IMAGE WATERMARKING OPTIMIZATION ALGORITHMS IN TRANSFORM DOMAINS AND FEATURE REGIONS

HAI TAO

Thesis submitted in fulfilment of the requirements of the award of the degree of Doctor of Philosophy (Computer Science)

Faculty of Computer Systems and Software Engineering
UNIVERSITI MALAYSIA PAHANG

April 2012

ABSTRACT

Digital watermarking techniques have been explored considerably since its first appearance in the 1990s. The achieved tradeoffs from these techniques between imperceptibility and robustness are controversial. To solve this problem, this study proposes the application of artificial intelligent techniques into digital watermarking by using discrete wavelet transform (DWT) and singular value decomposition (SVD). To protect the copyright information of digital images, the original image is decomposed according to two-dimensional discrete wavelet transform. Subsequently the preprocessed watermark with an affined scrambling transform is embedded into the vertical subband (HL_m) coefficients in wavelet domain without compromising the quality of the image. The scaling factors are trained with the assistance of Particle Swarm Optimization (PSO). A new algorithmic framework is used to forecast feasibility of hypothesized watermarked images. In addition, the novelty is to associate the Hybrid Particle Swarm Optimization (HPSO), instead of a single optimization, as a model with SVD. To embed and extract the watermark, the singular values of the blocked host image are modified according to the watermark and scaling factors. A series of training patterns are constructed by employing between two images. Moreover, the work takes accomplishing maximum robustness and transparency into consideration. HPSO method is used to estimate the multiple parameters involved in the model. Unfortunately, watermark resistance to geometric attacks is the most challenge work in traditional digital image watermarking techniques which causes incorrect watermark detection and extraction. Recently, the strategy of researchers has introduced image watermarking techniques using the invariant transforms for their rotation and scale invariant properties. However, it suffers from local transformations which make watermarks difficult to recover. This thesis will introduce a set of content based image watermarking schemes which can resist both local geometric attacks and traditional signal processing attacks simultaneously. These schemes follow a uniform framework, which is based on the detection of feature points which are commonly invariant to Rotation, Scaling and Translation (RST), therefore they naturally accommodate the framework of geometrically robust image watermarking. As a result, it will first introduce the theories about the feature extraction and the basic principles on how feature points can act as locating resynchronization between watermark insertion and extraction discussed in detail. Subsequently, it will present several content-based watermark embedding and extraction methods which can be directly implemented based on the synchronization scheme. Further detailed watermarking schemes which combine feature regions extraction with counter propagation neural network-based watermarks synapses memorization are then presented. The performance of watermarking schemes based on framework of feature point shows the following advantages: (a) Good imperceptibility. It is obvious that the watermarking schemes show a little influence on watermark invisibility; (b) Good robustness. The proposed scheme is not only robust against common image processing operations as sharpening, noise adding, and JPEG compression etc, but also robust against the desynchronization attacks such as rotation, translation, scaling, row or column removal, cropping, and local random bend etc.

ABSTRAK

Teknik *watermarking* digital telah diterokai sejak kemunculan pertamanya pada tahun 1990-an. Pengimbangan yang dicapai ini menjadi kontroversi antara kebolehlihatan dan keteguhan teknik-teknik tersebut. Untuk menyelesaikan masalah ini, kajian ini mencadangkan teknik kepintaran buatan ke dalam *watermarking* digital dengan menggunakan diskret koncah mengubah (DWT) dan penguraian nilai singular (SVD). Untuk melindungi maklumat hak cipta imej digital, imej asal terurai mengikut koncah diskret mengubah dua dimensi. Seterusnya pra proses watermarking dengan mengubah affined rawak yang tertanam di dalam subband menegak (HL_m) pekali dalam domain ombak kecil tanpa menjejaskan kualiti imej. Faktor-faktor scaling dilatih dengan bantuan *Particle Swarm Optimization* (PSO). Satu rangka kerja algoritma baru digunakan untuk meramal kemungkinan imej hipotesis watermarking. Di samping itu, pembaharuan ini adalah untuk mengaitkan *Hybrid Particle Swarm Optimization* (HPSO), dan bukannya pengoptimuman satu, sebagai satu model dengan SVD. Untuk menerapkan dan cabutan watermarking, nilai-nilai tunggal imej tuan rumah yang telah disekat telah diubah suai mengikut watermarking dan faktor-faktor penskalaan. Satu siri corak latihan yang dibina dengan menggunakan antara dua imej. Selain itu, penyelidikan ini mencapai tahap keteguhan maksimum dan kebolehlihatan. Kaedah HPSO digunakan untuk menganggar parameter berbilang yang terlibat dalam model. Malangnya, rintangan *watermarking* yang berupa serangan geometri di dalam teknik tradisional *watermarking* imej digital yang menyebabkan pengesanan dan pengestrakan *watermarking* salah. Strategi penyelidik semasa telah memperkenalkan teknik imej *watermarking* yang menggunakan perubahan yang tidak berubah kepada ciri-ciri putaran dan skala tak berubah. Walau bagaimanapun, ia mengalami transformasi tempatan yang membuatkan watermarking susah untuk pulih. Tesis ini akan memperkenalkan satu set imej kandungan berasaskan skim watermarking yang boleh melawan kedua-dua serangan geometri dan serangan pemprosesan isyarat tradisional secara serentak. Skim ini mengikut satu rangka kerja yang seragam, yang berasaskan pengesanan ciri-ciri penting dimana kebiasaannya tidak membawa perubahan kepada putaran, penskalaan dan penterjemahan, maka mereka secara semulajadi akan menampung rangka kerja geometri watermarking imej teguh. Oleh itu, ia akan memperkenalkan teori-teori tentang pengekstrakan ciri dan prinsip-prinsip asas bagaimana ciri-ciri penting boleh bertindak sebagai penempatan penyelarasan semula antara penyisipan dan pengekstrakan watermarking dibincangkan secara terperinci. Kemudian, ia akan menghuraikan beberapa kaedah pembenaman dan pengekstrakan watermarking muatan asas yang boleh terus dilaksanakan berdasarkan skim penyelarasan. penerangan selanjutnya mengenai skim watermarking yang menggabungkan pengekstrakan ciri kawasan dengan rangkaian neural perambatan kaunter berasaskan watermarking sinaps hafalan kemudiannya dibentangkan. Prestasi skim watermarking yang berdasarkan rngka kerja ciri penting menunjukkan kelebihan berikut: (a) Baik dalam keadaan tidak ketara. Ia jelas bahawa bahawa skim watermarking menunjukkan pengaruh yang kecil ke atas keadaan tidak ketara watermarking; (b) Keteguhan yang baik. Skim yang dicadangkan bukan sajaha teguh terhadap operasi pemprosessan imej biasa sebagai penajam, penambahan bunyi bising, pemampatan JPEG dan sebagainya, tetapi juga teguh terhadap serangan penyelarasan semula seperti putaran, penterjemahan, penskalaan, penyingkiran lajur dan baris, pemotongan, pembengkokkan rawak tempatan dan lain-lain.

TABLE OF CONTENTS

CHAPTER 3 METHODOLOGIES

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

X	Input Training Vectors $X=(X_1, X_{2,\ldots} X_n)$
Y	Input Training Watermarks $Y= (Y_1, Y_{2,\ldots} Y_m)$
D	Neuron Vectors Of The Kohonen Layer $D=(D_1, D_{2,\ldots} D_l)$
W	Weight Interconnecting Between X Input Layer To Neuron Unit D_i $W=(W_{1i}, W_{2i,\ldots} W_{ni})$
V	Weight Interconnecting Between Y Input Layer To Neuron Unit D_i $V=(V_{1i}, V_{2i,\ldots} V_{mi})$
X^*	Output Vectors In The Grossberg Layer $X=(X_1, X_{2,\ldots} X_n)$
Y^*	Output Watermarks In The Grossberg Layer $Y= (Y_1, Y_{2,\ldots} Y_m)$
T	Weight Interconnecting Between Host Image X Output Layer To Ith Neuron Unit D_i $T=(T_{1i}, T_{2i,\ldots} T_{ni})$
U	Weight Interconnecting Between Watermark Y Output Layer To Ith Neuron Unit D_i $U=(U_{1i}, U_{2i,\ldots} U_{mi})$
$\alpha(k)$	Learning Parameters During Kohonen Learning
$\beta(k)$	Learning Parameters During Grossberg Learning

LIST OF ABBREVIATIONS

ACR	Affine circular regions
BCD	Binary Coded Decimal
CR	Cirque regions
LCR	Local circular regions
LoG	Laplacian-of- Gaussians
NFC	Near field communication
SR	Subregions
PDA	Personal digital assistant
DVD	Digital Versatile Disc
SVD	Singular Value Decomposition
DWT	Discrete Wavelet Transform
PNN	Probabilistic Neural Network
AI	Artificial Intelligence
NC	Normalized Correlation
UQI	Universal Quality Index
DCT	Discrete Cosine Transform

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Due to the rapid and comprehensive development of network technologies, digital multimedia contents can be delivered with maintained good quality, almost immediate transmission protection and low price of multimedia contents has recently developed into a significant problem because of purchaser's insufficient recognition of the possession of intellectual property. Therefore, over the past a couple of decades, digital multimedia technology has turned up to search for responses to the question: can researchers ensure tamper-resistance and protect the copyright of digital contents by processing, communicating and storing digital information encoded in procedures where digital media content be able to effortlessly be distributed through communication channels? Today it is fully apprehended that the answer is positive, and numerous researchers all over the world are studying towards the considerably progressive technical target of protecting the ownership of digital contents. The efforts would dramatically protect inventions represented in digital form for being vulnerable to illegal possession, duplication and dissemination. Digital watermarking (Cox I.J., et.al. 1997) is the process of embedding or hiding digital information called watermark into a multimedia product, and then the embedded data can later be extracted or detected from the watermarked product. The technique can protect digital content copyright and ensure tamper-resistance, which is indiscernible and hard to remove by unauthorized persons.

Up to now, two traditionally-used strategies, spatial-domain (Takahashi A., et al. 2005) and transform domain (Kim T.Y., et al. 2004) techniques have been developed for digital image watermarking. The former category is designed to insert directly a watermark into the original image by a factor, which would lead to fair-quality watermarked images. The latter approach, for taking advantage of perceptual properties, is devised to embed a watermark into transform domains of the original images. The types watermarking schemes have good performances of robustness to the most common signal processing manipulations such as JPEG compression, filtering, and addition of noise (Cox I.J., et al. 1997; Cox I.J., et al. 2001; Lu C.S., et al. 2000). The common image processing operators are applied to watermarked images for removing the watermark or decreasing its energy, and the result is that the extracted watermark is unrecognizable or insufficient as the validate evidence.

Unfortunately, the ineffectiveness of existing traditional watermarking algorithms is described by the robustness against unintentional or malicious geometric attacks (Licks V. and Jordan R., 2005). Especially, geometrical attacks cause synchronization errors between the original watermark and the extracted one through the extraction procedure. In other words, the watermark still includes in watermarked images, but its positions have been changed. Therefore, traditional watermarking systems need to be extended for the resilience to watermarked data geometrical modifications. In the developed frameworks, synchronization errors correction is now possible. Besides facilitating more efficient copyrighted protection and robustness against common image processing operators and desynchronization attacks, adaptation of geometrically invariant image features can potentially offer a greater robust capacity to detect watermarks without synchronization errors, especially when applied to survive local distortions such as Random bending attacks. The development of such framework is an essential starting point for organizations that wish to improve, or replace currently existing watermarking algorithms based pixels, frequency or other transform coefficients for watermarks embedding and to develop a set of means to establish and maintain feature-based watermarking of geometric distortions correction.

1.2 DEFINITION OF WATERMARKING

A great number of multimedia information is now being generated, distributed and stored with digital forms, Newspapers, and magazines. For example, these have published online to provide real-time coverage of stories with high-quality audio, still images, and even video sequences. The explosive accretion in using public networks such as the Internet has further encouraged the online presence of publishers by providing an inexpensive and quick way to distribute their work. However, the great growth of digital media is not limited to news organizations. Commercial music may be downloaded off of the Internet and purchased, stock photography vendors digitize and sell photographs in electronic form, and Digital Versatile Disc (DVD) systems provide movies with clear images and CD-quality sound. Unfortunately, media stored in digital form are vulnerable in a number of ways. First of all, digital media may be redistributed and copied simply, either legally or illegally, at low cost and with no loss of information. In addition, today's fast computers allow digital media to be easily manipulated, so it is possible to incorporate portions of a digital signal into one's own work without regard for copyright restrictions placed upon the work.

Digital watermarking is considered as a partial solution to the problem of protecting copyright ownership. Essentially, watermarking is defined as the process of embedding sideband data directly into the samples of a digital audio, image, or video signal. Sideband data is typically “extra” information that must be transmitted along with a digital signal, such as block headers or time synchronization markers. It is important to realize that a watermark is not transmitted in addition to a digital signal, but rather as an indispensable part of the signal samples. The value of watermarking comes from the fact that regular sideband data may be modified or lost when the digital signal is converted between formats, but the samples of the digital signal are typically unchanged.

To elucidate this concept further, it is helpful to consider an analogy between digital watermarks and paper watermarks. Watermarks have traditionally been used as a form of authentication for paper currency and legal documents. A watermark is embedded within the fibers of paper when it is first constructed, and it is essentially invisible unless held up to viewed at a particular angle or a special light. More importantly, a watermark is very difficult to remove without destroying the paper itself, and it is not transferred if the paper is photocopied. The targets of digital watermarking are similar, and it will be shown in the next section that digital watermarks require similar properties.

Before the concept of watermarking can be explored further, three important definitions must first be established. A host signal is a raw digital audio, image, or video signal that will be used to contain a watermark. A watermark itself is loosely defined as a set of data, usually in binary form, that will be stored or transmitted through an original signal. The watermark may be as small as a single bit, or as large as the number of samples in the host signal itself. It may be a copyright notice, a secret message, or any other information. Watermarking is the process of embedding the watermark within the host signal. Finally, a secret key may be necessary to embed a watermark into a host signal, and it may be needed to extract the watermark data afterwards (Cox et al., 1997).

1.3 PROBLEM STATEMENTS

Digital watermarking algorithms are effectively applied to associated broadcast monitoring systems and copy control applications. In combination with digital rights management systems, these techniques can solve the bottleneck of the intellectual property dilemma in audio- and image-related business areas. In an early stage of watermarking, users considered resisting to geometric attacks as an advantage of one technique over alternative implementations. For feature-based watermarking schemes, however, surviving geometric attacks is a precondition. The past 10 years have witnessed a important advancement in people recognizing of geometrical attacks and methods for surviving them. Some approach proposed particular types of attacks, although just a few of watermarking methods, in fact, survived the huge set of potential variations of combined approaches. Even afterwards, many researchers identifying of these threats, which the attacks compel on the performance of existent and upcoming methods are limited. It may just reflect the limitations of efficient benchmarking procedures and theoretical grounds for evaluating them..

(Cox et al. 1997) proposed a spread spectrum watermarking scheme based on discrete cosine transform (DCT). The scheme aims to hide Gaussian distributed noise-style watermarks. But these noisy style watermarks may not offer any resistance for compressing the image data or for low-pass filtering attacks. (Lee et al. 2006) presented a Genetic Algorithm-Based watermarking algorithm in the discrete wavelet transform domain. Wavelet-domain low-frequency region watermark insertion and genetic algorithm-based watermark extraction are possible in the algorithm. However, the major deficiency is the higher degree of visual distortion which is similar to the results shown in (Hisashi I., 2000). Additionally, GA suffers from important limitations of high computational costs which eventually results in low convergence speed. (Ziqiang et al., 2007) integrated DWT with particle swarm optimization (PSO) for watermarking digital images. The technique embeds watermark into coefficients of DMT that holds value larger than some threshold value. Subsequently the extraction is performed through PSO. However, an obvious limitation of their proposed method is that the application of PSO was simply done for evaluating the feasibility of the extracted watermarks.

Additionally, (Chung et al. 2007) gave a guideline to embed the watermark into both U and V components of the images using SVD. However, it was important to mention that the previously cited watermarking schemes based on singular vectors cannot preserve the orthgonalization of the U and V matrices. (Aslantas V 2008, 2009) presented two optimized watermarking scheme using genetic algorithm (GA) and differential evolution algorithm to obtain multiple scaling factors for embedding watermark based on SVD-based watermarking method of (Liu and Tan, 2002). However, (Zhang and Li 2005) noted that the watermarking algorithm was fundamentally flawed in that the extracted watermark was not the embedded one but decided by the reference watermark. The reference watermark generated the pair of SVD matrices used in the watermark detector. In the watermark detection process, the fact that the exploited SVD matrices relied on the reference watermark biased the false positive detection rate such that it had a probability of one. Therefore, any reference watermark that is being explored in an arbitrary image can be detected. However, less research work has been reported so far on the corrected optimal SVD-based image watermarking scheme.

Furthermore, while the common image processing operations reduce watermark energy, desynchronization attacks induce synchronization errors between the original and the extracted watermark during the detection process. Most of the previous watermarking schemes are robust to common image processing operations, but show severe problems to de-synchronization attacks. Today, most watermarking methods cannot reach the main approach which is efficiently insensitive to various attacks. It is still a wide and attractive field for further research in which innovative methods and techniques may be established. In this thesis, it propose geometrically invariant digital image watermarking approaches to construct watermark synchronization using neural networks and local feature detectors to achieve its goals.

Watermark resistance to geometric attacks is the most challenge work in traditional digital image watermarking techniques which causes incorrect watermark detection and extraction. Recently, the strategy of researchers has introduced image watermarking techniques using the invariant transforms for their rotation and scale invariant properties. However, it suffers from local transformations which make watermarks difficult to recover. For solving these problems, researchers proposed a series of feature-based geometrically invariant watermarking algorithms simplifying to synchronization deformation. Basically, any given watermarking system should be able to have good performance of robustness, fidelity and data payload. Robustness ensures that the retriever is still able to extract the watermark information even if the watermarked image is deformed by various attacks. Fidelity deals with whether a watermark was inappropriately embedded according to the perceptual between the original and watermarked image. Finally, payload refers to the amount of efficient bits that can be embedded in original images and retrieved reliably under normal operations.

1.4 RESEARCH OBJECTIVES

To acquire accomplishing maximum robustness and transparency into consideration in transform domain.

To obtain the highest possible level of robustness while maintain the perceptual transparency in feature regions.

1.5 RESEARCH CONTRIBUTIONS

This work provides the following set of original contributions:

In transform domain, the corrected SVD-based optimal watermarking technique is proposed for ownership protection based on hybrid particle swarm optimization (HPSO). Experimental results show both the significant improvement in transparency and the robustness under attacks. Simulation results demonstrate that the proposed scheme can effectively improve the quality of the watermarked image and resist to common image manipulations such as adding noise, resizing compression, tempering, etc. and some geometric attacks.

In addition, the algorithm is devoted to introduce a novel algorithmic framework for solving an optimal embedding and extracting problem in DWT domain. In the proposed technique, the retrieval of watermark is distinguished with three important features: i) it does not depend upon the availability of the original image; ii) it makes an effective use of PSO for parameters estimation; iii) it possesses an appreciative capability for simultaneously optimizing multiple scaling factors for obtaining the highest possible level of robustness while maintaining the perceptual transparency in embedding watermark images.

In feature regions, the algorithm is devoted to propose a novel geometrically invariant watermarking method for solving an optimal embedding and extracting problem using Harris-Laplace operators and counter propagation neural networks. Sufficient experiments demonstrate the better robustness of this approach than others' scheme in the same level of imperceptibility, especially in resisting geometry attacks and combined attacks.

In addition, the second method first proposes a geometrically invariant digital image watermarking technique to construct watermark synchronization using synapses memorization and affine covariant region. The comparison of the presented approach with previous algorithms in terms of robustness and imperceptibility is also provided.

The experimental results show that the proposed scheme has the remarkable performance in resistant to common image processing operations survival the desynchronization attacks.

Finally, to design gray-level watermark extraction scheme against desynchronization attacks, the third method proposed a novel geometrically invariant watermarking scheme based on grouping Harris-Laplace detector and the counter propagation neural network with low computational complexity, good visual quality and reasonable resistance toward desynchronization attacks. In the simulation results, it demonstrates that the proposed image watermarking is not only imperceptibility and robust against common image processing operations such as sharpening, noise adding, and JPEG compression etc, but also robust against the geometric distortions such as rotation, translation, scaling, row or column removal, cropping, and local random bend etc.

1.6 SCOPE OF THE THESIS

To devoted to introduce a novel algorithmic framework for solving an optimal embedding and extracting problem. The optimal algorithm achieves this by using a forecasted feasibility for parameters evaluation in DWT domain.

To correct and propose SVD-based optimal watermarking technique for ownership protection based on hybrid particle swarm optimization (HPSO). The singular values of the host image are modified by embedding the watermark into the blocked host images according to employing multiple scaling factors. The HPSO, individuals and new generation are created, not only by crossover and mutation operators as in GA, but also by PSO.

To develop a feature-based watermarking framework for attempting to reacquire synchronization, allowing for complicated tradeoff between the three aforementioned properties. To do so, the next part first investigates and develops feature selection procedures which can be employed as a set of nonoverlapped and stable regions within the framework including: Harris–Laplace detector and affine covariant region detectors and other improved feature detectors. Specifically, the counter propagation neural network is applied to watermarks detection and extraction. It is not so much a new discovery as it is a novel combination of previously existing network types. Hecht-Nielsen synthesized the architecture from a combination of a structure known as a competitive network and Grossberg structure. The operation of the network is quite straightforward. The existence of a reset mechanism will remove the current input pattern if another is stored. And this storage effect appears to be permanent. This long-term memory behavior applies the efficient evidence for extracting watermarks from seriously distorted watermarking images. And it handles low computational complexity, good visual quality and reasonable resistance toward desynchronization attacks, in particular the issues of bit error probability.

1.7 THESIS ORGANIZATION

The remainder of this dissertation is organized as follows. Chapter 2 provides a summary of related work regarding the typical framework of image watermarking, characteristics, applications and attacked techniques of watermarking systems, and existing geometrically invariant watermarking. Chapter 3 describes specific methodologies in the areas of transform domains images feature selection and artificial intelligent techniques. Chapter 4 presented an optimal robust image watermarking technique based on Discrete Wavelet Transform (DWT), and presents a novel optimal robust image watermarking technique based on HPSO which is robust against a variety of common image-processing attacks and some geometric attacks. Chapter 5 provides three algorithms which the watermarks are embedded in the synapses of counter propagation Neural Network. Experiments demonstrates that the proposed image watermarking framework is not only imperceptibility and robust against common image processing operations such as sharpening, noise adding, and JPEG compression etc, but also robust against the geometric distortions such as rotation, translation, scaling, row or column removal, cropping, and local random bend etc. Finally, Chapter 6 concludes the work by providing a summary of the accomplishments as well as future directions for research.

CHAPTER 2

BACKGROUNDS AND LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter reviews the appropriate background literature and describes the concept of watermarking, characteristics of watermarking systems, the classification of digital watermarking applications and attacked operators. Scientific publications included into the literature survey have been chosen in order to build a sufficient background that would help out in solving the research problems stated in Chapter 1. In addition, Chapter 2 presents general concepts and definitions used and developed in more details in Chapters 3, 4 and 5. The thesis is decided to divide the feature point theoretical background, methodologies and experiments into three parts, presented in Chapters 3, 4 and 5 because of the specific structure of the thesis, which presents three different algorithms for geometric invariant image watermarking, contrary to the usual schemes with the valued-added cover images in the special regions. Therefore, the theoretical background and literature review in subjunction to the particular concept is given as a separate chapter in the respective chapters. In this manner, it much easier for the reader to follow the presented concepts, and the chapters themselves can also be read as standalone readings.

In the first section, the properties of the general watermarking frameworks that are exploited in the process of encoding and detecting watermarking are shortly reviewed. A survey of the key digital image watermarking algorithms and techniques is presented subsequently. The characteristics of watermarking systems are described for evaluating the performance of watermarking systems. There are five important issues that are usually considered in the most practical application; they are highlighted in the following subsections. In addition, digital watermarking is described as an efficient method for the protection of ownership rights of digital audio, image, video and other data types. It can be applied to different applications including digital signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control, and secret communication. Watermarking attacks can be classified into two broad categories: destruction attacks: including image compression, image cropping, spatial filtering, etc., and synchronization attacks: including image rotation, image shifting and pixelhine deletion. The chapter lists and describes some of these conventional attacks in the following sections.

For constructing geometric invariant watermarking, four mainstream schemes are introduced by literature reviews on watermarking algorithms robust to the geometrical distortions. Most of these efforts confine to theoretically analyzing and quantifying the effect of the global and local affine transform to the performance of the watermarking algorithms.

2.2 HISTORY OF WATERMARKING

The thought to communicate secretly is as ancient as communication itself. First stories appeared in the old Greek literature, which can be explained as early records of covert communication, for example, in Homer's Iliad, or in tales by Herodotus. The word "steganography," which is still used until today, derives from the Greek language and means covert communication. In (Kobayashi M., 1997; Petitcolas F.A.P., et al.1999), they have investigated the historical facts of covert communication in detail, including the broad use of methods for covert and secret communication before and during the two World Wars, and steganographic methods for analog signals. Although the historical background is very interesting, this part does not cover it here in detail. Please refer to (Kobayashi M., 1997; Petitcolas F.A.P., et al.1999) for an in-depth inquisition of historic aspects.

Paper watermarks arose in the art of handmade papermaking about 700 years ago. The oldest watermarked paper discovered in archives dates back to 1292 and has its origin in Fabriano, Italy, which is considered the birthplace of watermarks. At the