"PERCEPTUAL WATERMARKING FOR DIGITAL IMAGES USING 2-LEVEL DISCRETE WAVELET TRANSFORM"

Name of Student: Akshay Sachdeva(071048)

Rishabh Sinha (071159)

Vikrant Rana(071014)

Name of supervisor: Prof. Tapan Kumar Jain

May, 2011

Submitted in partial fulfillment of the Degree of Bachelor of Technology

DEPARTMENT OF ELECTRONICS and COMMUNICATION ENGINEERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT

Table Of Contents

LIST OF FIGURES

CERTIFICATE

This is to certify that the work titled **"PERCEPTUAL WATERMARKING FOR DIGITAL IMAGES USING 2-LEVEL DISCRETE WAVELET TRANSFORM"** is submitted by **AKSHAY SACHDEVA , RISHABH SINHA** and **VIKRANT RANA** in partial fulfillment for the award of degree of Bachelor of Technology in Jaypee University of Information Technology, WAKNAGHAT, SOLAN has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor ..... Tapan Jain

Name of Supervisor ..... Tapan Jain

Designation ..... Sr. Lecturer

Date 23.05.2011

ACKNOWLEDGEMENT

I would like to express my sincere thanks to Prof. **Tapan Kumar Jain**, Department of Electronics and Communication Engineering, for his constant encouragement and guidance during this project. His continuous involvement in the progress of my project was of great help to me. He has been a constant source of inspiration and has helped me at each step of the project. I would like to thank him for his valuable suggestions in the project which improved the usefulness of the system as a whole.

The Zeal to accomplish the task of formulating the project could not have been realized without the support and cooperation of the faculty members of ECE Department. We sincerely thank Prof. (Dr.) T. S. Lamba, Dean (A & R) and Prof. (Dr.) Sunil V. Bhooshan HOD (ECE) for their consistent support throughout the project work.

Date: 23/05/2011

Name of the students:

Akshay Sachdeva Akshay ..

Rishabh Sinha Sinha

Vikrant Rana Rana

Summary

In this project we are presenting a watermarking scheme using, the Discrete Wavelet Transform (DWT). In a DWT based scheme, the DWT coefficients are modified with the data that represents the watermark. Along with DWT, we have also used SVD which is one of the most useful tools of linear algebra with several applications in image compression, watermarking and other signal processing fields. After decomposing the cover image into four bands, we have applied the SVD to each band, and embedded the same watermark data by modifying the singular values. Modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks.

CHAPTER 1

INTRODUCTION

1.1 History

The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing can also be found in Kautilya's "Arthashastra". The use of watermarks is almost as old as paper manufacturing. The first paper watermark was used in 1282, in Italy. By the 18th century, watermarks on paper in Europe and America had been used as trademarks, to record the manufactured date, or to indicate the size of original sheets.

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne, in their paper: A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673.

The term used by Tirkel and Osborne was originally used in Japan-- from the Japanese-- "denshi sukashi" -- literally, an "electronic watermark".

The digital watermark is hidden in plain view; hence it is a form of steganography. Functionally, the term "digital watermark" is used to describe that which enables differentiation between copies of the "same" content in an imperceptible manner. Many watermarking systems take this a step further, hiding the data so that attempts at erasure results in degradation of the quality of the content.

1.2 Information hiding techniques

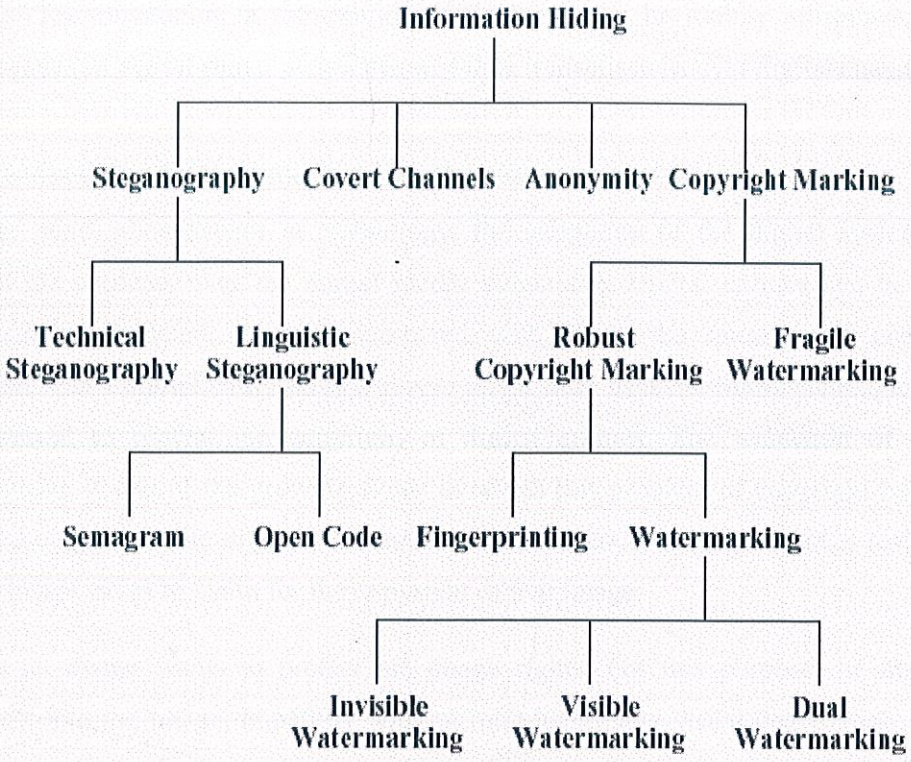


Fig 1.1 Information hiding techniques

1.3 Digital Media – The new face of communication

The world is primarily analog. However, the quality obtained in analog signal processing and transmission is often far from the desired. The Digital domain offers a lot of advantages over the Analog domain. This has leaded us to switch over to the former domain. Thus, digital systems both for signal processing and transmission have gained importance over the past few years. Digitization of real life analog signals requires sampling and quantization. This leads to the loss of some information in the form of quantization error. However, by suitably adjusting the number of quantization levels this error may be limited so as to render undetectable by the human senses, which have a finite resolution capability.

Transmissions over digital channels provide high noise immunity and efficient utilization of channel capacity through multiplexing. Digital systems and channels are highly cost effective. The revolution in information technology may be mainly attributed to the advancements in digital signal processing and data transmissions over digital channels.

1.4 The need for Watermarking in the current scenario

With the rapid advancement in technology, the simplicity of the digital systems has rendered the contents over the digital media vulnerable. Digital entities can be easily duplicated, manipulated, or even tampered with. Thus the question of copyright associated with a digital entity faces a severe threat from hackers. Many techniques have been devised to protect the copyright of digital entities. The technique of digital watermarking is one of the growing fields in which this problem of copyright has been addressed elegantly. The digital watermark is a secret code or image hidden inside the original image, so as to claim for the copyright of that image.

Suppose an owner wants to protect his image rights. For this purpose, he inserts a watermark into the image, hopefully without introducing any visual degradation. When needed, he proves his ownership by retrieving his watermark, despite possible image modifications. It is clear that this type of scenario is based on a robust and invisible signature.

1.5 Digital Watermarking

Digital watermarking is the process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy.

A generalized watermark model consists of watermark encoding and detection processes as shown in Fig. 1.2 and Fig. 1.3. The inputs to the embedding process are the watermark, the cover object and a secret key. The key is used to enforce security and to protect the watermark. The output of the watermarking scheme is the watermarked data. The channel for the watermarked data could be a lossy, noisy, unreliable channel. Thus the received data may be different from the original watermarked data. The inputs for extraction are

the received watermarked data and the key corresponding to the embedding key. The output of the watermark recovery process is the recovered watermark [24, 25].

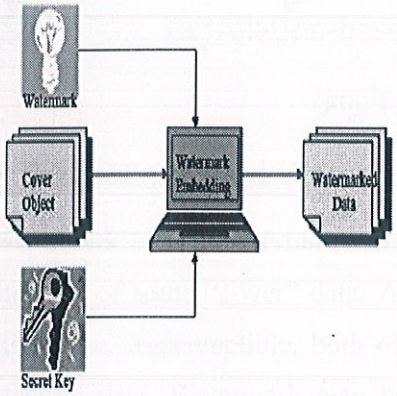


Fig. 1.2 Watermark embedding.

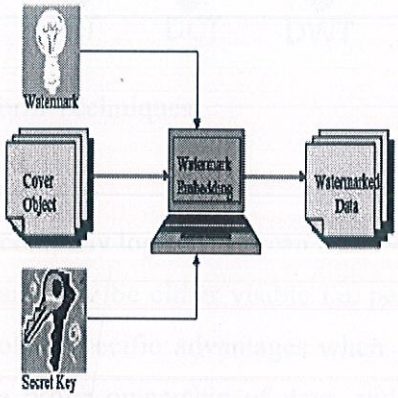


Fig.1.3. Watermark detection.

1.6 Domains Available

Spatial domain: Watermark is embedded using Least Significant Bit (LSB), Statistical, Feature and Block based techniques. Spatial-domain techniques work with the pixel values directly. Generally, spatial domain watermarking is easy to implement from a computational point of view, but too fragile to resist numerous attacks.

Transform domain: Some of the transform based watermarking techniques used the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Singular Value Decomposition (SVD). Transform-domain techniques employ various transforms, either local or global. The wavelet transform is another type of the transform domain. In order to have more promising techniques, researches were directed towards watermarking in the transform domain, where the watermark is not added to the image intensities, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the transform inversely.

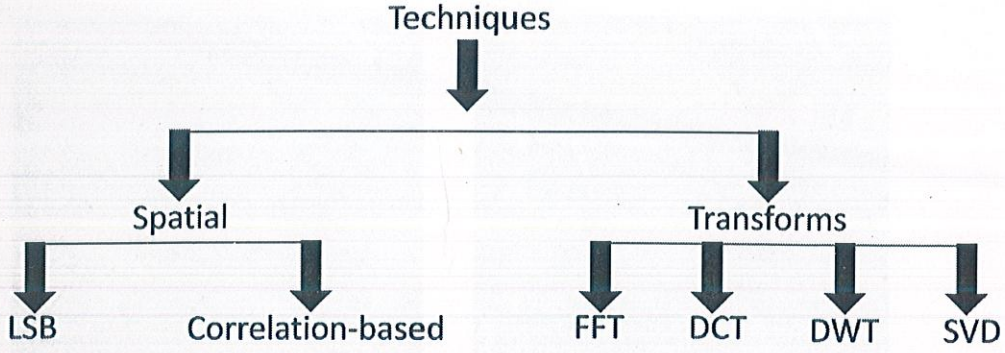


Fig. 1.4 Transform Techniques

1.7 What is a Digital Watermark?

A watermark is an identifying feature, like a company logo, which can be used to provide protection of some "cover" data. A watermark may be either visible i.e. perceptible or invisible i.e. imperceptible, both of which offer specific advantages when it comes to protecting data. Watermark may be used to prove ownership of data, and also as an attempt to enforce copyright restrictions.

Watermarking is the process involved in embedding a watermark into some cover data. The process may take place either in the spatial domain or some transformed domain like the Fourier Domain or Discrete Cosine Domain amongst others. In the case of watermarking in some transform domain our images must be transformed to the domain first and then the watermark embedding is performed and the resulting image gets transformed back to the spatial domain. To provide more robustness to a watermark against attack it is advisable to embed the watermark in some transform domain

a b

Fig:-1.5 showing original (a) and watermark images (b) (invisible)

1.8 Model for a Watermarking System

A generalized watermarking system may be devised in fig1.5. In the Watermark Insertion Block, copyright information is hidden inside the original piece of work in an encrypted form [16].

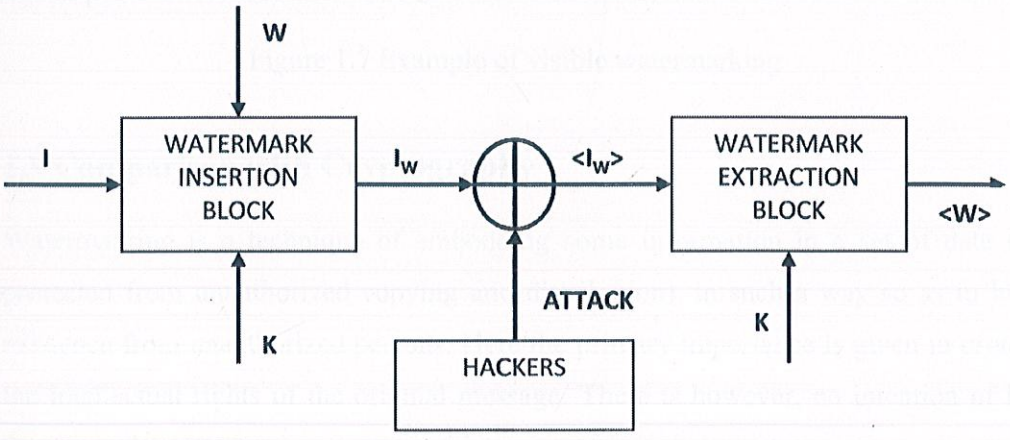


Figure: 1.6 Generalized Model for a WATERMARKING SYSTEM

The original image, I is processed inside this watermark insertion system. The other input to this block is the copyright information or the watermark, W to be embedded inside I using the secret key, K. Thus, the final image available in the market is a composite

image, I_W containing the encrypted logo inside the original image. This composite image available in the market has every possibility of being attacked by the hackers in a bid to destroy the watermark embedded inside it, to generate the hacked version, $<I_W>$ of the composite image. Once the hackers become successful in destroying the watermark the original piece of work becomes susceptible to all kinds of fraud. The primary aim of the Watermarking Extraction Block is to successfully extract an estimate of the copyright information, <W> from the hacked version **$<I_W>$.** The better the watermarking system the more <W> resembles W.

Figure 1.7 Example of visible watermarking

1.9 Comparison with Cryptography

Watermarking is a technique of embedding some information in a set of data (to be protected from unauthorized copying and distribution), in such a way so as to hide its existence from unauthorized persons. Here the primary importance is given in protecting the intellectual rights of the original message. There is however, no intention of hiding the original message

.Cryptography is used to restrict the access to the original message (data) itself by scrambling it with a key before putting it on the digital media. The intended user is having the key to access the data by de-scrambling the encrypted message. So, there is no

additional information stored in the message to claim intellectual property rights. Once such data is decrypted there is no way to track its reproduction or retransmission.

In watermarking the attacks on the original data can be classified as Intentional and unintentional. Unintentional attacks include the common signal processing such as low pass filtering, median filtering, digital to analog and analog to digital conversion, re-sampling and re-quantization, and common geometric distortions such as rotation, translation, cropping and scaling. Intentional attacks include collusion and forgery.

Attacks used by Cryptanalyst are cipher text only, known plain text, chosen cipher text and chosen plain text. In cipher text only attacks, the Cryptanalyst knows the cipher text to be decoded. The cryptanalyst may have decoded message, which together may be used for a known plain text attack. The chosen plain text attack is the most favorable case for the Cryptanalyst. In this case Cryptanalyst has some cipher text, which corresponds to some selected plain text. If the encryption algorithm and the cipher are available the Cryptanalyst encrypts plain text looking for matches in cipher text. This chosen cipher text attack is used to deduce the sender's key. The challenge with cryptography is not in detecting that something has been encrypted, but decoding the encrypted message.

Watermarking is a complement to cryptography but cannot replace it. If the hidden mark is encrypted, it must be decrypted if discovered, which provides another layer of protection.

1.10 Types of Watermarks

1) On the basis of Perceptibility:

- Visible
- Invisible

2) On the basis of Robustness:

- Fragile
- Semi fragile
- Robust

3) On the basis of Inserted Media:

- Text
- Image
- Audio
- Video

4) On the basis of Processing Method:

- Spatial
- Spectral

5) On the basis of Necessary data for Extraction

- Blind
- Informed

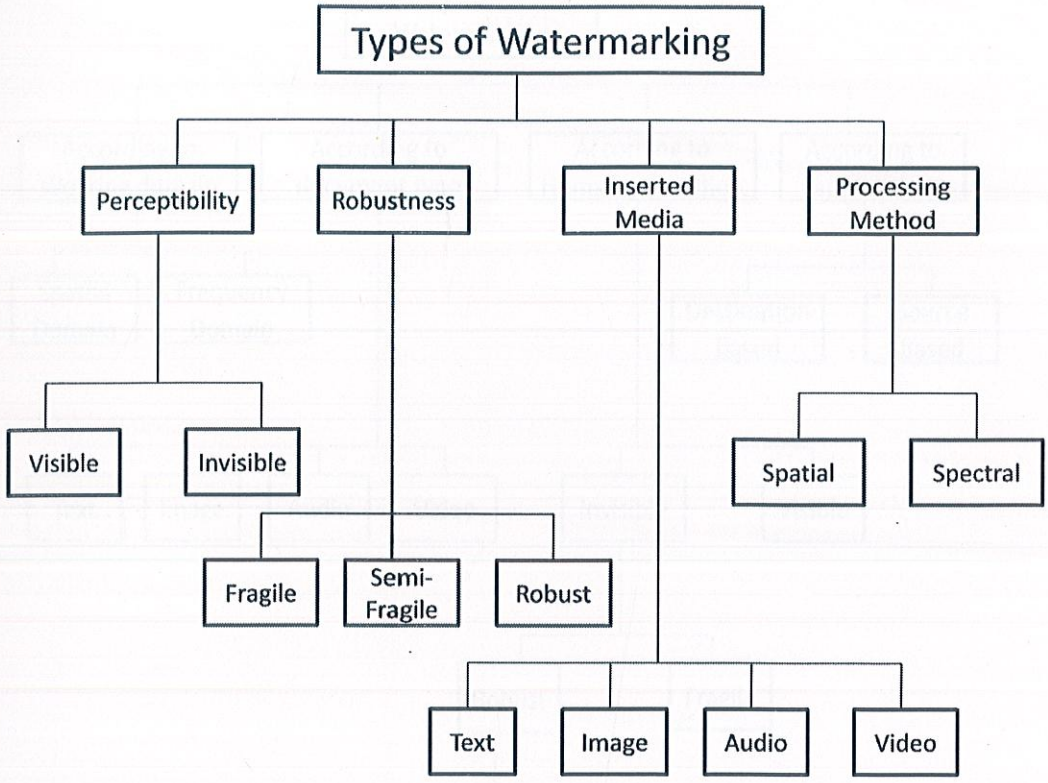


Fig: 1.8 Chart of Types of watermarks

1.11 Digital Watermarking Techniques

Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in spatial domain. An alternative to spatial domain watermarking is frequency domain watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Different types of watermarks are shown in the figure 1.7.

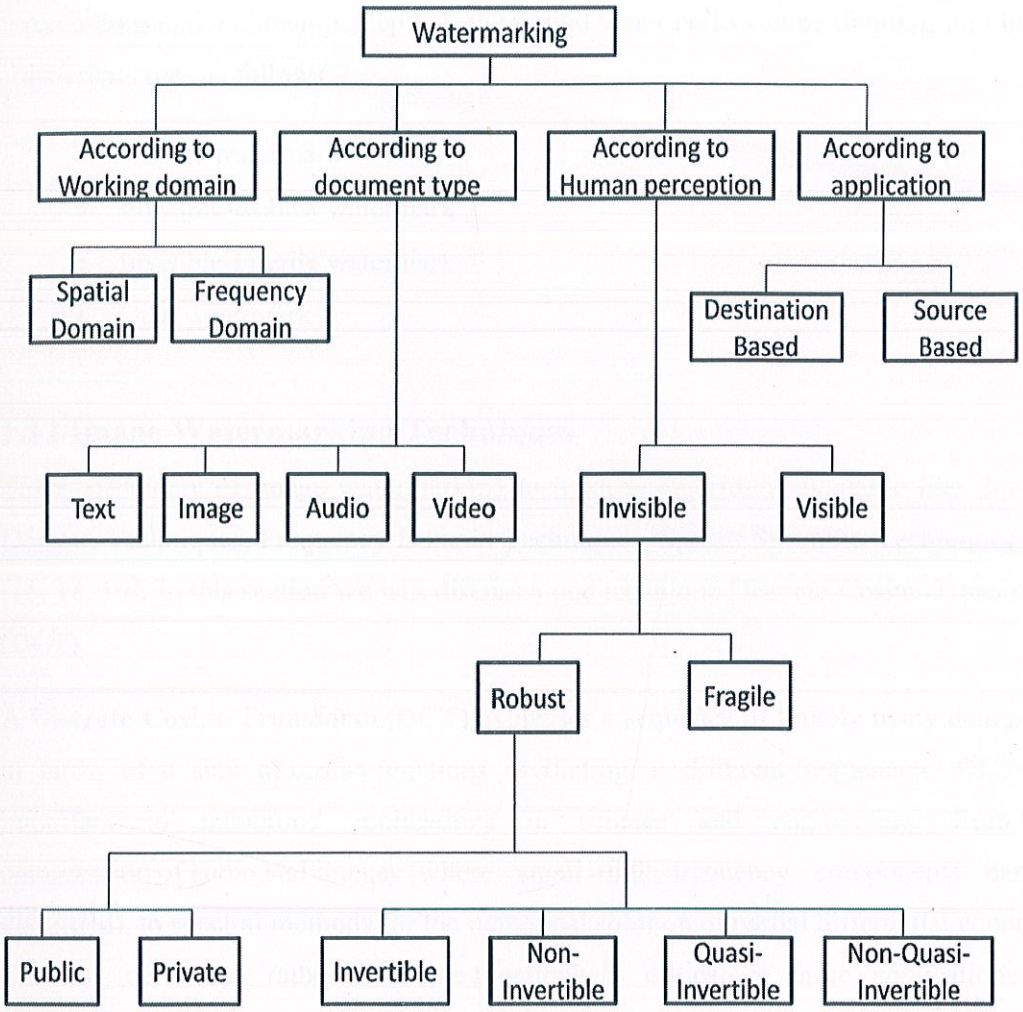


Fig: 1.9 Chart of Watermarking Techniques.

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the human perception, the digital watermarks can be dividing into three different types as follows.

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

1.12 Image Watermarking Techniques

There are plenty of image watermarking techniques algorithms available like Spatial Domain Techniques, Frequency Domain Techniques, Spread Spectrum Techniques etc [15, 18, 19]. In this section we will discuss a one technique Discrete-Cosine-Transform (DCT).

A **Discrete Cosine Transform (DCT)** expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio and images (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as explained below, fewer are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

1.13 Why this project?

Watermarking is a relatively new and unexplored field in which much of research is going on all over the world and it has the potential to provide simple and easily implemental solution to rightful ownership. Most of the standard cryptographic techniques are beyond the use because of their complexity and their weakness in providing copyright protection. In this work we have developed an algorithm in transform domain (discrete cosine transform) for gray level image as watermark. The work can be extended to video, speech and audio.

CHAPTER 2

WATERMARKING SYSTEMS

2.1 Introduction

Powerful signal processing techniques and ease of modification have made the world shift towards digital representation of multimedia signals such as image, audio and video. The rapid growth of Internet is also fuelling this process. The vendors however, fear to put their multimedia data over the Internet, because there is no way to track the illegal distribution and violation of copyright protection. Watermarking comes into the scenario as a powerful solution to this problem. The important feature of watermarking is that the ordinary users may not detect its presence in the product.

2.2 Properties of Watermarks

There are a number of measurable characteristics that a watermark should exhibit. These include that it should be difficult to notice, robust to common distortions of the signal, resistant to malicious attempts to remove the watermark, support a sufficient data rate commensurate with these application, allow multiple watermarks to be added and that the decoder be scalable.

2.2.1 Imperceptibility

The watermark should not be noticeable to the viewer, nor should then watermark degrade the quality of the original image. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms probably, still leave room for an imperceptible signal to be inserted. This may not be true for the next generation compression algorithms. Thus, to survive the next generation of lossy compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer.

2.2.2 Robustness

The watermark must be difficult to remove. If only partial knowledge is available (e.g. the exact location of the watermark in an image is unknown) then attempts to remove or destroy a watermark, should result in severe degradation in fidelity before the watermark is lost.

2.2.3 Common signal processing

The watermark should still be retrievable even if common signal processing operations are applied to the data. These include digital to analog and analog to digital conversion, re-sampling and re-quantization and common signal enhancements to image contrast and color, or audio bass and treble.

2.2.4 Common Geometric Distortions (Image & Video data)

Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling.

2.2.5 Subterfuge Attacks: Collusion & Forgery

In addition, the watermarks should be robust to collusion by multiple individuals each possessing a watermarked copy of the data, i.e., the watermark should be robust to combining copies of the same data set to destroy the watermarks. Further, if a digital watermark is to be used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark with the intention of framing a third party.

2.2.6 Universal

The same digital watermarking algorithm should apply to all the three media under considerations. This is potentially helpful in the watermarking of multimedia products. Also, this feature is conductive to the implementation of audio and image/video watermarking algorithms on common hardware.

2.2.7 Unambiguous

The watermark retrieval should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack. In addition, the watermark procedure also ensures low false positive and low false negative detections.

2.2.8 False Positive Detection

It means the watermarking detector detects the presence of a watermark, even though it is not present. This should be as low as possible for a good watermarking technique.

2.2.9 False Negative Detection

The meaning of this is that the watermarking detector is not able to detect (due to some attacks or some channel effects) the presence of the watermark, even though it is not present. This also should be as low as possible.

Here one important point to note is that, there is a trade-off between the quantity of embedded data and the degree of robustness to host signal modification.

2.3 Attacks on watermarking systems

The different types of watermarking systems include common signal processing, geometric and other intentional attacks.

2.3.1 JPEG and MPEG Compression

The digital signals, which are discrete in, time domain result in a very large number of coefficients in the corresponding frequency domain representation. A large number of coefficients mean the necessity of more & more amount of space and increased computational time. However, it is observed that in case of audio & video signals maximum power is concentrated in the low frequency. Thus the inclusion of all the frequency coefficients results in an unnecessary increase of space and time complexity. This leads to the necessity of compression of the original source material for more efficient storage and transmission. Thus, the watermarking strategy should be such that

the watermark structure is not lost or distorted beyond recognition while discarding the high frequency coefficients during compression.

2.3.2 Filtering

The marketed image may undergo several filtering operations in the course of enhancement techniques. Such filtering operations include low pass, high pass, median or Gaussian filtering. It is absolutely necessary for the watermarked information to be resistant to all such filtering processes.

2.3.3 Rescaling

The watermark is also prone to be distorted or lost while the marketed image is rescaled.

2.3.4 Cropping

A common editing operation is the spatial rejection of a portion of the marketed image. Such an operation is also considered to be a serious threat to the watermarked information. This is a very important consideration when the watermarking is done in the spatial domain. This requires the watermarked information to be embedded in those areas of the original image which are significant, and if cropped away results in severe degradation of the actual image.

2.3.5 Jitter Attack

A simple and yet devastating attack on the watermark is to add a bit of jitter to the signal. In cases where the lower order bits are used to carry the watermark information, such an attack can totally destroy the hidden data.

2.3.6 Stir Mark

Stir mark is a geometric tool developed for simple robustness testing of image marking algorithms and other Steganography techniques. Stir Mark simulates a re-sampling process, i.e. it introduces the same kind of errors into an image as printing it on a high quality printer and then scanning it again with a high quality scanner. It applies a minor

geometric distortion; the image is slightly stretched, sheared, shifted or rotated by an unnoticeable random amount and then re-sampled using either bi-linear or Nyquist interpolation. In addition, a transfer function that introduces a small and smoothly distributed error into all the sample values is applied. This emulates the small non-linear analog/digital converter imperfection typically found in scanners and display devices. Stir Mark introduces a practically unnoticeable quality loss in the image if it is applied only once. However, after a few repeated operations the quality of the image detoriates to a noticeable extent.

2.3.7 The Mosaic Attack

The attack was motivated by a fielded automatic system for copyright piracy detection, consisting of a watermarking scheme plus a WebCrawler that downloads pictures from the Net and checks whether they contain a watermark. This type of attack usually chops an image into a number of small sub-images, which are embedded in a suitable sequence in a web page.

2.4 Applications of Watermarking [23].

2.4.1 Copyright Protection

The goal of watermarking for copyright protection is to embed a "mark" into the image data that can identify the copyright holder of the work. Together with owner Identification, one might also want to embed the mark (or fingerprint) indentifying the buyer of a work for circulation tracking. The mark can be a registered number, a text message or a graphical logo, or some unique pattern. The term watermark stems from the ancient art of marking paper with a logo for the same purpose.

2.4.2 Image Authentication and Data Integrity

Another application of watermarking is image authentication and "Tamper Detection". Digital photographs are being used more and more as court evidence these days. Here, watermarking is used to detect significant modifications of the image. Digital images are susceptible to seamless modifications from sophisticated image processing applications. Watermarks can here be used as a means to verify the genuineness of an image. Verification watermarks are required to be fragile, so that any modification to the image will destroy (or detect alter) the mark. Unlike cryptographic message digests which can only validate copies, watermarking for image authentication should tolerate some well defined image distortion.

2.4.3 Data Hiding and Image Labeling

Data hiding or steganography tries to invisibly embed the maximum amount of data into a host signal (e.g. an image). This allows communication using often enciphered message without attracting the attention of a third party. Typically, robustness requirements are low for steganographic purposes; instead invisibility and capacity are of prime importance.

Image Labeling is an application where information about the image content is encoded as a watermark and inserted into the image to assist image retrieval from a database or provide extra information to the viewer.

2.4.4 Watermarking Everything

Watermarking that is the technique of placing and transmitting small amounts of Data imperceptibility in host or covers data, has recently found many applications. Nowadays, there exist watermarking methods for virtually every kind of digital media: text documents,, images, video, audio , even for 3-D polygonal models , maps and computer programs Interestingly, watermarking technology is not limited to digital media but also applicable to chemical data like protein structure .

CHAPTER 3

METHODOLOGIES FOR WATERMARKING

3.1 Why do we need a transform?

Mathematical transformations are applied to signals to obtain further information from that signal that is not readily available in the raw signal (time, space or any type of signal) before the transmission.

For time domain signal, the time amplitude representation is not always a best representation of the signal for most signal processing related application. The same is true for two-dimensional image. The pixel or space domain representation is not always the best representation.

In many cases the most distinguished information is hidden in the frequency content of the signal. The frequency spectrum of a signal is basically the frequency components (spectral components) of that signal i.e. it shows what frequencies exists in the signal and with the help of Fourier Transform we can measure frequency, or find the frequency content of a signal.

3.2 Transforms Available

The following transforms have been used for the watermarking process:

3.2.1 Fourier Transform

The Fourier Transform, a pervasive and versatile tool, is used in many fields of science as a mathematical or physical tool to alter a problem into one that can be more easily solved.

The Fourier Transform, in essence, decomposes or separates a waveform or function into sinusoids of different frequency which sum to the original waveform.

Two Dimensional Fourier transforms simply involve a number of 1 dimensional Fourier transforms. 2D transform of a 1K by 1K image requires 2K 1D transforms. This follows directly from the definition of the Fourier transform of a continuous variable or the

Discrete Fourier Transform of a discrete system [4, 5, 6].

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N} kn} \qquad \text{k= 0. . . N-1}$$

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{\frac{2\pi i}{N} kn} \qquad \text{n=0. . . N-1}$$

3.2.2 Discrete Cosine Transform

Discrete cosine transform (DCT) is widely used transform in image processing, especially for compression. Some of the applications of two-dimensional DCT involve still image compression and compression of individual video Frames etc. The DCT works by separating images into parts of differing frequencies. A countless number of papers discussing DCT algorithms is strongly witnessing about its importance and applicability. It turns over the image edge to make the image transformed into the form of even function. It's one of the most common linear transformations in digital signal process technology [4, 5, 6, 7, 8, 27].

$$X_k = \sum_{n=0}^{N-1} x_n \cos[\frac{\pi}{N}(n + \frac{1}{2})k] \qquad \text{k=0, . . . , N-1}$$

3.2.3 Discrete wavelet transform

Wavelet

A wave is an oscillating function of time or space that is periodic. The wave is an infinite length continuous function in time or space. In contrast, wavelets are localized waves. A wavelet is a waveform of an effectively limited duration that has an average value of zero.

A family of wavelets can be generated by dilating and translating the mother wavelet $\psi(x)$ which is given by:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})$$

Here, **a** is the scale parameter and ***b*** is the shift parameter.

Wavelet Transform

The wavelet transform (WT) provides a time-frequency representation of the signal. The wavelet transform was developed to overcome the shortcomings of the short-time Fourier transform, which can be used to analyze non-stationary signals. The main drawback of the STFT is that it gives a constant resolution at all frequencies, while the wavelet transform uses a multi-resolution technique by which different frequencies are analyzed with different resolutions. The wavelet transform is generally termed *mathematical microscope* in which big wavelets give an approximate image of the signal, while the smaller wavelets zoom in on the small details. The basic idea of the wavelet transform is to represent the signal to be analyzed as a superposition of wavelets [12,13,14].

The Continuous Wavelet Transform (CWT) of a one-dimensional signal *x(t)* is given by:

$$W_f(a,b) = \int_{-\infty}^{\infty} x(t)\,\psi_{a,b}\,(t)dt$$

Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT) is obtained by filtering the signal through a series of digital filters at different scales. The scaling operation is done by changing the resolution of the signal by the process of sub sampling [1]

The DWT can be computed using either convolution-based or lifting-based procedures. In both methods, the input sequence is decomposed into low-pass and high-pass sub-bands, each consisting of half the number of samples in the original sequence.[2,3]

The Discrete Wavelet Transform (DWT) has become a very versatile signal processing tool over the last decade. In fact, it has been effectively used in signal and image

processing. The advantage of DWT over other traditional transformations is that it performs multi resolution analysis of signals with localization both in time and frequency. The DWT is being increasingly used for image compression today since it supports features like progressive image transmission (by quality, by resolution), ease of compressed image manipulation, region of interest coding, etc.

The DWT performs single-level two-dimensional wavelet decomposition. It computes the approximation coefficients matrix and detailed coefficients matrices obtained by wavelet decomposition of the input image [20, 22, 28, 29].

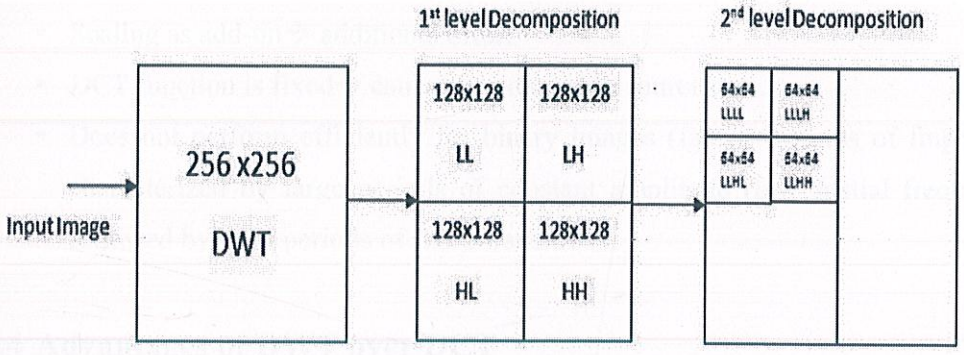


Fig 3.1 Block Diagram of 2nd level DWT Decomposition

3.2.4 Singular Value Decomposition

Today multimedia content (image, video, audio, etc.) enriches integrity of a digital image becomes increasingly important in digital forensics and multimedia security. Singular value decomposition (SVD) is a matrix factorization and provides a new way for extracting algebraic and geometric features from an image. SVD has been used in many fields such as data compression, signal processing and pattern analysis. Human's daily life, its prosperity also attracts malicious attackers and abusers with different motivations. Detecting tampered regions and proving the authenticity [9].

In SVD based watermarking every real matrix P is decomposed into the product of three matrices P=U*S*V' where U and V are orthogonal matrices and S is a diagonal matrix with which contains the singular values of P, the columns of U are called left singular vectors of P and columns of V are called right singular vectors of P [26].

3.3 Disadvantages of DCT:

- Only spatial correlation of the pixels inside the single 2-D block is considered and the correlation from the pixels of the neighboring blocks is neglected.
- Impossible to completely decorrelate the blocks at their boundaries using DCT.
- Undesirable blocking artifacts affect the reconstructed images or video frames. (High compression ratios or very low bit rates).
- Scaling as add-on→ additional effort
- DCT function is fixed→ cannot be adapted to source data.
- Does not perform efficiently for binary images (fax or pictures of fingerprints) characterized by large periods of constant amplitude (low spatial frequencies), followed by brief periods of sharp transitions.

3.4 Advantages of DWT over DCT

- No need to divide the input coding into non-overlapping 2-D blocks, it has higher compression ratios avoid blocking artifacts.
- Allows good localization both in time and spatial frequency domain.
- Transformation of the whole image→ introduces inherent scaling.
- Better identification of which details relevant to human perception→ higher compression ratio.(64:1 vs. 500:1).
- Higher flexibility: Wavelet function can be freely chosen

3.5 Advantages of SVD-DWT over DWT.

- In a DWT based scheme, the DWT coefficients are modified with the data that represents the watermark whereas, while performing SVD-based watermarking,

we apply SVD to the cover image and obtain the singular values. These singular values are then modified to embed the watermark in the image [10, 11].

- DWT-SVD since in this watermarking system watermarks inserted in the lowest frequencies (LL sub band) are resistant to one group of attacks, and watermarks embedded in highest frequencies (HH sub band) are resistant to another group of attacks. If the same watermark is embedded in 4 blocks, it would be extremely difficult to remove or destroy the watermark from all frequencies.

Chapter 4

PROBLEM ANALYSIS

4.1 Aim of Project

We use watermarking scheme based on Discrete Wavelet Transform (DWT) and DWT-Singular Value Decomposition (SVD). After decomposing the cover image into four bands, the DWT coefficients are modified to embed the watermark data in case of DWT and in case of DWT-SVD we apply the SVD to each band, and embed the same watermark data by modifying the singular values. Modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks.

4.2 Resources

4.2.1 MATLAB

MATLAB is a high-level language and interactive environment that enables you to perform computationally intensive tasks faster than with traditional programming languages such as C, C++, and Fortran.

Key Features:

* High-level language for technical computing
* Development environment for managing code, files, and data
* Interactive tools for iterative exploration, design, and problem solving
* Mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, and numerical integration
* 2-D and 3-D graphics functions for visualizing data
* Tools for building custom graphical user interfaces
* Functions for integrating MATLAB based algorithms with external applications and languages, such as C, C++, Fortran, Java, COM, and Microsoft Excel

4.2.2Image Processing Toolbox

Perform image processing, analysis, and algorithm development Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. You can restore noisy or degraded images, enhance images for improved intelligibility, extract features, analyze shapes and textures, and register two images. Most toolbox functions are written in the open MATLAB language, giving you the ability to inspect the algorithms, modify the source code, and create your own custom functions.

It supports a diverse set of image types, including high dynamic range, gigapixel resolution, ICC-compliant color, and tomographic images. Graphical tools let you explore an image, examine a region of pixels, adjust the contrast, create contours or histograms, and manipulate regions of interest (ROIs). With the toolbox algorithms you can restore degraded images, detect and measure features, analyze shapes and textures, and adjust the color balance of images.

Key Features:

* Image enhancement, filtering, and deblurring
* Image analysis, including segmentation, morphology, feature extraction, and measurement
* Spatial transformations and image registration
* Image transforms, including FFT, DCT, Radon, and fan-beam projection
* Workflows for processing, displaying, and navigating arbitrarily large images
* Modular interactive tools, including ROI selections, histograms, and distance measurements
* ICC color management
* Multidimensional image processing
* Image-sequence and video display

4.3.1 Embedding:

1. Using DWT, decompose the cover image A into 4 sub bands: LL, HL, LH, and HH.
2. Apply SVD to each sub-band image.
3. Apply SVD to the visual watermark.
4. Modify the singular values of the cover image in each sub-band with the singular values of the visual watermark.
5. Obtain the 4 sets of modified DWT coefficients.
6. Apply the inverse DWT using the 4 sets of modified DWT coefficients to produce the watermarked cover image.

4.3.2) Extraction:

1. Using DWT, decompose the watermarked (and possibly attacked) cover image A* into 4 sub-bands: LL, HL, LH, and HH.
2. Apply SVD to each sub-band image.
3. Extract the singular values from each sub-band.

Construct the four visual watermarks using the singular vectors.

4.4 Our observations regarding the proposed watermarking scheme can be summarized as follows:

• SVD is a very convenient tool for watermarking in the DWT domain. We observed that the scaling factor can be chosen from a fairly wide range of values for LL, and also for the other three bands. As the LL band contains the largest wavelet coefficients, the scaling factor is chosen accordingly.

• In most DWT-based watermarking schemes, the LL band is not modified as it is argued that watermark transparency would be lost. In the DWT-SVD based approach, we experienced no problem in modifying the LL band.

• Watermarks inserted in the lowest frequencies (LL subband) are resistant to one group of attacks, and watermarks embedded in highest frequencies (HH subband) are resistant to another group of attacks. If the same watermark is embedded in 4 blocks, it would be extremely difficult to remove or destroy the watermark from all frequencies.

• One advantage of SVD-based watermarking is that there is no need to embed all the singular values of a visual watermark. Depending on the magnitudes of the largest singular values, it would be sufficient to embed only a small set. This SVD property has been exploited to develop algorithms for lossy image compression.

Experimental results demonstrate that this method is robust against several attacks such as. The DWT-SVD based watermarking scheme was tested using twelve attacks. The chosen attacks were Gaussian blur, Gaussian noise, pixilation, JPEG compression, JPEG 2000 compression, sharpening, rescaling, rotation, cropping, contrast adjustment, histogram equalization, and gamma correction.

4.5 Flowchart

4.5.1 DWT Embedding:

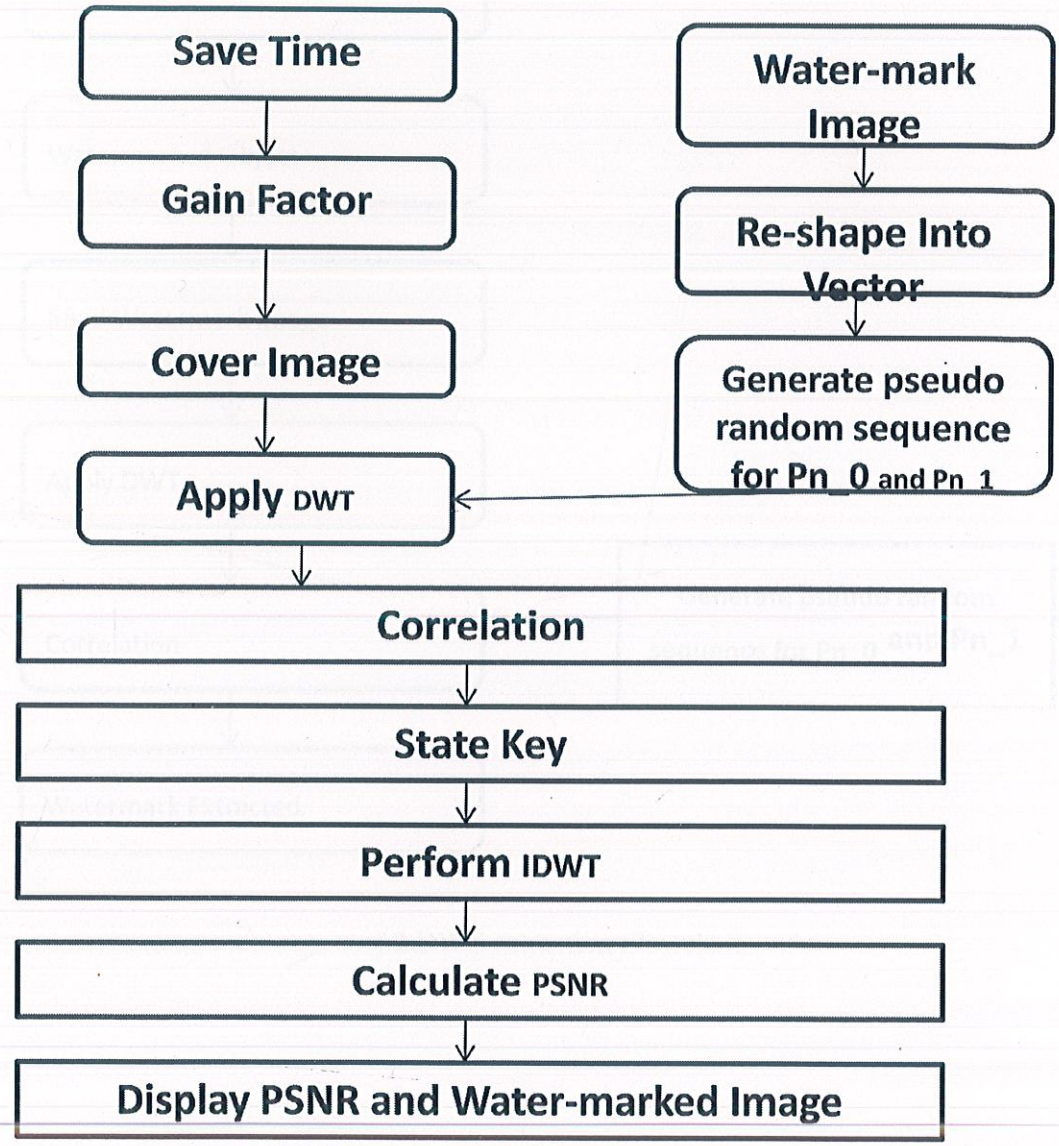
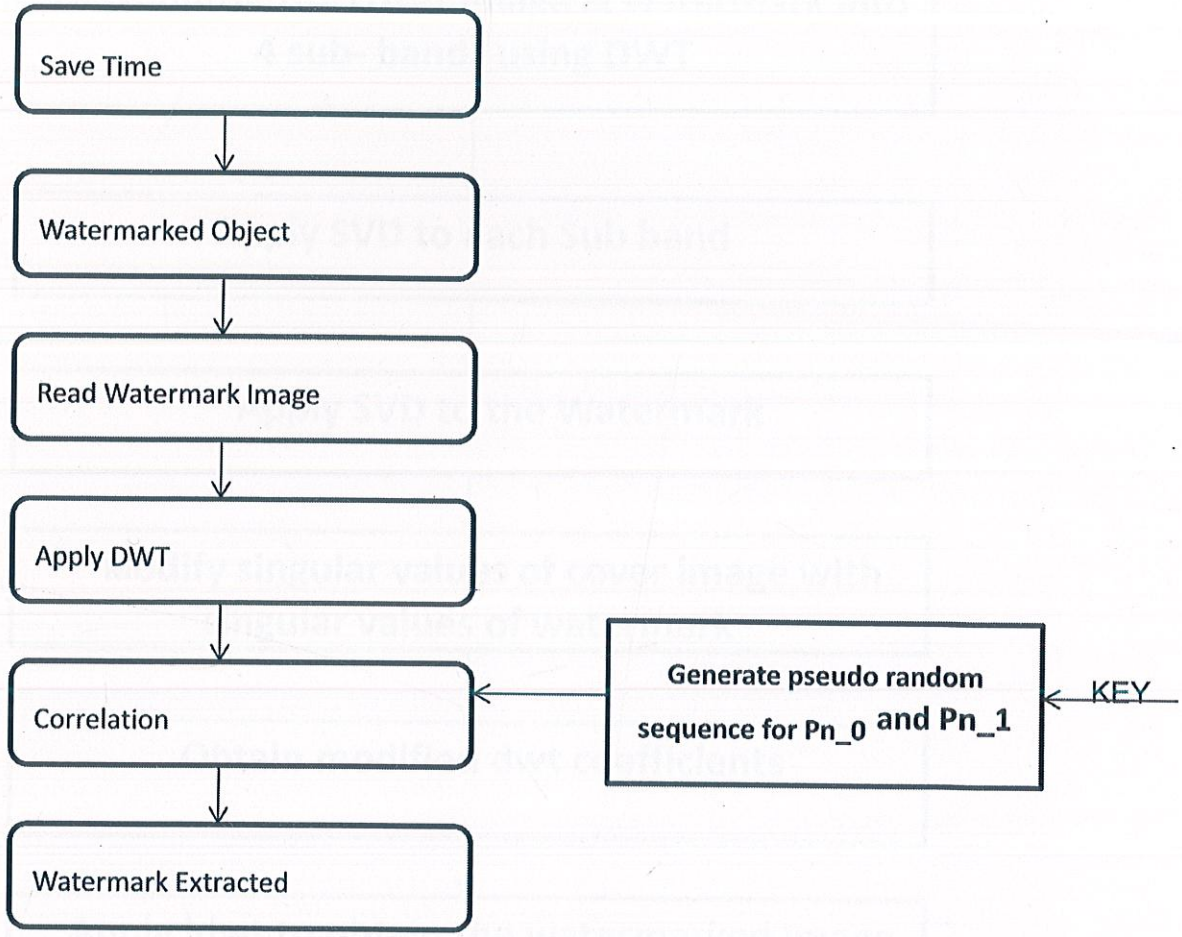


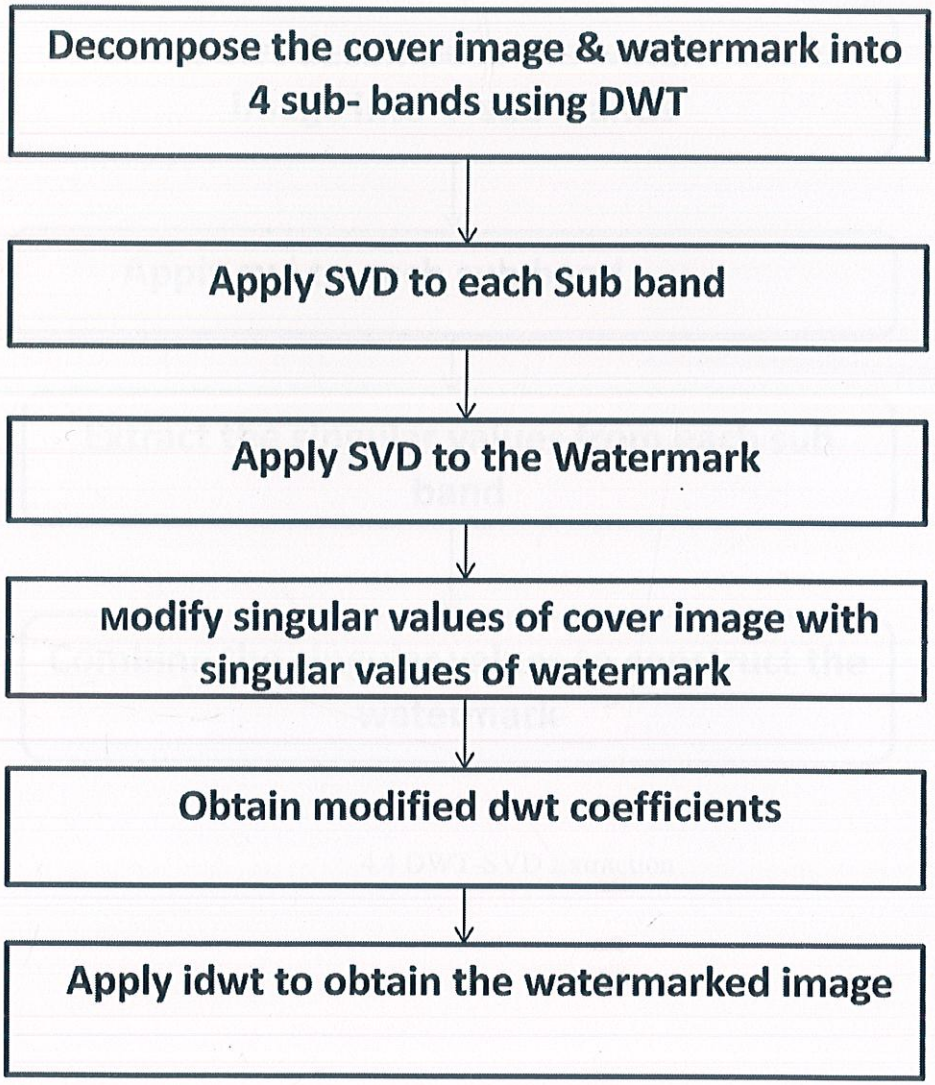
Fig4.1 DWT embedding Flowchart.

4.5.2 DWT Extraction:



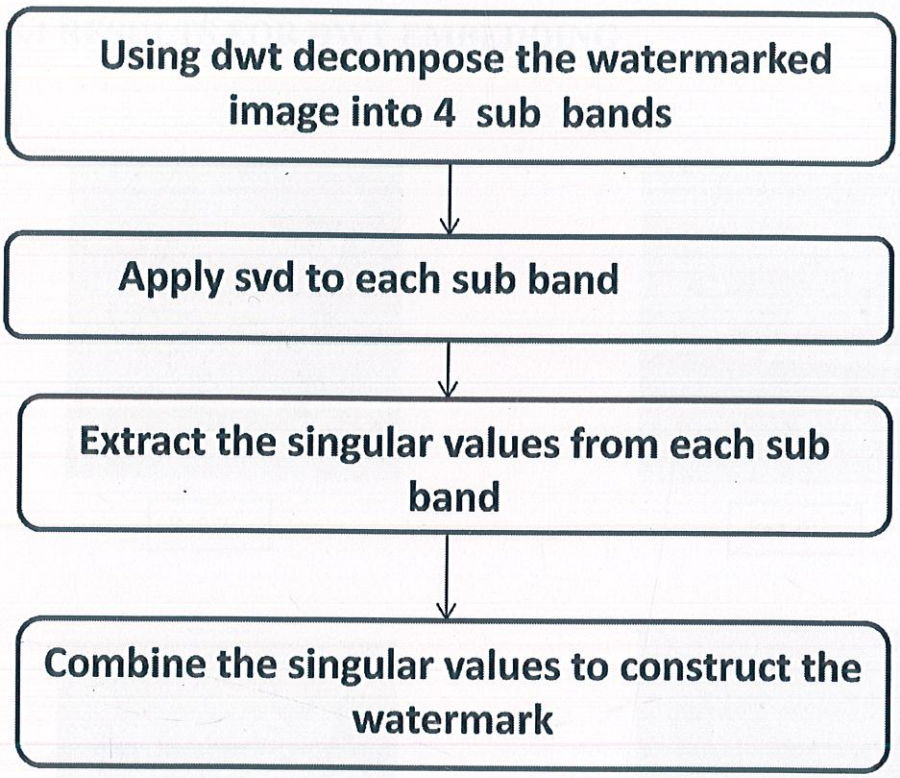
4.2 DWT extraction Flowchart

4.5.3 DWT-SVD Embedding:



4.3 DWT-SVD Embedding Flowchart

4.5.4 DWT-SVD Extraction:



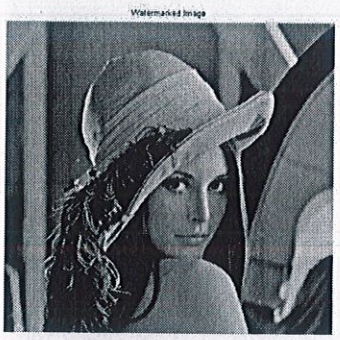
4.4 DWT-SVD Extraction

CHAPTER 5

RESULTS AT A GLANCE

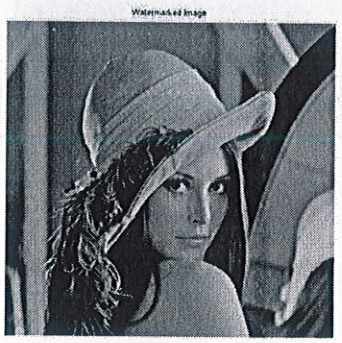
5.1 RESULTS FOR DWT EMBEDDING

K=0.2



K=1.0

K=1.5



K=2.0

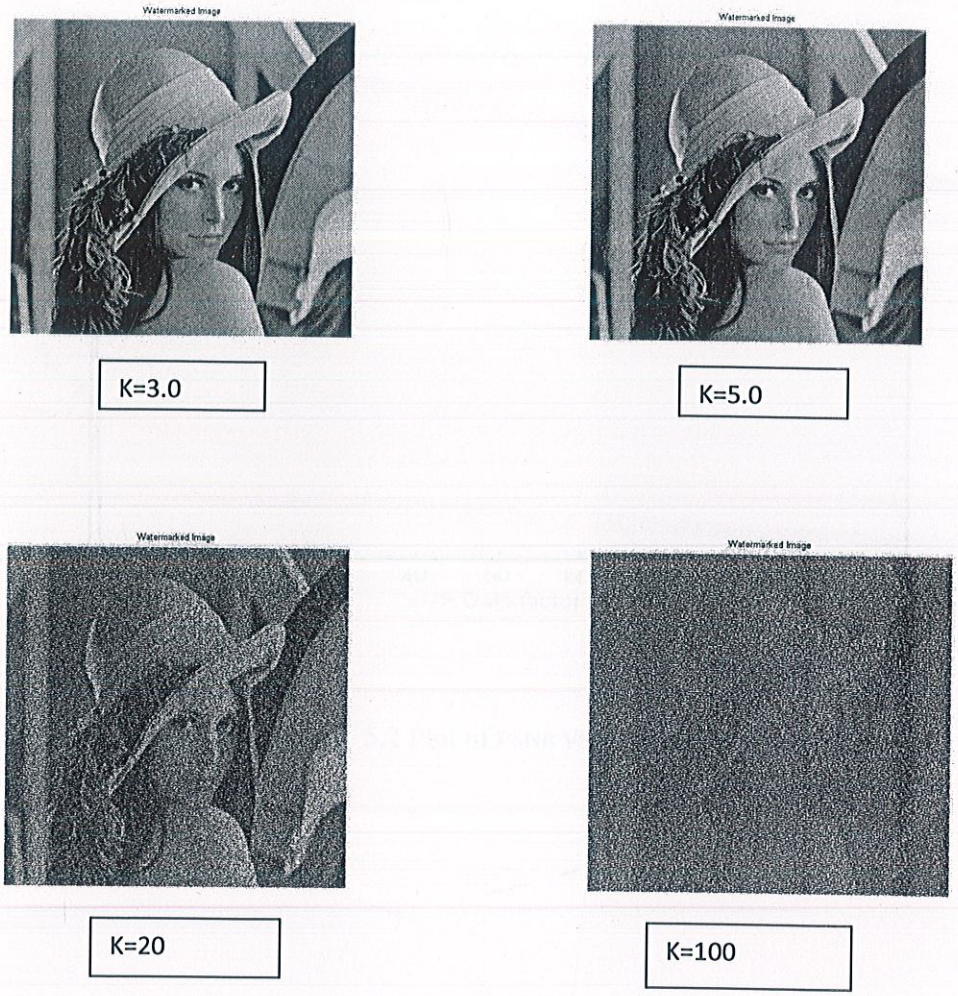


Fig. 5.1 Results for DWT embedding for various values of K

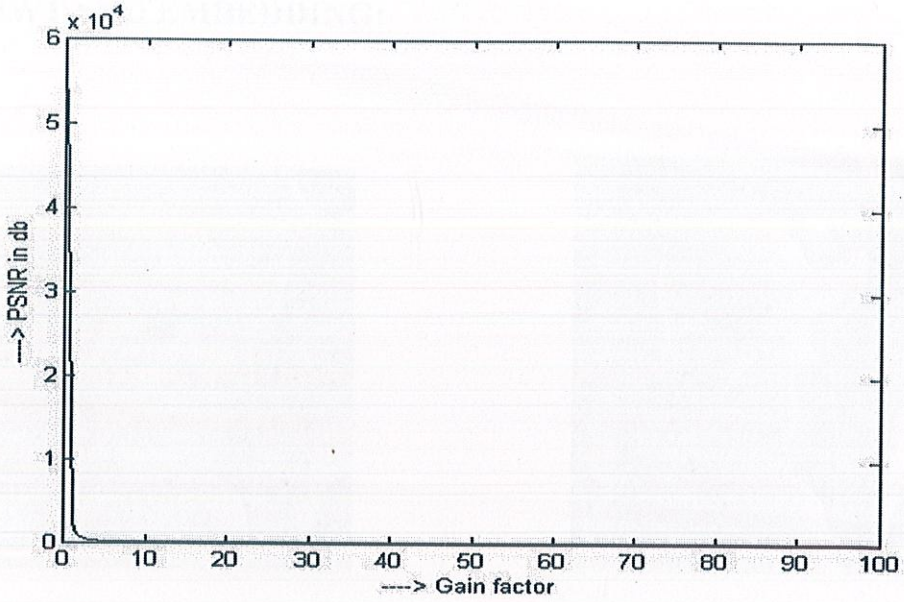


Fig. 5.2 Plot of PSNR VS GAIN FACTOR

5.2 DWT EXTRACTION:

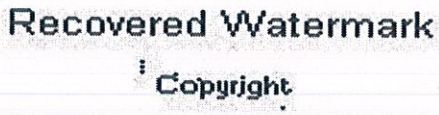


Fig. 5.3 DWT extraction results

5.3 DWT-SVD EMBEDDING:

ORIGINAL IMAGE

WATERMARKED IMAGE,K=2

Fig. 5.4 DWT-SVD embedding results

5.4 DWT-SVD EXTRACTION:

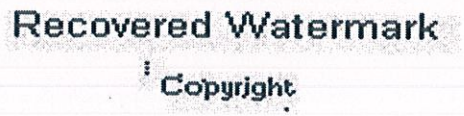


Fig. 5.5 DWT-SVD extraction results

Chapter 6

Conclusion

The technique used by us is block based and hence it is more efficient. Moreover the watermark is embedded in all the four coefficients so the image is resistant to many attacks. Embedding the visual watermark in both the frequency component low and high robust scheme can resist different attacks. Embedding in low frequencies increases the robustness with respect to attacks that have low pass characteristics like filtering, lossy compression, and geometric distortions while making the scheme more sensitive to modifications of the image histogram, such as contrast/brightness adjustment, gamma correction, and histogram equalization. Watermarks embedded in middle and high frequencies are typically less robust to low-pass filtering, lossy compression and small geometric deformations of the image but are highly robust with respect to noise adding, and nonlinear deformations of the gray scale.

Chapter 7

Contribution of the project

Digital watermarking contributes as a solution to copy protection of multimedia objects and to discourage counterfeiting (in the case of stamps and currency). In the modern era, proving authenticity is becoming increasingly important as more of the world's information is stored as readily transferable bits. Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer. Copyright abuse is the motivating factor in developing new encryption technologies. One such technology is digital watermarking. Thus following are our project contributions:

- Establishing ownership by embedding identifying data.
- Tracking the movement of authorized copies by embedding a unique serial number in each copy.
- Attaching meta-data that pertains to the image such as a time, date, and location stamp

REFERENCES

[1] Chen Yongqiang1, Zhang Yanqing2, and Peng Lihua3, "A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network", Proceedings of the 2009 International Symposium on Information Processing (ISIP'09) Huangshan, P. R. China, August 21-23, 2009, pp. 298-301

[2] Andrew B. Watson, Gloria Y. Yang, Joshua A. Solomon, and John Villasenor,"Visibility of Wavelet Quantization Noise", IEEE Transactions on image processing ,Vol. 6,No. 8, August 1997.

[3] A. Grzeszczak ,M.K. Mandal, S. Panchanathan, "VLSI implementation of discrete wavelet transform",Dec 1996 Vol. 4, pp. 421-433.

[4] Hyesook Lim, Vincenzo Piuri, Earl E. Swartzlander,"A Serial-Parallel Architecture for Two-Dimensional Discrete Cosine and Inverse Discrete Cosine Transforms", Dec 2000, Vol. 49, pp. 1297-1309.

[5] H. Lim, C. Yim, E.E. Swartzlander Jr., "Finite Word-Length Effects Of An Unified Systolic Array For 2-D DCT/IDCT", 1996 IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'96).

[6] C. Candan, M.A. Kutay, H.M. Ozaktas, "The discrete fractional fourier transform," IEEE Transactions on Signal Processing, May 2000, Vol. 48, pp. 1329-1337.

[7] A.I. Zayed, "A convolution and product theorem for the fractional Fourier transform", IEEE Signal Processing Letters, Apr 1998,Vol. 5, pp. 101-103.

[8] Kyung L. Heo, Sung M. Cho, Jung H. Lee,,Myung H. Sunwoo, "Application-Specific DSP Architecture For Fast Fourier Transform", 14th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'03)

[9] V. Klema, A.Laub, "The singular value decomposition: Its computation and some applications", IEEE Transactions on Automatic Control, Apr 1980, Vol. 25, pp. 164-176

[10] David Gleich, Leonid Zhukov, "SVD based Term Suggestion and Ranking System," icdm, pp.391-394, Fourth IEEE International Conference on Data Mining (ICDM'04), 2004.

[11] S. Esakkirajan, T. Veerakumar, P. Navaneethan, "Best Basis Selection Using Singular Value Decomposition," icapr, pp.65-68, 2009 Seventh International Conference on Advances in Pattern Recognition, 2009.

[12] Xiu-bi Wang, "Image enhancement based on lifting wavelet transform," 4th International Conference on Computer Science & Education, 2009. ICCSE '09., pp. 739-741.

[13] Tao Huang, Lele Qin, " Image denoising research based on lifting wavelet transform and threshold optimization", 2009 3rd IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications ,pp. 1218 – 1220.

[14] C.M. Patil, S. Patilkulkarani, "Iris Feature Extraction for Personal Identification Using Lifting Wavelet Transform", International Conference on Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09, Dec 28-29, pp. 764 – 766.

[15] F. Hartung and M. Kutter, "Multimedia watermarking Technique", IEEE proceeding on Signal Processing", Volume 87, NO.7, pp.1079-1107, July 1999.

[16] N. Memon,& P.W. Wong (1998). Protecting digital media content. Communications of the ACM, 41(7), 35-43.

[17] J. Dittmann, A. Mukherjee & M. Steinebach, (2000, March 27 - 29). Media-independent watermarking classification and the need for combining digital video and audio watermarking for media authentication. Paper presented at the Proceedings of the international conference on information technology: Coding and computing, Las Vegas, Nevada.

[18] C.I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual Models," IEEE Journal on Selected Areas in Comm., vol 16, no. 4, pp. 525-539, May 1998.

[19] F. Hartung and M. Kutter, "Multimedia Watermarking Technique", IEEE Proceeding on Signal Processing", Volume 87, NO.7, pp.1079-1107, July 1999.

[20] O.G Pla, Lin E.T, and Delp E.J, "A Wavelet Watermarking Algorithm Based on a Tree Structure", Tech. Rep., Polytechnic University of Catalonia, Spain, 2004.

[21] Z Yuehua., C. Guixian and D. Yunhai, "An Image Watermark Algorithm Based on Discrete Cosine Transform Block Classifying", ACM Int. Conf., pp. 234-235, 2004..

[22] X. J. Wu, Hu. Z. Gu, and J.Huang "A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters", Tech. Rep., Sun Yat-Sen University, China, , 2005.

[23] C. I. Podilchuk and E. J. Delp, "Digital Watermarking:Algorithms and Applications," IEEE Signal Processing Magazine, , pp. 33-46, July 2001

[24] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.

[25]] R. G.vanSchyndel, A. Z. lTrkel and C.F.Osbome, "A Digital Watermark" IEEE, 1994.

[26] V. I. Gorodetski, L. J. Popyack, V. Samoilov and V. A. Skormin, "SVD-based Approach to Transparent Embedding data into digital images," International Workshop on Mathematical Methods, Models and Architechtures for Computer network Security (MMMACNS 2001), St. Petersbug, Russia, May 21-23, 2001.

[27] Reduction of discrete cosine transform/ quantisation/ inverse quantization/ inverse discrete cosine transform computational complexity in H.264 video encoding by using an efficient prediction algorithm.

[28] M. Vishwanath, R.M. Owens, "A Common Architecture For The DWT and IDWT," asap, pp.193, 1996 IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'96), 1996.

[29] Christian Tenllado, Javier Setoain, Manuel Prieto, Luis Piñuel, Francisco Tirado, "Parallel Implementation of the 2D Discrete Wavelet Transform on Graphics Processing Units: Filter Bank versus Lifting," IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 3, pp. 299-310, Mar. 2008.

BIBLIOGRAPHY

[1] M.Antonini, M. Barlaud, P. Mathieu, I.Daubechies, "Image coding using wavelet transform", IEEE Transactions on Image Processing, VOL. 1, pp. 205 – 220, Apr 1992.

[2] S. Arivazhagan and L. Ganesan, "Texture segmentation using wavelet transform", Vol. 24, Issue 16, Dec 2003, pp. 3197-3203.

[3] Tinku Acharya and ChaitaliChakrabarti, "A Survey on Lifting-based Discrete Wavelet Transform Architectures", The Journal of VLSI Signal Processing Volume 42, Number 3,pp. 321-339.

[4] Loukhaoukha, K. Chouinard, and J.-Y, "Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification" , 11th Canadian Workshop on Information Theory, 2009. CWIT 2009., pp. 177 -182.

[5] Stefano Gnavi, Barbara Penna, Marco Grangetto, Enrico Magli, and Gabriella Olmo," Wavelet Kernels on a DSP: A Comparison between Lifting and Filter Banks for Image Coding", EURASIP Journal on Applied Signal Processing Volume 2002 (2002), Issue 9, Pages 981-989.

[6] NikolayPolyak, William A. Pearlman, "Wavelet decomposition and reconstruction using arbitrary kernels: a new approach," icip, vol. 3, pp.866, 1998 International Conference on Image Processing (ICIP'98) - Volume 3, 1998.

[7] Forrest M. Hoffman, "An Introduction to Fourier Theory".

[8] Ken Cabeen and Peter Gent, "Image Compression and the Discrete Cosine Transform".

[9] G. H. Golub and C. F. Van Loan, Matrix Computations, 3/e, Johns Hopkins University Press, Baltimore, 1996.

[10] V.C. Klema, "The Singular Value Decomposition: Its Computation and Some Applications," IEEE Trans. Automatic Control, Vol. 25, pp164-176, 1980.

[11] Xiao Bing KANG and Sheng Min WEI, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics", 2008 International Conference on Computer Science and Software Engineering.

[12] L.B. Almeida, "An introduction to the angular Fourier transform," Acoustics, Speech, and Signal Processing, 1993. ICASSP-93, 1993 IEEE International Conference on , vol.3, pp.257-260, Apr 1993.

[13] L.B. Almeida, "The fractional Fourier transform and time-frequency representations ," Signal Processing, IEEE Transactions on , vol.42, no.11, pp.3084-3091, Nov 1994.

[14] A.I. Zayed, "On the relationship between the Fourier and fractional Fourier transforms," Signal Processing Letters, IEEE , vol.3, no.12, pp.310-311, Dec 1996.

[15] Chen Wen-Hsiung, C.Smith, S.Fralick, "A Fast Computational Algorithm for the Discrete Cosine Transform," Communications, IEEE Transactions on , vol.25, no.9, pp. 1004- 1009, Sep 1977.

[16] Jianmin Jiang and GuocanFeng , "The spatial relationship of DCT coefficients between a block and its sub-blocks," Signal Processing, IEEE Transactions on , vol.50, no.5, pp.1160-1169, May 2002.

[17] YoucaiGao; Jinwei Wang; ShiguoLian; , "Optimum detection for Barni's multiplicative watermarking in DWT domain," Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on , vol., no., pp.1308-1311, 25-27 Aug. 2008.

[18] Luc Lamarche; Yan Liu; Jiying Zhao; , "Flaw in SVD-based Watermarking," Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on , vol., no., pp.2082-2085, May 2006.

[19] XiushanNie, Ju Liu, Xianqing Wang, Jiande Sun, "Watermarking for 3D Triangular Meshes Based on SVD," iih-msp, pp.430-433, 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009.

[20] WimSweldons, "The Lifting Scheme: A New Philosophy in Biorthogonal Wavelet Constructions".

[21] N. Polyak, W.A. Pearlman, "Wavelet decomposition and reconstruction using arbitrary kernels: a new approach," icip, vol. 1, pp.660, 1997 International Conference on Image Processing (ICIP'97) - Volume 1, 1997.

[22]Farid Ahmed, "A dual Fourier-wavelet domain authentication-identification watermark," Opt. Express 15, 4804-4813 (2007).

[23]VassiliosSolachidis, Ioannis Pitas, "Watermarking Polygonal Lines Using Fourier Descriptors", vol. 24, no. 3, pp. 44-51, May/June 2004 .

[24] Tribhuwan Kumar Tewari and VikasSaxena, "An Improved and Robust DCT Based Digital Image Watermarking Scheme.", International Journal of Computer Applications , June 2010.

[25] Ameya K Naik and RaghunathHolambe, " A Blind DCT Domain Digital Watermarking for Biometric Authentication", International Journal of Computer Applications, February 2010.

[26] K. Raghavendra and K.R. Chetan, "DWT Based Blind Digital Video Watermarking Scheme for Video Authentication", International Journal of Computer Applications ,August 2010.

[27] Zhu-zhiJia, Hong-yu Zhu, Wan-sheng Cheng, "A Blind Watermarking Algorithm Based on Lifting Wavelet Transform and Scrambling Technology," icece, pp.4576-4579, 2010 International Conference on Electrical and Control Engineering, 2010.

[28] DashunQue; Li Zhang; Ling Lu; Liucheng Shi; , "A ROI Image Watermarking Algorithm Based on Lifting Wavelet Transform," Signal Processing, 2006 8th International Conference on , vol.4, no., 16-20 2006.

[29] Miyazaki, A.; Uchiyama, F.; , "An Image Watermarking Method using the Lifting Wavelet Transform," Intelligent Signal Processing and Communications, 2006. ISPACS '06. International Symposium on , vol., no., pp.155-158, 12-15 Dec. 2006.

[30] Emir Ganic Ahmet M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking:Embedding Data in All Frequency.