the perceptual shaping module, where it is applied to the cover image in DCT-domain, generating a perceptual mask. In the watermarking stage, the watermark is shaped using the perceptual mask. The conceivable attack is performed on the watermarked image in the attack module. In the decoding module, the embedded message is retrieved from the corrupted image. The watermark imperceptibility at the embedding stage and BCR at the decoding stage, are then used in the scoring criterion of the GP module. In this way, the GP module evaluates the performance of its several generated GPSFs.

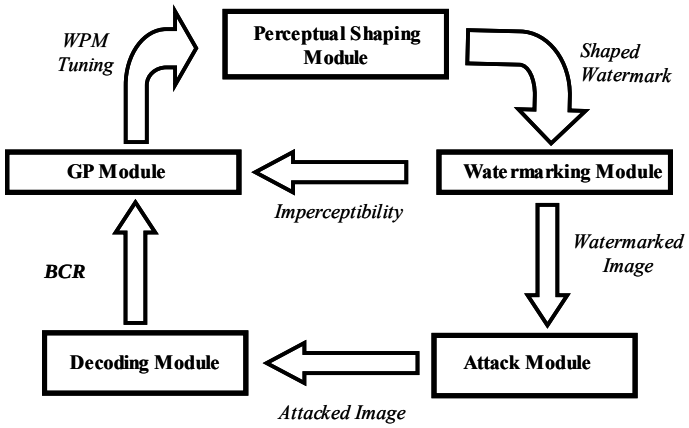

Figure 5.1 Basic architecture of attack-resistant GPSS

5.2.1 Evolution of Perceptual Shaping Function

5.2.1. The GP Module

The GP settings for evolving GPSF are as under:

GP Function Set: Function set in GP is a collection of functions available to the GP system. In our GP simulations, we have used simple functions, including four binary floating arithmetic operators (+, -, *, and protected division), *LOG, EXP, SIN* and *COS*.

GP Terminals: To develop initial population of GPSF, we consider GPSF as watermark shaping function and the characteristics of HVS as independent variables. By doing this, in essence, we are letting GP exploit the search space representing different possible forms of dependencies of the watermark shaping function on the characteristics of HVS. Therefore, the current value of WPM-based perceptual mask, DC and AC DCT coefficients of 8x8 block are provided as variable terminals (equation 5.2 and figure 5.2). Random constants in the range [-1,1] are used as constant terminals.

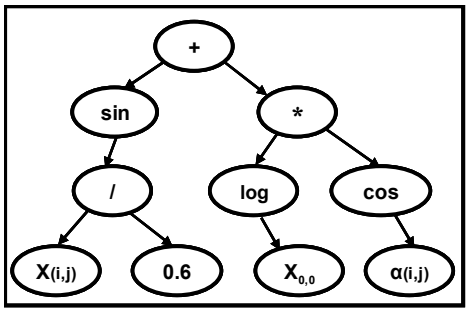

Figure 5.2 An example GP tree representing attack-resistant GPSF

Fitness Function: As explained earlier, a fitness function in GP directs the GP search mechanism towards the desired solution. In analogy to filtering process, it could be considered as providing feedback about how sound an individual of the GP population is performing at the given task. Every perceptual shaping function of a GP population is evaluated in terms of structuring the watermark. The evaluation is based on how well is the SSIM measure at a certain level of watermark power as well as how high the BCR value is:

$$Fitness = W_1 * SSIM_{E.S} + W_2 * BCR_{attack} \quad (5.1)$$

where $SSIM_{E,S}$ denotes the structure similarity index measure of the marked image at a certain level of estimated robustness. W_1 and W_2 represent the corresponding weightage of the two terms in the fitness.

If W_1 and W_2 are set to 1.0, the fitness attains a maximum value of 2.0. Thus, each individual perceptual shaping function of a GP population is scored using equation 5.1 as a fitness function. The greater the fitness is, the better the individual has performed.

Termination Criterion: The GP simulation is ceased when one of the following conditions is encountered:

1. The fitness score exceeds 1.99 with MSS ≥ 20.0.
2. The number of generations reaches the predefined maximum number of generations.

5.2.1.2 Perceptual Shaping Module: Achieving Resistance against Conceivable Attack

Since an image/video, after all is going to be viewed by a human observer, therefore, HVS must be considered while modelling an image/video watermarking system. To exploit the characteristics of HVS, a perceptual model is used to tailor a watermark according to the cover image. This enables us to embed a large energy watermark at low cost of resultant distortion to the cover image. The perceptual shaping module is provided with the individual GPSF by the GP module. Each of these GPSFs is operated on the cover image in DCT-domain. GPSF returns a value corresponding to the selected DCT coefficient of a block. The magnitude of this value represents the perceptual strength of the alteration made to that coefficient. The functional dependency of the perceptual shaping function on the characteristics of HVS can be represented as follows:

$$\alpha(k_1, k_2) = f\left(T(i,j),\ X_{0,0},\ X(i,j)\right) \tag{5.2}$$

where the first variable, T is the visibility threshold representing frequency sensitivity of HVS. $X_{0,0}$ is the DC DCT coefficient, while $X(i,j)$ is the AC DCT coefficient of the current block. They represent the luminance sensitivity and contrast masking characteristics of HVS respectively.

Operating the GPSF on all of the DCT coefficients, we obtain the perceptual mask for the current cover image. The product of the spread-spectrum sequence and expanded message bits is multiplied with this

perceptual mask to obtain the watermark. The 2-D watermark signal $\mathbf{W}$ (figure 2.1 and 5.3) is given as:

$$\mathbf{W} = \boldsymbol{\alpha} \cdot \mathbf{S} \cdot \mathbf{b} \tag{5.3}$$

As we are genetically tuning WPM whose corresponding perceptual mask is represented by $\boldsymbol{\alpha}$, therefore, equation 5.3 will be modified as follows:

$$\mathbf{W} = \boldsymbol{\alpha}_G \cdot \mathbf{S} \cdot \mathbf{b} \tag{5.4}$$

Where $\boldsymbol{\alpha}_G$, representing perceptual mask corresponding to GPSF, incorporates the dependencies from WPM, AC and DC coefficients and the intended attack.

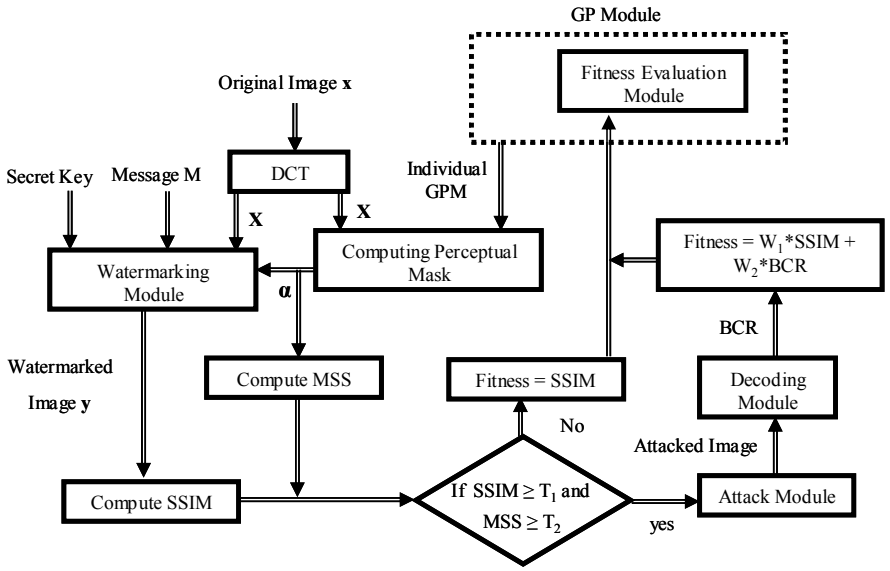

Figure 5.3 Detailed structures of the attack-resistant GPSS

If A denotes the information about the distortion of the intended attack, then equation 5.2 is modified to include the resultant changes in the distribution of the DCT coefficients caused by the attack as follows:

$$\alpha_G(k_1, k_2) = f\left(\alpha(k_1, k_2),\ X_{0,0},\ X(i, j),\ A\right) \tag{5.5}$$

It should be noted that the dependence of α_G on A is not explicit; rather it represents the implicit learning of the GP search mechanism in view of the conceivable attack.

5.2.1.3 Watermarking Module

The performance of each individual GPSF of the GP population is evaluated by watermarking module. This module implements the spread

spectrum based watermarking technique proposed by Hernandez et al. [5]. The embedding in DCT-domain is performed using equation 4.4. The watermarking module of our proposed technique provides the imperceptibility of the resultant watermark as a feedback to the GP module. The structure of how different sub-modules work within the GPSS is shown in figure 5.3.

5.2.1.4 Attack Module

In this module, the anticipated attack is performed on the watermarked image. We assume that the decoding module is fixed and does not modify in accordance to the attack. Specifically, to develop Wiener attack-resistant GPSF, before decoding the embedded message, we perform Wiener attack. Similarly to develop JPEG, Median filtering, and Gaussian attack-resistant GPSFs, GP simulations are carried out separately with each attack being performed before decoding the message.

5.2.1.5 Decoding Module

The decoding module receives the corrupted image after an attack as an input. It performs decoding of the embedded message as discussed in [5]. The same GPSF, as used in the embedding stage, is used to obtain the perceptual mask for the received image. The perceptual mask is then used to obtain sufficient statistics for the Maximum Likelihood based decoder.

5.2.2 Bonus Fitness-based Evolution

In the decoding stage, both imperceptibility and robustness requirements of a watermark are implemented through the use of multi-objective fitness function [24-27]. One way to perform this is to use equation 5.1. However, the drawback of this type of fitness function is that due weightage for learning the distribution of the DCT coefficients of each block of a cover image is not incorporated. In other words, instead of searching for a superior and image independent GPSF, main effort of the GP search is spent on searching a GPSF that results in high BCR value. Consequently, optimization of robustness versus imperceptibility tradeoff is belittled. This type of GPSF is not image adaptive and might have very poor performance for attacks other than the intended attacks. This problem is solved by using the idea of bonus fitness that we have used in our earlier work [35]. As can be examined from figure 5.3, those GPSF that make a better tradeoff between robustness and imperceptibility, are given bonus fitness. The bonus fitness is the amount of resistance against the intended attack in terms of BCR_{attack}. Thus equation 5.1 is modified as follows:

$$Fitness = \begin{cases} W_1 * Fitness_1 + W_2 * Fitness_2 & if\ SSIM \geq T_1\ and\ MSS \geq T_2 \\ W_1 * Fitness_1 & otherwise \end{cases} \quad (5.6)$$

where $Fitness_1 = SSIM_{E.S}$ while $Fitness_2 = BCR_{attack}$ and T_1, T_2 are lower bounds of $SSIM_{E.S}$ and MSS respectively.

In this way, the second driving force is separated from the first and basic driving force through the concept of bonus fitness. Otherwise, the GP simulation will usually tend to focus on the second requirement and will altogether neglect the basic requirement. Figure 5.4 elaborates this idea of bonus fitness incorporated in the GP search. We can observe that in each generation, those GPSF that make a good tradeoff are tagged (they are represented with star symbol and thus conceptually separated from the main GP search beam). A competition in terms of the 2nd fitness among these tagged GPSF then starts immediately. The overall fitness is improved with improvement in both types of fitness. The selection of when to tag an individual GPSF, by judging the tradeoff, is of crucial importance. It is implemented by requiring the MSS and SSIM values to lie above certain lower bounds. The smaller these lower bounds for fulfilling the first fitness criteria are, the larger is the diversity among the tagged GPSFs.

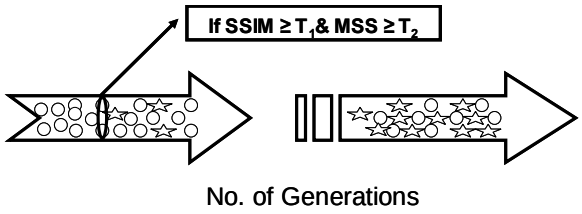

Figure 5.4 Block diagram of the bonus fitness idea

5.2.3 Testing Performance of the Best-evolved GPSF

In order to assess the performance of the best-evolved GPSF, its expression is saved at the end of the GP simulation. The best-evolved GPSF is then compared with that of WPM in terms of watermark shaping. Where by the watermark shaping ability is assessed by computing watermark imperceptibility as well as robustness measures. Figure 5.5 shows the details of the testing phase for the evolved GPSF.

5.3. Implementation Details

The GP parameter settings are shown in table 5.1, while the remaining parameters are used as default in the software. The

watermark power, represented by MSS, is constrained to lie above a certain lower bound for all the individuals. To assign bonus fitness, we have taken T_1, T_2, W_1 and W_2 as 0.96 , 20.0, 1.0 and 1.0 respectively. The values of T_1, T_2 are set empirically.

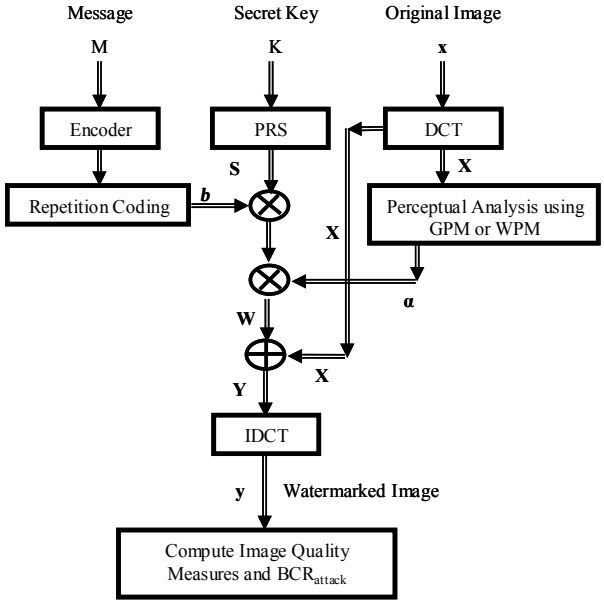

Figure 5.5 Details of the testing method for the attack-resistant GPSF

In the testing phase, all images except Baboon and Boat are of size 256x256. The attacks for which specific GPSF are developed, include adaptive Wiener filtering of window size 3x3, JPEG compression (QF = 80), Median filtering of window size 3x3 and Gaussian noise of σ = 50. In order to develop GPSF, keeping population size equal to 300 and no. of generations 30, the GP simulation consumes about one hour on a Pentium IV machine (2.0 GHz speed and 256 Mb RAM). In the testing phase, the watermarking scheme using the best-evolved GPSF spends about 30 sec to watermark Lena image. The rest of the implementation details are the same as in section 4.3.

5.4 Results and Discussion

5.4.1 Perceptual Shaping Using GPSF

In figure 5.6, watermarking strength corresponding to each bandpass DCT coefficient of block-based DCT is shown. These strengths

are produced by the Wiener attack-resistant GPSF for Lena image. It is observed that depending upon the current AC and DC coefficient, it provides suitable imperceptible alterations according to the spatial content of that block. This fact indicates that GPSF is able to exploit HVS for shaping the watermark according to any cover image. In other words, GPSF makes the watermarking technique adaptive with respect to the cover image. The resultant watermark is shown in figure 5.7.

Table 5.1 GP Parameter setting for evolving anticipated attack-resistant GPSF

Objective:	**To evolve conceivable attack-resistant GPSF**
Function Set:	+, -, *, protected division, *SIN, COS,* and *LOG*
Terminal Set:	Constants: *random constants in range* of [-1, 1] Variables : $X_{0,0}/1024, \lvert X(i,j)\rvert$ *and* $\alpha(i,j)$
Fitness :	*SSIM*
Selection:	Generational
Population Size:	260
Initial max.Tree Depth	6
Initial population:	Ramped half and half
Operator prob. type	Variable
Sampling	Tournament
Expected no. of offspring	rank89
Survival mechanism	Keep best
Real max level	31
Termination:	Generation 32

5.4.2 Imperceptibility of the resultant watermark

In figure 5.10, we have shown the difference image, obtained by subtracting the original image (figure 5.8) from the watermarked image (figure 5.9) in spatial domain. The pixel intensity of the difference image is amplified ten times for illustration purpose. Although, DCT domain is used for embedding, still GPSF is able to learn the spatial distribution of the Lena image, as most of the strong embedding is performed in highly textured areas.

5.4.3 GPSF developed for Wiener Attack

In table 5.2, both WPM and Wiener attack-resistant GPSF are compared in terms of the marked image quality and $(1-BCR_{attack})$ for 8 different standard images. The perceptual masks corresponding to both perceptual shaping functions are multiplied with some scaling factor to achieve equal distortion of the resultant watermarked image (in terms of approximately equal SSIM value for each image). It is observed that although evolved using Lena image, Wiener attack-resistant GPSF is image independent. This is because its imperceptibility measures are comparable to that of WPM for the entire test images. However, in terms of $(1-BCR_{attack})$ performance, the Wiener attack-resistant GPSF has superior performance as compared to that of WPM, for almost all of the test images. The Wiener attack-resistant GPSF is given below:

$$\boldsymbol{\alpha}_{\mathbf{G}}(k_1,k_2) = \cos(\sin(\boldsymbol{\alpha}(k_1,k_2)) + \boldsymbol{\alpha}(k_1,k_2)) + (\log(\cos(0.22897)) + 0.22897) * X(i,j) \qquad (5.7)$$

It can be observed that in this realization of α_G, α_G depends on α and $X(i,j)$. While, the dependence on A is implicitly being learned.

5.4.4 GPSF developed for Gaussian Noise Attack

Table 5.3, shows the same comparison in case of Gaussian noise attack (σ = 50). Again, Gaussian attack-resistant GPSF has comparable performance to that of WPM in terms of imperceptibility, while superior performance in case of robustness $(1-BCR_{attack})$. Figure 5.11, shows the watermarked image after being attacked by the Gaussian noise. Whereas, figure 5.12 demonstrates the $(1-BCR_{attack})$ versus standard deviation performance of both perceptual shaping functions. It can be observed that Gaussian noise attack-resistant GPSF has low $(1-BCR_{attack})$ values corresponding to different standard deviations.

5.4.5 GPSF developed for JPEG Compression Attack

Figure 5.13, 5.14 and table 5.4 show the same comparison in case of JPEG attack. It is observed that imperceptibility performance of the JPEG attack-resistant GPSF is low as compared to that of WPM (low SSIM values corresponding to less energy watermark embedding). But on the other hand, the improvement in $(1-BCR_{attack})$ performance in this case is far better from the previous two cases.

5.4.6 GPSF developed for Median Filtering Attack

Table 5.5, compares the evolved Median attack-resistant GPSF to that of WPM. In this case the imperceptibility performance at a certain level of watermark power is comparable, but $(1-BCR_{attack})$ performance is again superior.

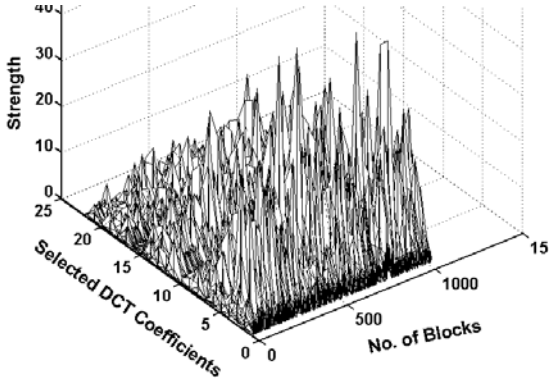

Figure 5.6 Watermarking strength distribution corresponding to the attack-resistant GPSF

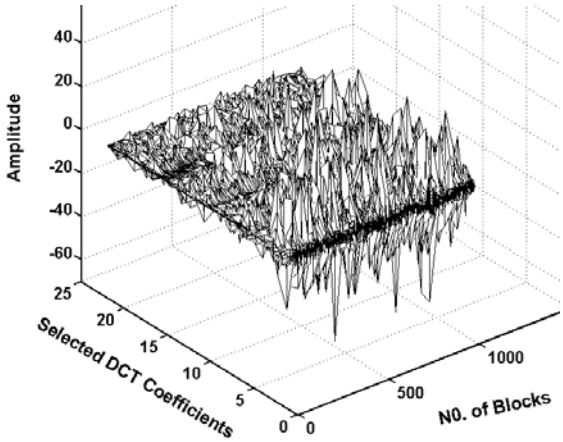

Figure 5.7 Watermark distribution corresponding to the attack – resistant GPSF

Figure 5.8 Original Image

Figure 5.9 Watermarked Lena Image using Attack-resistant GPSF

Figure 5.10 Difference Image

Figure 5.11 Watermarked image after Gaussian attack

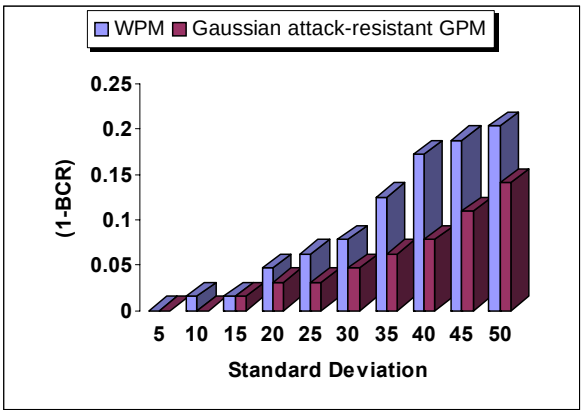

Figure 5.12 (1- BCR) versus standard deviation performance of both perceptual shaping functions

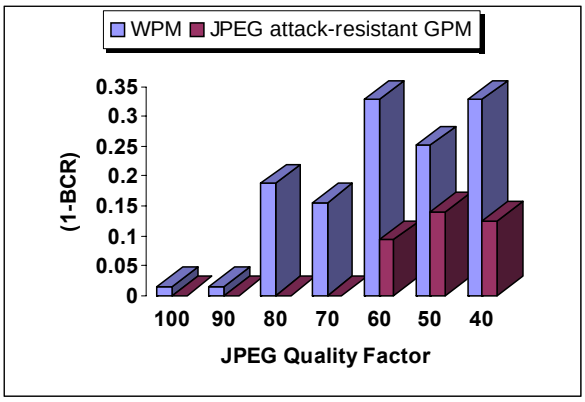

Figure 5.14 (1- BCR) versus quality factor of JPEG compression attack

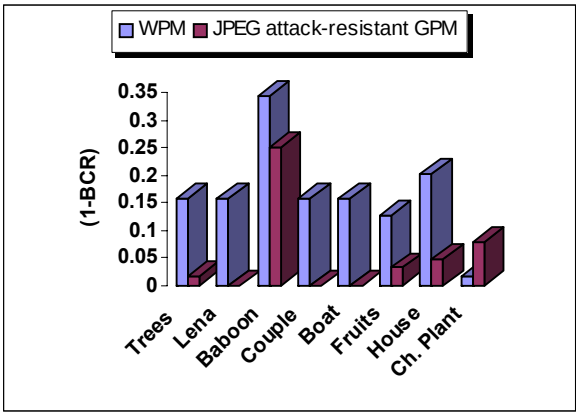

Figure 5.15 (1- BCR) versus JPEG attack (QF= 70) for different images

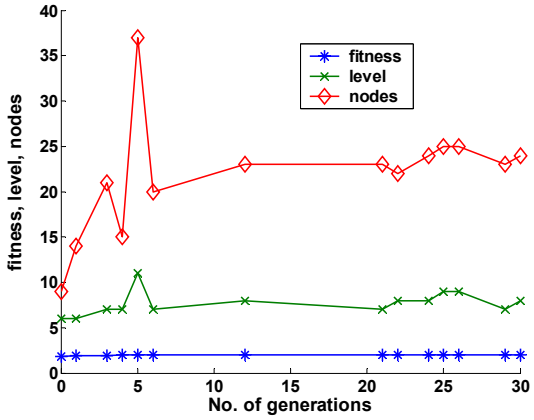

Figure 5.16 Accuracy versus complexity plot of GP simulation for evolving median filtering attack-resistant PSF

Table 5.2 Wiener attack-resistance performance comparisons

Images	Perceptual Model	Scaling factor	MSS	SSIM	WDR	*w*PSNR	(1-BCR)
Trees	WPM	0.30123	63.4553	0.9737	-29.604	40.617	0.125
	GPSF	0.48	83.991	0.9738	-28.386	39.951	0.0469
Lena	WPM	0.30123	23.696	0.9816	-33.3294	43.245	0.2656
	GPSF	1.282	17.1462	0.9816	-34.7357	44.0532	0.0
Baboon (232x248)	WPM	0.30123	72.2899	0.9779	-27.3715	43.477	0.0469
	GPSF	0.519	89.7937	0.9779	-26.4274	43.277	0.0313
Couple	WPM	0.30123	62.3051	0.9711	-28.913	40.2752	0.0938
	GPSF	0.552	80.3543	0.9711	-27.8227	39.68	0.0781
Boat (232x248)	WPM	0.30123	55.9301	0.9730	-29.908	40.6763	0.125
	GPSF	0.52	67.9235	0.9731	-29.065	40.144	0.0313
Fruits	WPM	0.30123	36.278	0.9737	-33.6307	41.3071	0.2344
	GPSF	0.513	71.0392	0.9771	-30.818	39.7361	0.1719
House	WPM	0.30123	26.643	0.9745	-33.6307	41.3071	0.0781
	GPSF	0.5524	39.1316	0.9745	-31.9648	39.7503	0.0781
Chemical Plant	WPM	0.30123	42.3627	0.9778	-29.4101	41.556	0.0781
	GPSF	0.494	56.589	0.9778	-28.1518	40.8834	0.0561

Table 5.3 JPEG attack-resistance performance comparisons

Images	Perceptual Model	Scaling factor	MSS	SSIM	WDR	*w*PSNR	(1-BCR)
Trees	WPM	0.30123	63.4553	0.9737	-29.604	40.617	0.0625
	GPSF	1.505	67.8033	0.9737	-29.3161	40.4706	0.0469
Lena	WPM	0.30123	23.696	0.9816	-33.3294	43.245	0.2031
	GPSF	1.554	25.126	0.9816	-33.0744	43.1152	0.1875
Baboon (232x248)	WPM	0.30123	72.2899	0.9779	-27.3715	43.477	0.0781
	GPSF	1.59	74.627	0.9778	-27.232	43.45	0.0313
Couple	WPM	0.30123	62.3051	0.9711	-28.913	40.2752	0.0625
	GPSF	1.694	67.173	0.9712	-28.588	40.1253	0.0469
Boat (232x248)	WPM	0.30123	55.9301	0.9730	-29.908	40.6763	0.0938
	GPSF	1.594	57.696	0.973	-29.772	40.606	0.0938
Fruits	WPM	0.30123	36.278	0.9737	-33.6307	41.3071	0.1563
	GPSF	1.53	42.734	0.9771	-33.025	41.0104	0.1406
House	WPM	0.30123	26.643	0.9745	-33.6307	41.3071	0.1719
	GPSF	1.609	27.1527	0.9745	-33.547	41.288	0.1563
Chemical Plant	WPM	0.30123	42.3627	0.9778	-29.4101	41.556	0.0781
	GPSF	1.51	46.917	0.9778	-28.966	41.289	0.0781

Table 5.4 Gaussian noise attack-resistance performance comparisons

Images	Perceptual Model	Scaling factor	MSS	SSIM	WDR	*w*PSNR	(1-BCR)
Trees	WPM	0.30123	63.4553	0.9737	-29.604	40.617	0.2344
	GPSF	0.787	40.533	0.9737	-31.55	40.7437	0.0469
Lena	WPM	0.30123	23.696	0.9816	-33.3294	43.245	0.1719
	GPSF	1.252	18.83	0.9816	-34.329	43.313	0.0
Baboon (232x248)	WPM	0.30123	72.2899	0.9779	-27.3715	43.477	0.3438
	GPSF	1.163	78.475	0.9778	-27.014	41.488	0.2188
Couple	WPM	0.30123	62.3051	0.9711	-28.913	40.2752	0.2188
	GPSF	1.072	104.39	0.971	-26.659	36.9406	0.0781
Boat (232x248)	WPM	0.30123	55.9301	0.9730	-29.908	40.6763	0.1563
	GPSF	1.178	63.283	0.973	-29.362	38.104	0.0781
Fruits	WPM	0.30123	36.278	0.9737	-33.6307	41.3071	0.25
	GPSF	1.563	49.919	0.9771	-32.353	40.3825	0.0625
House	WPM	0.30123	26.643	0.9745	-33.6307	41.3071	0.1719
	GPSF	1.818	24.124	0.9745	-34.055	41.562	0.0
Chemical Plant	WPM	0.30123	42.3627	0.9778	-29.4101	41.556	0.1875
	GPSF	0.978	20.622	0.9778	-32.535	42.4616	0.0781

Table 5.5 Median filtering attack-resistance performance comparisons

mages	Perceptual Model	Scaling factor	MSS	SSIM	WDR	*w*PSNR	(1-BCR)
Trees	WPM	0.30123	63.4553	0.9737	-29.604	40.617	0.1563
	GPSF	1.413	26.869	0.9737	-33.34	42.5537	0.0156
Lena	WPM	0.30123	23.696	0.9816	-33.3294	43.245	0.1563
	GPSF	1.128	10.2681	0.9816	-36.9644	45.06	0.0
Baboon (232x248)	WPM	0.30123	72.2899	0.9779	-27.3715	43.477	0.3438
	GPSF	1.544	35.026	0.9779	-30.527	44.149	0.25
Couple	WPM	0.30123	62.3051	0.9711	-28.913	40.2752	0.2188
	GPSF	1.65	34.089	0.971	-31.53	41.4407	0.0
Boat (232x248)	WPM	0.30123	55.9301	0.9730	-29.908	40.6763	0.1563
	GPSF	1.382	23.9525	0.973	-33.6025	42.4273	0.0
Fruits	WPM	0.30123	36.278	0.9737	-33.6307	41.3071	0.125
	GPSF	1.066	12.3244	0.9771	-38.4293	41.865	0.0313
House	WPM	0.30123	26.643	0.9745	-33.6307	41.3071	0.2031
	GPSF	1.003	10.0407	0.9745	-37.8633	44.3606	0.0469
Chemical Plant	WPM	0.30123	42.3627	0.9778	-29.4101	41.556	0.0156
	GPSF	1.405	24.8827	0.9778	-31.7236	42.4763	0.0781

The reason behind this is that the attack-resistant GPSF spreads the watermark energy in such areas, where the attack as well as the distortion affect is less.

Figure 5.15 shows the accuracy versus complexity plot of GP simulation. It is observed that as generations pass by, improvement in fitness of the best Median attack-resistant GPSF is achieved at the cost

of its complexity. That is, with increase in fitness of the best GPSF of a generation, its genome's total number of nodes as well as its average tree depth increases. The above analysis of the various evolved GPSFs indicate that GPSS develops GPSF that results in cover image as well as attack dependent restructuring of the watermark.

5.5 Conclusions

In this chapter we have considered the GP-based perceptual shaping of a digital watermark in accordance to the cover image and anticipated attack. The GP tuned GPSFs are image adaptive and the GPSS as a whole is attack adaptive. A significant improvement in resistance against the intended attack is achieved by letting the GP search exploit the attack information. This is in essence, like attack-informed embedding. Both these attributes of a GPSF; superior tradeoff and high resistance against an anticipated attack, are obtained by incorporating the concept of bonus fitness in multi-objective fitness function. Developing GPSF needs considerable execution time (about one hour). However, once the best GPSF is developed, then employing GPSF for watermark shaping is quite straight forward and easy to implement. Even in the development phase, with the use of fast and parallel processing based implementations of GP [38-39], it is possible to use GP-based watermarking to real business applications. The proposed GPSS is applicable for tuning other perceptual shaping functions as well. In addition to the selection of suitable strength, the selection of DCT coefficients for embedding as proposed in [8] may also be performed. This will require the whole 63 AC coefficients of a DCT block to be considered for embedding, instead of the middle frequency coefficients. This may further improve the resistance against the intended attack, as different attacks usually affect different frequency bands in DCT block.

Chapter 6

Achieving Robustness against a Cascade of Conceivable Attacks during Watermark Shaping

In this chapter, we let the GP exploit the characteristics of human visual system, as well as information pertaining to the distortion caused by a set of conceivable attacks. The set of conceivable attacks are carried out in sequence, before extracting the embedded message obliviously. Improvement in imperceptibility and reduction in bit incorrect ratio after attack, have been employed as the multi-objective fitness criteria in the GP search. The actual performance of the genetic perceptual shaping function is judged through experiments, which validate the use of intelligent search techniques in shaping a watermark according to the set of conceivable attacks.

6.1 Introduction

With the exception of fragile watermarking systems, almost all watermarking systems need to be resistant against any intentional or unintentional processing of the watermarked image. This attribute of a watermarking system is usually called robustness. These attacks and their countermeasures are studied in the context of the watermark applications, as different applications are mostly concerned with a different set of conceivable attacks [1]. Therefore, while designing a watermarking system, its intended application and thus the corresponding set of conceivable attacks are of prime importance.
Usually robustness is achieved at the cost of imperceptibility. As these two properties contradict each other, therefore, while designing a watermarking system, one need to make a delicate balance between these properties in accordance to the anticipated application. This need has prompted the use of intelligent optimization techniques; where by the issue of making balanced alteration to the original features during embedding is formulated as an optimization problem. This includes the work by Huang et al [8], where keeping in view the robustness versus imperceptibility tradeoff; optimal embedding positions in a block-based DCT domain watermarking are selected using Genetic Algorithms. Exploiting machine-learning capabilities for improvement of watermarking schemes, we have been employing GP for developing optimal perceptual shaping functions-shaping functions that make an effective tradeoff between robustness and imperceptibility [9-11]. In chapter 3, we have concentrated on optimal shaping of a digital

watermark for the whole DCT-domain based watermarking scheme. In chapter 4 using GP, we have developed perceptual shaping functions for the block-based DCT domain watermarking schemes. This model is image adaptive and offers superior performance in terms of tradeoff as compared to the conventional Watson's model originally designed for JPEG compression. On the other hand, in chapter 5, in addition to the tradeoff, we have exploited the conceivable attack information as well. For this purpose, we have considered it as a multi-objective optimization problem, achieving an optimal tradeoff as well as structuring the watermark in accordance with the conceivable attack.

Besides striking a tradeoff between robustness and imperceptibility, machine-learning techniques are also applied to the detection of a hidden message i.e. classifying watermarked and unwatermarked works. Lyu et al [20] have used high order statistics as features and Support Vector Machine (SVM) as classifier for detecting hidden messages in an image. Fu et al [21], have proposed optimal watermark detection by exploiting the generalization capabilities of SVM. Yu et al [22], have used neural networks in watermarking for enhancing robustness against some of the common attacks.

Perceptual models as those of Watson's, do not take into consideration the watermark application and thus the anticipated attacks. For instance, we consider a scenario, where a watermarked image is expected to be JPEG compressed, transmitted through a channel characterized by Gaussian noise, and further distorted by an adversary using Wiener estimation. In this set of circumstances, it is judicious to structure the watermark in view of these anticipated attacks. Other pertinent examples, where the watermarking system needs to be robust against a set of conceivable attacks exist in literature [1]. Few set of conceivable attacks that are likely to occur between embedding and detection stages of a watermark include; digital-to-analog conversion, analog recording , re-recording and noise reduction in case of audio signal, while analog-to-digital conversion, lossy compression and format conversion in case of a possible video transmission.

Restructuring of a watermark in view of the anticipated attack is mostly performed by keeping high watermark strength for those selected coefficients that are less affected by the attack. However, firstly this requirement needs to consider limitations imposed by imperceptibility. Secondly, this requirement varies for different types of attacks. Consequently, as described earlier, our aim in this work is to propose and study an automatic system that can restructure the watermark in accordance to the cover image and intended attacks. Specifically, we propose a system for developing suitable perceptual shaping functions, which are application-specific, but image independent.

We address these requirements through the following contributions:

1. We comprehend the fact that while dealing with attacks, achieving resistance against of a set of conceivable attacks is a more realistic

approach instead of making a watermark resistant to an individual conceivable attack.

2. We realize the fact that making a watermark robust against a set of conceivable attacks is hard to be handled analytically, and thus propose a method that can intelligently generate an application-specific PSFs.

6.2. Proposed Attack-resistant Perceptual Shaping

Figure 5.1 illustrates the basic architecture of our proposed scheme for developing perceptual shaping functions. Five modules work in a cyclic fashion. We first explain the overall working of the basic architecture. Details of the individual modules are given in section 6.1.

The GP module produces a population of GPSF. Each GPSF is presented to the perceptual shaping module, where it is applied to the cover image in DCT-domain, generating a perceptual mask. In the watermarking stage, the watermark is shaped using the perceptual mask. The conceivable attacks are performed in a sequence on the watermarked image in the attack module. In the decoding module, the embedded message is retrieved from the corrupted image. The watermark imperceptibility at the embedding stage and BCR_{attack} at the decoding stage, are then used in the scoring criterion of the GP module (figure 5.1). In this way, the GP module evaluates the performance of its several generated GPSFs.

6.2.1 Detailed Structure of the GP Training Phase

The basic details are the same as given in section 5.2. The modules which have been modified are explained as follows:

6.2.1.1 Assessing Performance of each individual of a GP Population

GP fitness function is supposed to rank each individual of the population. It is designed to provide feedback about how well an individual of the GP population is performing at the given task. More details are given in section 2.3.1. Every perceptual shaping function of a GP population is evaluated in terms of structuring the watermark. The evaluation is based on how well is the SSIM measure at a certain level of watermark power as well as how high the BCR value is:

$$Fitness = W_1 * Fitness_1 + W_2 * BCR_{attack} \quad (6.1)$$

where $Fitness_1 = W_{10} * SSIM_{E.S} + W_{11}(wPSNR/46)$ represents a measure of watermark imperceptibility in terms of two recently proposed image

quality measures. $SSIM_{E.S}$ denotes the structure similarity index measure of the marked image at a certain level of estimated robustness. *W* represents the corresponding weightage of the different terms used in the fitness.

A fair enough quality of the resultant watermarked image in terms of *ωPSNR* that we observed through empirical analysis is approximately 46 db, while the maximum value that *SSIM* can achieve is 1.0. As a result, in $Fitness_1$, we divide the *ωPSNR* by 46 in order to scale its value to 1.0 as well. If W_1 and W_2 are set to 1.0, while W_{10} and W_{11} are set 0.5 each, the fitness attains a maximum value near to 2.0.

Thus, each individual perceptual shaping function of a GP population is scored using equation 6.1 as a fitness function. The greater the fitness is, the better the individual has performed.

6.2.1.2 Ceasing GP Simulation

The GP simulation is ceased when one of the following conditions is encountered:

1. The fitness score exceeds 1.99 with MSS ≥ 8.0.
2. The number of generations reaches the predefined maximum number of generations.

6.2.1.3 Attack Module

In this module, attacks are performed on the watermarked image. We assume that the decoding module is fixed and does not modify in accordance to the attacks. Specifically, to develop the application-specific GPSF, the related set of conceivable attacks is carried out on the watermarked image before decoding the embedded message.

The bonus fitness is the amount of resistance against the intended attack in terms of BCR_{attack}. Thus equation 6.1 is modified as follows:

$$Fitness = \begin{cases} W_1 * Fitness_1 + W_2 * BCR_{attack} & if \quad Fitness_1 \geq T_1 \quad and \quad MSS \geq T_2 \\ W_1 * Fitness_1 & otherwise \end{cases} \tag{6.2}$$

where T_1, T_2 are lower bounds of $Fitness_1$ and MSS respectively.

6.2.2 Performance Evaluation on the Test Images

In order to assess the performance of the best-evolved GPSF, its expression is saved at the end of the GP simulation. The best-evolved GPSF is then compared with that of WPM in terms of watermark shaping for various test images. Here in, the watermark shaping ability is assessed by computing watermark imperceptibility as well as robustness measures.

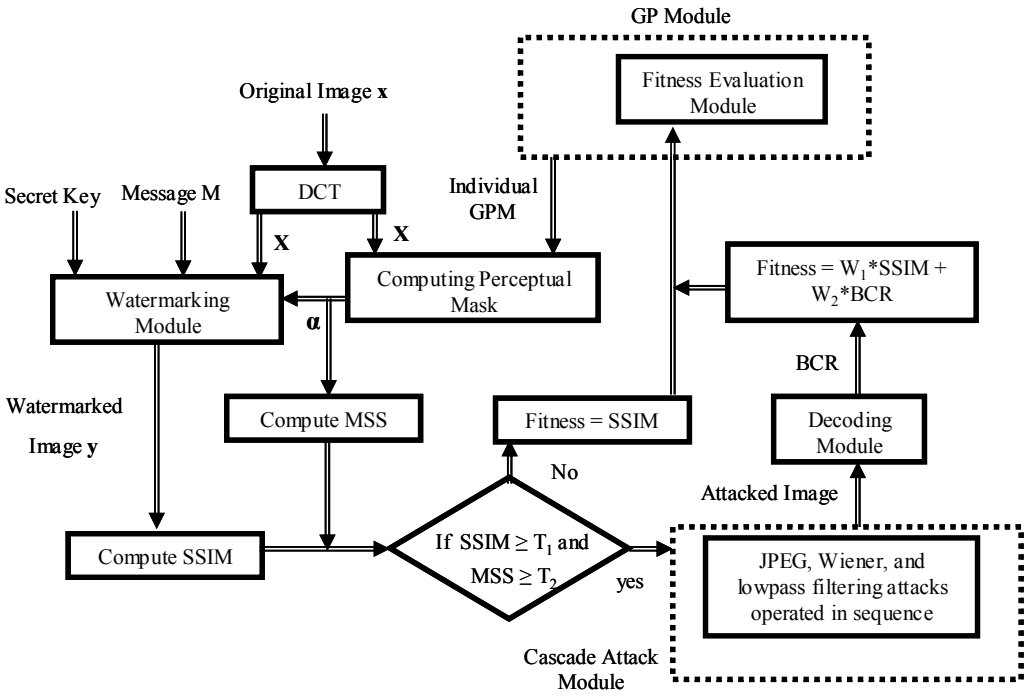

Figure 6.1 Detailed structure of the cascade attacks-resistant GPSS

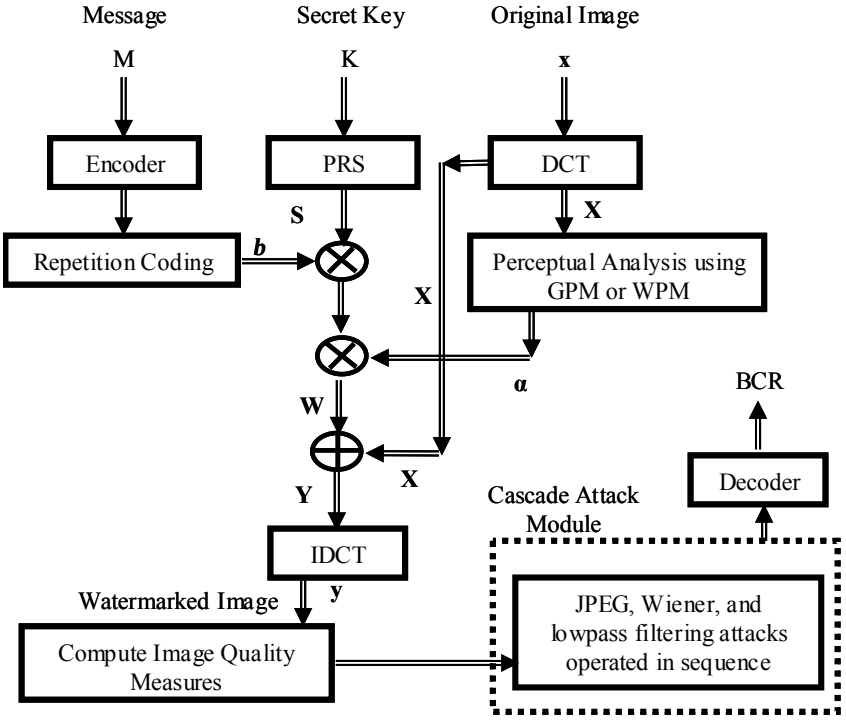

Figure 6.2 Details of the testing phase for the evolved cascade attacks-resistant GPSF

We have strived to compare both perceptual shaping functions in a harsh environment. Firstly, low power embedding is performed. Increasing the watermark strength and thus reducing imperceptibility will most probably improve message retrieval performance in case of both perceptual shaping functions. Secondly, only repletion coding is employed, both in evolution and testing phase. Employment of advance channel coding strategies, for example low density parity check [40] and turbo [69] coding, would certainly improve the overall message retrieval performance in both cases. Figure 6.2 shows the details of the testing phase for the evolved GPSF.

6.3. Implementation Details

The GP parameter settings are shown in table 5.1, while the remaining parameters are used as default in the software.
To assign bonus fitness, we have taken T_1, T_2, W_1 and W_2 as 0.98 , 8.0, 1.0 and 1.0 respectively. W_{10} and W_{11} are set 0.5 each. The values of T_1, T_2 are set empirically.
The set of conceivable attacks for which specific GPSF is developed, include, JPEG compression (QF = 90), adaptive Wiener filtering of window size 3x3, and Lowpass filtering.

6.4. Results and Discussion

6.4.1 Performance Comparison in terms of Perceptual Shaping

Figure 6.3 illustrates the distribution of the selected DCT coefficients. Figure 6.4, on the other hand, shows the corresponding distribution of the strength of alterations. This distribution of strength of alterations is obtained using the best-evolved GPSF for Lena image. It is observed that depending upon the current AC and DC coefficient; it provides suitable imperceptible alterations according to the spatial content of that block. This fact indicates that GPSF is able to exploit HVS for shaping the watermark according to any cover image. The resultant watermark is shown in figure 6.5.

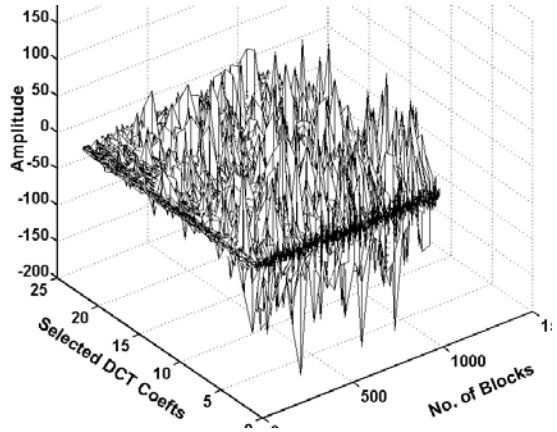

Figure 6.3 Distribution of the modified DCT coefficients

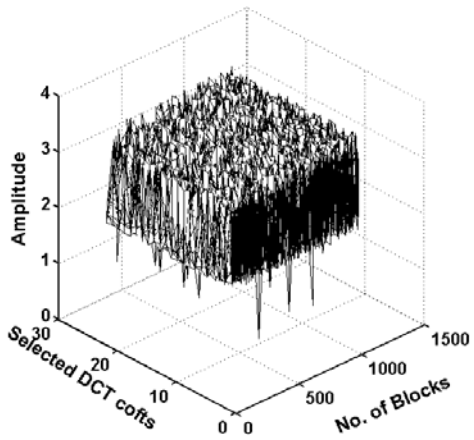

Figure 6.4 Distribution of the watermarking strength

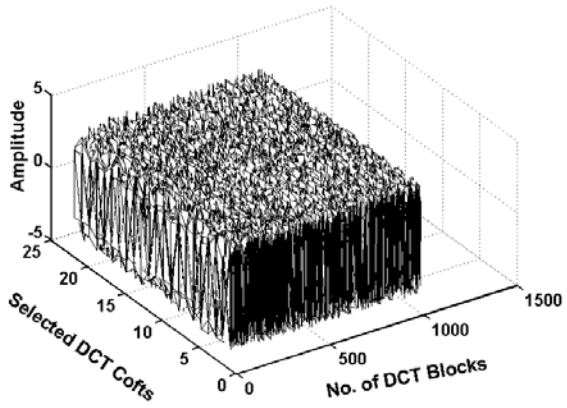

Figure 6.5 Watermark distribution

Figure 6.6 Original Image

Figure 6.7 Watermarked Lena Image using the evolved cascade attacks-resistant GPSF

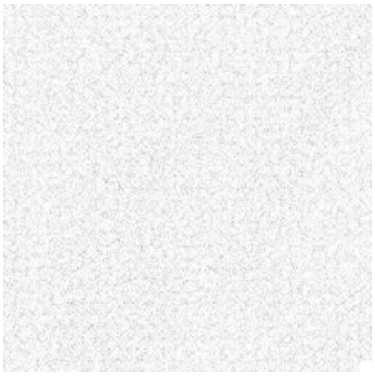

Figure 6.8 Difference Image

In figure 6.8, we have shown the difference image, obtained by subtracting the original image (figure 6.6) from the watermarked image (figure 6.7) in spatial domain. The pixel intensity of the difference image is amplified ten times for illustration purpose.

6.4.2 Performance Comparison against the Cascade of Conceivable Attacks

In table 6.1, both WPM and best-evolved GPSF are compared in terms of the marked image quality and $(1-BCR_{attack})$ for 8 different standard images. The perceptual masks corresponding to both perceptual shaping functions are multiplied with some scaling factor to achieve equal distortion of the resultant watermarked image (in terms of approximately equal SSIM value for each image). It is observed that although evolved using Lena image, best-evolved GPSF is image independent. This is because its imperceptibility measures are comparable to that of WPM for the entire test images. However, in terms of $(1-BCR_{attack})$ performance, the best-evolved GPSF has superior performance as compared to that of WPM, for almost all of the test images. The best-evolved GPSF in prefix notation is given below:

$$\begin{aligned}\boldsymbol{\alpha}_{\mathbf{G}}(k_1,k_2) = {} & \log(*(+(*(\log(\alpha(k_1,k_2)),\max(c1,\sin(c2))),*(\cos(\alpha(k_1,k_2)),0.77939)),\\ & -(-(\cos(z),\log(0.25848)),/(*(\alpha(k_1,k_2),X(i,j)),\sin(0.12886)))))\end{aligned} \tag{6.3}$$

where

$$c1 = \max(\max(\mathrm{X(i,j)},\mathrm{z}),\max(\alpha,\mathrm{X}_{0,0})) \quad \text{and} \quad c2 = \log(\mathrm{X(i,j)}+,\mathrm{X}_{0,0})$$

Also, it should be noted that z represents the index of the selected DCT coefficient in zigzag order inside a DCT block. This modification of allowing z as an independent variable is performed to cope for the effectiveness of location inside a DCT block in view of the attacks. Besides the first modification; cascade of attacks instead of a single attack, this in essence, is the major difference of this chapter as against chapter 5. The general functional form of GPSF, in comparison to equation 5.5, is now given as:

$$\alpha_G(k_1,k_2) = f(\alpha(k_1,k_2),\ X_{0,0},\ X(i,j),\ z, A) \tag{6.4}$$

Table 6.1 GP Parameter setting for evolving anticipated Cascade attack-resistant GPSF

Test Images	Perceptual Model	Watermark strength	Decoding performance		
		Scaling Factor	wPSNR	SSIM	1-BCR
Lena	WPM	0.3660	44.3450	0.9811	0.2344
	GPSF	0.7100	45.3382	0.9814	0.0625
Trees	WPM	0.4100	43.2389	0.9806	0.1875
	GPSF	1.125	44.6309	0.9813	0.1175
Baboon (232x248)	WPM	0.5040	44.5299	0.9810	0.1250
	GPSF	0.1250	45.1228	0.9813	0.1031
Couple	WPM	0.4400	42.8138	0.9810	0.0938
	GPSF	0.9750	43.8208	0.9812	0.0625
Boat (232x248)	WPM	0.4020	43.5568	0.9812	0.0938
	GPSF	0.8600	44.5875	0.9813	0.0781
Airplane	WPM	0.2440	46.2615	0.9809	0.0156
	GPSF	0.5550	46.7912	0.9811	0.0469
Watch	WPM	0.4250	44.3692	0.9813	0.1875
	GPSF	0.7200	45.6630	0.9813	0.1094
Fruits	WPM	0.3310	44.0709	0.9807	0.0469
	GPSF	0.7100	45.0101	0.9813	0.0313
House	WPM	0.3140	45.3106	0.9815	0.0625
	GPSF	0.6400	45.8659	0.9812	0.0250
Chemical Plant	WPM	0.4730	42.7162	0.9810	0.1719
	GPSF	0.9450	43.6662	0.9813	0.1094

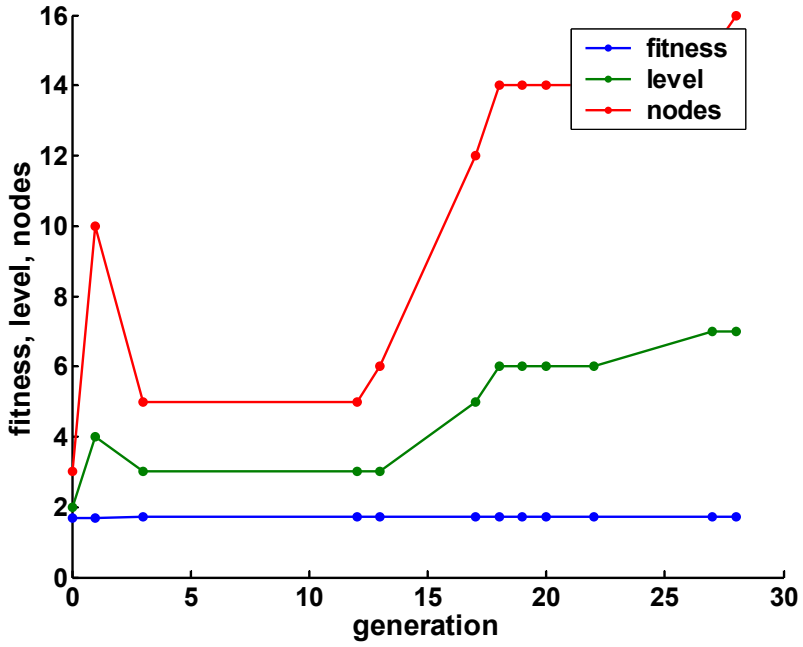

Figure 6.9 Accuracy versus complexity plot of GP simulation for evolving cascade attacks-resistant GPSF

6.4.3 Fitness-gain versus Complexity of GP Simulation

Striving for improved fitness-based performance, the GP simulation mostly generates complex individuals during the stepwise refinement process. This is because more lengthy and complex expressions may incorporate exploitation of certain features ignored by others. In GP literature [25, 26, 30], several techniques are applied to help evolve concise, but accurate expressions. The accuracy versus complexity curve of our GP simulation is shown in figure 6.9. It can be observed that as generations pass by, improvement in fitness of the best individual is achieved at cost of its complexity. That is, with increase in fitness of the best perceptual shaping function of a generation, its genome's total number of nodes as well as its average tree depth increases.

6.5. Conclusions

We have practically demonstrated the potential of watermark shaping stage for fusing the watermark in accordance to a set of conceivable attacks. The proposed scheme develops image adaptive and application-specific perceptual shaping functions, able to shape the watermark in accordance to any cover image and a given set of conceivable attacks. Watermark imperceptibility is ensured by making GP exploit HVS Characteristics in the DCT domain. On the other hand, the significant improvement in resistance against the a given set of conceivable attacks is achieved by letting the GP search, exploit the information pertaining to the distortion caused by given set of conceivable attacks. Both the imperceptibility and effective robustness attributes are obtained by incorporating the concept of bonus fitness in multi-objective fitness function. The proposed technique is easy to understand, implement, and possess potential of being used in real business applications.

Chapter 7

Conclusions

Concealment of a watermark is an interesting problem. In order to make the watermark imperceptible, one is prompted to use the perceptually insignificant coefficients. This generally, tilts the distribution of watermark energy towards the high frequency, which lessens the expected robustness. The reliability of a watermark, on the other hand, generally entails watermark energy to be embedded in perceptually significant coefficients. Thus, from one end we are pushed to use high frequency, while from the other end to use low frequency. This leaves us with nothing, except to make a delicate balance between these two contradicting requirements. The distribution of this balance, considering the two dimensional distribution of coefficients, depends on the given cover image as well as the application. A given cover image could be highly textured in nature, on contrary; it could be of smooth nature. Further, it could have low and high components both in balanced amount. Even further, some applications may require high robustness and low concealment or low robustness but high concealment. Consequently, an efficient, intelligent, and dynamic system that can fulfil these basic requirements is needed the most.

We have tried to develop such intelligent technique−technique based on GP, which develops applications–specific, but image adaptive perceptual shaping functions. Chapter 3-4 discuss the development of perceptual shaping functions possessing image adaptive capabilities. Here, the main target in the optimization problem is to decrease the perceptual distance between the watermarked and original image, while keeping the estimated robustness fixed.

Chapter 5-6, on the other hand, discuss the development of perceptual shaping functions possessing image adaptive as well as application-specific capabilities. In these chapters, we remodel our optimization problem and try to first decrease the perceptual distance at certain level of estimated robustness. But, once a certain lower level of perceptual distance is reached, we also strive for improvement in actual robustness through the use of our bonus fitness idea for implementing multi-objective function in GP. Specifically, chapter 6 explains our proposed approached of developing perceptual shaping functions that shape the watermark not only according to the given cover image, but according to a battery of conceivable attacks as well.

7.1 Contributions: Details in reference to individual chapters

We further elaborate our main contributions by answering questions related to the perceptual shaping of a watermark. These questions are related to the hypothesis of our research work and are as follows:

1. Could we enhance the tradeoff between robustness and imperceptibility as compared to the existing perceptual shaping functions?
2. Is the actual robustness truly depicted by estimated robustness?
3. Besides enhancing tradeoff, could we use perceptual shaping for achieving effective resistance against anticipated attacks?
4. Does the increasingly trend of sophistication of the watermarking systems and of the corresponding malicious attempts, requires the use of intelligent search techniques in watermarking?

The relevant details concerning answers to these questions are as follows:

7.1.1 Could we enhance the tradeoff between robustness and imperceptibility as compared to the existing perceptual shaping functions?

In chapter 3, a GPSF is evolved that effectively shapes the watermark according to the cover image in full-frame DCT domain. Unlike the heuristic techniques used in [2] that search for a constant watermarking strength for each new cover image, the GPSF is image adaptive and selects a suitable watermarking strength for each *DCT* coefficient. The evolved perceptual shaping functions for full-frame DCT is quite general and can be used in any full frame *DCT* domain-based watermarking technique.

In chapter 4, the developed perceptual shaping functions for block-based DCT domain is a combination of frequency and luminance sensitivity as well as contrast masking. It offers superior performance to that of Watson's perceptual model [16] in terms of watermarked imperceptibility.

7.1.2 Is the actual robustness truly depicted by estimated robustness based on watermark power?

Our analysis in chapter 4 shows that high power embedding does not always reflect high practical robustness. We have assumed watermark power to be depicting robustness. For this purpose, we have used MSS (equation 2.1) as a measure representing estimated robustness. However, our analysis in chapter 4 shows that high power embedding may not always mean high actual robustness.

7.1.3 Besides enhancing tradeoff, could we use perceptual shaping for achieving effective resistance against anticipated attacks?

In chapter 5, we have considered the GP-based perceptual shaping of a digital watermark in accordance to the cover image and anticipated attack. The GP tuned GPSFs are image adaptive and the GPSS as a whole is attack adaptive. A significant improvement in resistance against the intended attack is achieved by letting the GP search exploit the attack information. This is in essence, like attack-informed embedding. Both these attributes of a GPSF; superior tradeoff and high resistance against an anticipated attack, are obtained by incorporating the concept of bonus fitness in multi-objective fitness function.

In chapter 6, We have practically demonstrated the potential of watermark shaping stage for fusing the watermark in accordance to a set of conceivable attacks. The proposed scheme develops image adaptive and application-specific perceptual shaping functions, able to shape the watermark in accordance to any cover image and a given set of conceivable attacks.

7.1.4 Does the increasingly trend of sophistication of the watermarking systems and of the corresponding malicious attempts, requires the use of intelligent search techniques in watermarking?

This is almost true because even modeling the distortions introduced by the watermark addition itself, is not so simple. In addition to this, if a single attack is carried out, then modeling the distortion becomes more difficult. For example, some effort has been put to model distortion introduced due to JPEG compression attack [66]. If instead of a single attack, we have a battery of conceivable attacks, then modeling the resultant distortion analytically becomes almost impossible. Both in chapter 5 and 6, we have shown that GP is able to learn the information pertaining to distortion caused by either a single or a battery of attacks. This information is then exploited by the GPSFs to shape the watermark in accordance to these attacks.

This is only one issue that we are discussing in context of the potential use of intelligent techniques in watermarking. As discussed in

chapter 6, various machine learning-based approaches have been carried out in detection of watermark signals.

7.2 Future Work

We expect the use of intelligent techniques in complicated watermark applications to be quite prospective. Few possible extensions to our work that are of very interesting nature and may have strong impact, both on the way watermarking embedding as well as elimination problem is perceived.

7.2.1 Selection of both embedding positions and strengths of alterations

In addition to the selection of suitable strength, the selection of DCT coefficients for embedding may also be performed. This will require the whole 63 AC coefficients of a DCT block to be considered for embedding, instead of the middle frequency coefficients. This may further improve the resistance against the intended attack, as different attacks usually affect different frequency bands in DCT block.

7.2.2 Employing intelligent techniques for developing efficient and application-specific decoders

In a watermarking system, the decoder structures are mostly fixed. They do not account for the normal processing or intentional attacks. Therefore, a method of automatically modifying the decoder structure in accordance to the given cover image and conceivable attack is thus needed. This would require exploiting the search space regarding types of dependencies of the decoder on different factors.

References

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and fundamentals, Morgan Kaufmann, San Francisco, 2002.

[2] Hsiang-Cheh Huang, Lakhmi C. Jain, Jeng-Shyang Pan, Intelligent Watermarking Techniques, World Scientific Pub Co Inc, 2004.

[3] K. Su. Jonathan and B. Girod, Power-spectrum conditions for energy–efficient watermarking, IEEE Trans. on Multimedia, 4 (4), Dec. 2002.

[4] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," Proc Int. Conf. Image Processing, Oct. 1997, vol. 1 pp. 520-523.

[5] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, DCT-Domain watermarking techniques for still images: Detector performance analysis and a new structure, IEEE Trans. on Image Processing, 9(1), (2000), 55-68.

[6] A. Briassouli , P. Tsakalides and A. Stouraitis, Hidden messages in heavy-tails: DCT domain watermark detection using alpha-stable models, IEEE Trans. on Multimedia, Vol. 7, issue 4, 2005, pp. 700-715.

[7] C. Podilchuk and W. Zeng, Image-adaptive watermarking using visual models, IEEE Journal on Selected Areas in Communications, 10(4), (1998), 525-540.

[8] H. C. Huang, S. Wang and J. S. Pan, Genetic watermarking based on transform domain technique, Pattern Recognition, vol. 37, 2004, pp. 555-565.

[9] A. Khan, A. M. Mirza, A, Majid, Optimizing perceptual shaping of a digital watermark using genetic programming, Iranian Journal of Electrical and Computer Engineering (IJECE), vol. 3, no. 2 2004, pp. 144-150.

[10] A. Khan, Anwar M. Mirza and A. Majid, “Intelligent Perceptual Shaping of a Digital Watermark: Exploiting Characteristics of Human Visual System,” International Journal of Knowledge-Based Intelligent Engineering Systems, Vol. 9, 2005, pp. 1-11.

[11] A. Khan and Anwar M. Mirza, Genetic Perceptual Shaping: Utilizing Cover Image and Conceivable Attack Information Using Genetic

Programming, International Journal of Information Fusion, Elsevier Science, 2005, (in press).

[12] A. Khan, A. Majid and Anwar. M. Mirza, Combination and Optimization of Classifiers in Gender Classification Using Genetic Programming, KES journal, Netherlands, Vol. 8, 2004, pp. 1-11.

[13] D. Kundur, D. Hatzinakos, Towards Robust Logo Watermarking Using Multiresolution Image Fusion Principles, IEEE Trans. on Multimedia, 6(1), 2004, pp. 185-198.

[14] P. Meerwald, and A. Uhl, A survey of wavelet-domain watermarking algorithms, Proceedings of SPIE, Security and Watermarking of Multimedia Contents III, v. 4314, San Jose, CA, USA, January 22 - 25,200.

[15] S. Voloshynovskiy, A. Herrigel, N. Baumgaetner, and T. Pun, A stochastic approach to content adaptive digital image watermarking, In third international workshop on Information Hiding, (Dresden, Germany), Sep. 29, 1999.

[16] A. B. Watson, Visual optimization of DCT quantization matrices for individual images, in Proc. AIAA Computing in Aerospace 9, San Diego, CA, (1993), pp. 286–291.

[17] A. J. Ahumada and H. A. Peterson, Luminance-model-based DCT quantization for color image compression, Proc. SPIE on Human Vision, Visual Processing, and Digital Display III, vol. 1666, 1992, pp. 365–374.

[18] A. B. Watson, G. Y. Yang, J. A. Solomon, and J. Villasenor, Visibility of Wavelet Quantization noise, IEEE Trans. on Image Processing 6, 1997, pp. 1164-1175.

[19] M. L. Miller, G. J. Doerr and I. J. Cox, Applying informed coding and embedding to design a robust, high capacity watermark, IEEE Trans. on Image Processing, 13(6), 2004, pp. 792-807.

[20] S. Lyu and H. Farid, Detecting hidden messages using high-order statistics and support vector machines, 5th international workshop on Information Hiding, Noordwijkerhout, The Netherlands, 2002.

[21] Y. Fu, R. Shen and H. Lu, Optimal watermark detection based on support vector machines, Proc. of International Symposium on Neural Networks, Dalian, China, August 19-21, 2004, pp.552-557.

[22] P.T. Yu, H.H. Tsai, J.S. Lin, Digital watermarking based on neural networks for color images, Signal Processing, Elsevier Science, 81, 663-671, 2001.

[23] S. Pereira, S. Voloshynovskiy, and T. Pun, Optimal transform domain watermark embedding via linear programming, Signal Processing, Elsevier Science, vol. 81, no. 6, June 2001, pp 1251-1260.

[24] W. Banzhaf, P. Nordin, R.E. Keller, and F.D. Francone, "Genetic Programming: An Introduction," *Morgan Kaufmann Publishers*, CA, 1998.

[25] D. E. Goldberg, Genetic algorithm in search, optimization, and machine learning, Reading, MA: Addison-Wesley, 1992.

[26] T. Loveard, "Genetic Programming for Classification Learning Problems", PhD Thesis, Royal Melbourne Institute of Technology, Australia, 2003.

[27] J. R. Koza, M. A. Keane, M. J. Streeter, M. Mydlowec, J. Yu, G. Lanza, Genetic Programming IV: Routine Human-Competitive Machine Intelligence, Springer Science+Buisness Media, Inc., 2005.

[28] S. Gustafon, "An Analysis of Diversity in Genetic Programming", PhD Thesis, University of Nottingham, UK, 2004.

[29] M. Barni, and F. Bartolini, Watermarking systems engineering: Enabling digital assets security and other application, Marcel Dekker, Inc. New York, 2004.

[30] W. B. Langdon and S. J. Barrett, Genetic Programming in Data Mining for Drug Discovery, Chapter 10 in Evolutionary Computing in Data Mining, Ashish Ghosh and Lakhmi C. Jain editors, Physica Verlag, 2004, pp. 211-235.

[31] M. Barni, F. Bartoline, V. cappellini and A. Piva, "A DCT domain system for Robust Image Watermarking," Technical report, department *di Ingegneria Ellettronica, Universitia Firenze*, 3, 50139 Firenze, Italy, 2001.

[32] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "A Secure, robust watermark for multimedia," Workshop on Information Hiding, Newton Institute, *Univ. of Cambridge*, May 1996.

[33] F. Bartolini, M. Barni, V. Cappellini and A. Piva, "Mask building for perceptually hiding frequency embedded watermarks," Proceeding of *5th IEEE international Conference on image Processing, ICIP'98,* Chicago, Illinois, USA, Oct. 4-7 1998, vol. 1, pp.450-454.

[34] F. M. Boland, J. J. K. O. Ruanaidh and C. Dautzenberg, "Watermarking digital images for copyright protection," Proc. *IEEE*

Conference on Image Processing and Its Applications, July 1995, pp. 326-331.

[35] Huang and Wu, A watermark optimization technique based on genetic algorithm, *Proc. SPIE, Visual Comm. Image*, Feb. 2003.

[36] A. N. Netravali and B. G. Haskell, "Visual psychophysics," In Digital Pictures: Representation and Compression, chapter 4. *Plenum Press, New York*, 1988.

[37] A. B. Watson, R. Borthwick and M. Taylor, "Image quality and entropy masking," *International Society for Optical Engineering, San Jose, California*, U.S.A., 1997, Vol. 3016, pp. 1-8.

[38] M. J. Nadenau, "Integration of human color vision models into high quality image compression," Ph.D. thesis, Signal Processing Laboratory, *Swiss Federal Institute of Technology*, Lausanne, Nov. 2000.

[39] J. O. Limb, "Distortion criteria of the human viewer," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 9, pp. 778-793, No.12, Dec. 1979.

[40] F. I. Koprulu, "Application to low-density parity-check codes to watermark channels," Ms. thesis, Electrical and Electronics Bogaziei University, Turkey, 2001.

[41] W. B. Langdon and B. F. Buxton., "Genetic programming for combining classifiers," In GECCO'2001, Morgan Kaufmann.

[42] H. Kahlman, and M. Hollich, "Genetic programming in C/C++," http://www.cis.upenn.edu/~hollick/genetic/papaer2.html.

[43] The Math Works, 2003.
http://www.mathworks.com./product/matlab

[44] B. S. Kim, J. G. Choi, C. H. Park, J. U. Won, D. M. Kwak, S. K. Oh, C. R. Koh, and K. H. Park, " Robust digital image watermarking method against geometrical attacks," *Real-Time Imaging , Elsevier Science*, vol. 9, pp. 139-149, 2003.

[45] S. Katzenbeisser, Information Hiding, Boston, London, Artech House, 2000.

[46] I. J. Cox and M. L. Miller, Electronic watermarking: The first 50 years, Int. Workshop on Multimedia Signal Processing, IEEE Proceedings, 2001.

[47] J. F. Delaigle, C. De Vleeschouwer and B. Macq, Watermarking algorithm based on a human visual model, Signal Processing, European Association for Signal Processing (EURASIP), 66(3), (1998), 319-335.

[48] J. A. Solomon, A. B. Watson, and A. J. Ahumada, Visibility of DCT basis functions: Effects of contrast masking, in Proc. Data Compression Conf., Snowbird, UT, 1994, pp. 361–370.

[49] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, Perceptual Watermarks for Digital Images and Video, Proc. of the IEEE, 87 (7), (1999), 1108-1126.

[50] M. Kutter and S. Winkler. A Vision-based Masking Model for Spread-Spectrum Image watermarking. IEEE Trans. on Image processing, 11(1), 2002, pp. 16-25.

[51] Christian J. van den Branden Lambrecht and Joyce E. Farrell, Perceptual Quality Metric for digitally coded color images,Proc. EUSIPCO, 1996, pp. 1175-1178.

[52] Z. Wang, A. C. Bovik H. R. Sheikh, Image quality assessment: From error measurement to structure similarity, IEEE Trans. on image Processing, 13(1), 2004.

[53] http://gplab.sourceforge.net

[54] Sara Silva, Jonas Almeida, Dynamic Maximum Tree Depth - A Simple Technique for Avoiding Bloat in Tree-Based GP, in Proc. of the Genetic and Evolutionary Computation Conference (GECCO-2003), Chicago, Illinois, USA, July-2003, pp. 1776-1787.

[55] P. Nordin, M. Brameier, F. Hoffmann, F. Francone, and W. Banzhaf, AIM-GP and Parallelism, Proceedings of Congress on Evolutionary Computation, Washington, 1999, IEEE Press, Piscataway, NJ, pp. 1059-1066.

[56] W. Kantschik and W. Banzhaf, Linear-Graph GP—A new GP Structure, EuroGP 2002, Kinsale, Ireland, Springer LNCS 2278, Berlin, 2002, pp. 83-92.

[57] A. Sequeira, D. Kundur, Communication and Information Theory in Watermarking: A Survey, Multimedia Systems and Applications IV, A. G. Tescher, B. Vasudev, and V. M. Bove, eds., Proc. SPIE (vol. 4518), pp. 216-227, Denver, Colorado, August 2001.

[58] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, Attack modeling: towards a second generation watermarking benchmark, Signal Processing, 81**,** 6, pp. 1177-1214, June 2001. Special Issue: Information Theoretic Issues in Digital Watermarking, 2001. V. Cappellini, M. Barni, F. Bartolini, Eds.

[59] M. Kutter and F. A. P. Petitcolas, A fair benchmark for image watermarking systems, Electronic Imaging '99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA, the International Society for Optical Engineering, Jan. 1999, pp. 25-27.

[60] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers and J. K. Su, Attacks on Digital Watermarks: Classification, Estimation Based Attacks, and Benchmarks, IEEE Commun. Mag. 39 (8) (2001) 118-126.

[61] F. Hartung, J. K. Su and B. Girod. Spread Spectrum Watermarking: Malicious Attacks and Counterattacks, in Proc. SPIE, Security & Watermarking Multimedia Contents, vol. 3657, San Jose, CA, Jan. 1999, pp. 147-158.

[62] Bum-Soo Kim, Jae-Gark Choi, Chul-Hyun Park et al., Robust digital image watermarking method against geometrical attacks, Real-Time Imaging, 9 (2003), 139-149.

[63] E. Praun, H. Hoppe and A. Finkelstein, Robust Mesh Watermarking,. Proceedings of SIGGRAPH 1999, Computer Graphics Proceedings, Annual Conference Series, ACM, pp.49-56.

[64] J.J.K. O'Ruanaidh, W.J. Dowling, F.M. Boland, Phase Watermarking of Digital Image, Proc. IEEE Int. Conf. on Image Processing, Vol. 3, Lausanne, Switzerland, 1996, pp. 239-242.

[65] T. Liang and J.J. Rodriguez. Robust Watermarking Using Robust Coefficients, Security and Watermarking Multimedia Contents II, SPIE,3971, 2000, pp. 326-335.

[66] C. Fei, D. Kundur and R. H. Kwong, Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression, IEEE Trans. on Image Processing, vol. 13, No. 2, 2004, pp.126-144.

[67] G. Brown, J. Wyatt, R. Harris and X. Yao, Diversity Creation Methods: A Survey and Categorization, Journal Information Fusion 6, 2005, 5-20.

[68] Mengjie Zhang, William D. Smart, Multiclass Object Classification Using Genetic Programming. EvoWorkshops 2004, pp. 369-378.

[69] N. Cvejic, D. Tujkovic and T. Seppänen, Increasing robustness of an audio watermark using turbo codes. Proc. IEEE International Conference on Multimedia & Expo, Baltimore, MD, 2003, pp.1217-1220.