A Novel Invisible Watermarking Methods Using Binary Watermarks

Neha Solanki[1], Sarika Khandelwal[2]
[1]Geetanjali Institute of Technical Studies, Udaipur
[2]Associate Professor, Geetanjali Institute of Technical Studies, Udaipur

Abstract- *In recent years the popularity of digital video based applications is accompanied by the need for copyright protection to prevent illicit copying and distribution of digital video. Copyright protection inserts authentication data such as ownership information and logo in the digital media without affecting its perceptual quality. In case of any dispute, authentication data is extracted from the media and can be used as an authoritative proof to prove the ownership. As a method of copyright protection, digital video watermarking has recently emerged as a significant field of interest and a very active area of research.*

In this work the targeted invisible watermarking is approached using Haar Wavelet functions, the watermark or message embedded into cover image, prior to it , image segmentation approach is utilized here to extract the object of interest in message and covert an 8bit or 16 bit message information to one bit binary message. The embedding is performed in odd and even blocks of LH and HL bands, by modulation the corresponding band value on the basis of proposed embedding rule set.

The retrieved results from the proposed experimental setup reveals that embedding a watermark can be performed more faster and more robust than the existing methodologies.

I. INTRODUCTION

The use of digital video has grown dramatically in recent times. Digital video applications include video-on-demand, video-conferencing, digital cinema, digital television, distance learning, entertainment, and advertising. Many users experience digital video when they watch a motion picture recorded on a digital videodisc (DVD) or downloaded over the internet. Proliferation of digital video into more applications is encouraged by improving compression technology, better authoring and editing tools, capture and display devices at low cost; and more available bandwidth in digital communication networks. The reproduction, manipulation and the distribution of digital multimedia (images, audio and video) via networks become faster and easier. Therefore, owners and creators of digital products are concerned about illegal copying of their product. As a result, security and copyright protection are becoming important issues in multimedia applications and services.

1.1 THE NEED OF WATERMARKING:

The aim here is to access the ownership or integrity of some pieces of information named after the watermark. In the use of watermark the watermark should be unobtrusive (perceptually invisible), robust, universal i.e. should be applicable to all three media under consideration, resilient to common signal processing and geometric distortions and intentional attack. Intentional attacks include forgery and attacks using one or more. domain and in the spatial domain.

Figure1.1: A general view of watermarking design

II. LITERATURE SURVEY

Continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. Watermarking sudden increase

in interest is most likely due to the increase in concern over IPR. Generally, the watermarking of still image, video, and audio demonstrate certain common basic concepts. Reported several watermarking applications in the literature depend on the services we wish to support.

2.1 HISTORY OF INFORMATION HIDING

The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the West appears in Homer's Iliad . Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history. An important techniques was the use of sympathetic inks. Later, chemically influences sympathetic inks were developed. This was used in World Wars I and II

Watermarking is the process that embeds data called watermark, tag or label into a multimedia object such that watermark can be detected or extracted to make an assertion about the object may an image or video or audio may also be text only.

2.2 CONTENT PROTECTION

Content protection is a challenging problem which involves conflicting interests. Content owners wish to ensure that their intellectual property is not misused, illegally copied, or distributed. The device manufacturers desire to keep their products inexpensive and simple, however, implementing technological content protection measures increases both the cost and complexit y of devices.

2.3 ENCRYPTION

Access control has often been addressed by the use of encryption. Encryption is the process of scrambling data into an unintelligible form. The original data is known as the plaintext and the scrambled data is known as the cipher text. The inverse process of obtaining the plaintext from the cipher text is known as decryption. Encryption provides confidentiality because a secret key is necessary for decryption. Traditionally, encryption has been used to ensure the confidentiality of sensitive information (such as electronic mail, military secrets, and financial information) transmitted through an insecure communications channel. For access control, video is encrypted and the decryption key is provided only after the access conditions have been satisfied. Obtaining the encrypted video alone (without the decryption key) does not allow the video to be displayed.

III. PROBLEM FORMULATION FOR HAAR BASED INVISIBLE EMBEDDING

This thesis resolves the many issues:

ISSUE 1: Till now there in no "Generic" nature in the watermarking algorithms available. More precisely, if certain approach is applicable for a gray level image, the same approach does not work for the other formats of an image.

ISSUE 2: Even if the gray color image watermarking algorithms are extended for RGB color images, the maximum work has been done for (y- luminance) color channel only because human eyes are less sensitive to detect the changes in (y- luminance) color channel. No attack impact which may affect the analysis of the color channels, ie, a particular attack, has been carried out [6-7]. Therefore, apart from choosing digital Image Watermarking as a major problem, we have chosen to identify the suitability of a color channel with respect to attack (if any) for multi-color channel images (True color windows BMP and uncompressed JPEG). We also decided to explore the ways such that attack impacts may be minimized before the watermark embedding process.

ISSUE 3: In most of the research paper, a watermarking scheme is finalized, it is applied to all test images. Each image is different and then some characteristics and after embedding the watermark data by a particular watermarking scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics. So we decided to explore the relationship between the performance of watermarking scheme and the cover image characteristics itself.

ISSUE 4: Most watermarking schemes are developed in a way that first a scheme is developed based on the extension of earlier presented one and then check its performance against the common image manipulations and known attacks. There are huge financial implications of watermarking schemes (say fingerprinting), but no scheme has been developed, which is, by design, resistant to at least one attack, to ensure that, a particular attack (having most financial issues) cannot be conducted by an attacker. Therefore we decided to design watermarking schemes such that an inherent nature in can be embedded to guarantee that at least one serious attack having most financial implications cannot be conducted on watermarked images.

3.1 DIGITAL WATERMARKING

Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be

detected or extracted later to make an assertion about the data. This information may be textual data the author, its copyright, etc; or it can be an image itself. Be hidden information is embedded by manipulating the contents of the digital data, allowing someone to identify original owner, or in the case of illicit duplication of purchased material, the buyer is involved. These digital watermarks remain intact under transmission / transformation, allowing us to protect our proprietary rights in digital form.

3.2 CLASSIFICATION

Digital watermarking is the process that embeds data called a watermark into a multimedia object in such a way that the watermark can be later on detected or extracted for object assertion purposes. Multimedia in commodities watermark is embedded, are usually called: the original cover signal, the host signal or bus work. A digital watermark is a distinguishing piece of information that is assigned to the data to protected. This is an important requirement the watermark cannot be easily extracted or removed from the watermarked object.

Watermarking techniques can be differentiated into the following four categories according to the type of the multimedia document to be watermarked:

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

According to the human perception, the digital watermarks can be classified into different categories, are as follows:

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

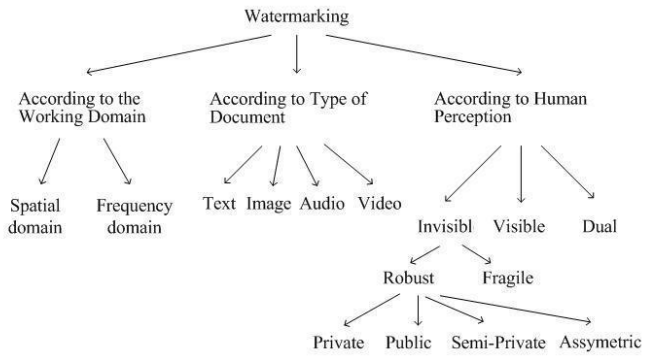


Fig-3.2.1 classification of digital watermarking

There are various ways to classify digital watermarking, such as: utility, medium, by detecting process, by content, and so on. There are some useful and effective ways:

3.2.1 Robustness

Robustness is one of the most important attributes of a digital watermark. Fragile digital watermark is a digital watermark that fails to be detected after the slightest modifies. A semi- fragile digital watermark is digital watermark that resists benign transformation but fails to be detected after malignant transformations

3.2.2 Capacity

It is a way to determines two different main classes of digital watermarking schemes by the length of the embedded messages. Zero bits or presence watermarking schemes, messages, zero assumption is slightly longer it is designed to detect the presence or the absence of the digital watermark in the marked object. Multiple bit watermarking or non-zero bits watermarking schemes, n-bit-long stream message is modulated in the watermark.

3.2.3 Blindness

If a digital watermarking requires the original data for watermark, it is known as non-blind watermarking. You do not need a digital native data for watermark, it is known as blind watermarking.

3.2.4 Embedding method

If the marked signal is obtained by an additive modification, thus embedding method is called spread spectrum. Marked signal is obtained from the quantization, this kind embedding method is known as quantization type. Marked signal is embedded by additive, then modification in the spatial domain, thus embedding method is called amplitude modulation. Spread spectrum is a digital watermark the best robustness but capacity is weak. The digital watermark is known quantization to be weak in robustness but have great capacity.

In Figure3.2.2 the embedding process for still images is presented and used for the explanation purposes.

Let us denote an original image by **I**, a watermark by **W**, the watermarked image by W **I** and K is the embedded key (see Figure 1). The embedding function mb E takes on its input the image **I**, watermark **W** and key K and generates a new watermarked image, denoted with W **I**. Introduction of

the embedded key K is necessary for enhancing the security aspect of the watermarking system. Before the embedding process, the original image can be either transformed in the frequency domain or the embedding can be performed in spatial domain. Depending on the selected domain selection of watermarking techniques. Is embedded in frequency domain, the inverse transform must be applied in order to obtain the watermarked image. Mathematically expressed, the embedding function for the spatial domain techniques can be represented as follows:

Emb W E (**I**,**W**,K) = **IW**

Frequency domain techniques, the following expression is valid.

Emb W E (**f** ,**W**,K) = **IW**

"f" represents the coefficient vector of the transformation applied.

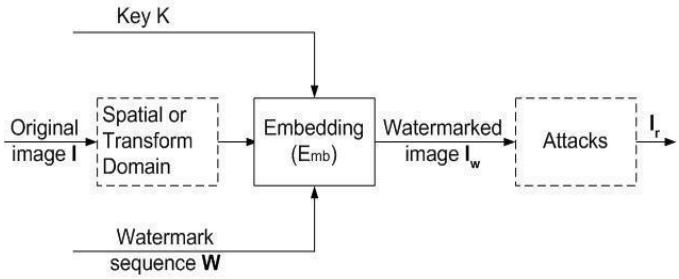


Figure 3.2.2: Embedding unit, as a part of a watermarking system

When the watermarked image is obtained and kept on Internet or transmitted over the communication channel possibly, the attacks occur (image is generated).

3.3 VISIBLE/INVISIBLE DIGITAL WATERMARKING

Visible and invisible are the two basic types of digital watermarking, and the digital watermark can be considered as either visible or invisible. Visible digital watermarking is a way by which anybody can put visible information in digital signals, the information is often a logo which identifies the owner of the digital signal. For example, a television broadcaster typically adds its logo to the corner your video, it is generally visible digital watermark. Invisible digital watermarking is a way by which anybody can hide information in digital signal and the information will not be perceived. Since it is invisible, and invisible digital watermarking has a Used extensively.

3.4 SPATIAL DOMAIN TECHNIQUES

The simplest example of spatial domain watermarking techniques to insert data into digital signals in noise free environments is least significant bit coding. There are several variants of the techniques. This essentially involves embedding watermark by replacing the least significant bit of the image data with a bit of the watermark data [8]. The most straightforward way to embed a watermark into an image in the spatial is to add a pseudo random noise pattern to the luminance values of its pixels. Schyndel, [10] proposed a method based on bit plane manipulation of the least significant bit (LSB) which offers easy and fast decoding. Macq LSB inserts the watermark around image contours [11].

3.5 TRANSFORM DOMAIN TECHNIQUES

Generally Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelete Transform (DWT) are used as the methods of data changes. In these methods, a watermark that one wishes to embed distributive in overall domain of an original data, and the watermark, is hardly being destroyed once embedded.

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods [8]. While there are many robust watermarks in the DCT domain, there are relatively fewer existing data hiding watermarking techniques in DCT domain [15]. Kim, [17] embed watermark bits as pseudo-random sequences in the frequency domain. Langelaar, [19] hide watermarks by removing or retaining selected DCT coefficients. Borg, [18] hide watermark in JPEG images by forcing selected DCT blocks to satisfy certain linear or circular constraint. Some embeds watermark patterns in the quantization module after DCT [23] or in selected blocks based on human visual models. Choi, utilize inter-block correlation by forcing DCT coefficients of a block to be greater or smaller than the average of the neighboring blocks [20].

In 1995, Cox, developed a new algorithm of using spread spectrum to embed a mark [9] To improve Cox method, Lu, [21] to improve the watermark using Cocktail the robustness and used Human Visual System (HVS) to maintain high fidelity of the watermarked image. Hsu etal. [22] Embed watermark bits by modifying the polarity of DCT and DWT coefficients and use a meaningful logo image as the watermark. While most schemes embed only a single watermark, some allow for multiple watermark embedding [6]. Some embed orthogonal watermarks and extend the single watermark algorithms for multiple watermarks [21].

After that the inverse transform should be applied to obtain the watermarked image. Since watermarks applied to transform domain will be dispersed over the entirety of the spatial image upon inverse transformation, this technique is more robust to cropping then the spatial technique.

The transform techniques commonly used for watermarking purposes are respectively: the Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT) and the Discrete Wavelet Transform. They are also less known approaches implementing the Complex Wavelet Transform (CWT) and the Fourier-Mellin Transform (FMT). With the standardization process of JPEG2000 and the shift from DCT- to wavelet-based image compression methods, watermarking schemes operating in wavelet transform domain have become even more interesting.

3.6 APPLICATION OF DIGITAL WATERMARKING

Digital watermarking has been widely and successfully applied in billions of media objects across a wide range of uses. This section will introduce some applications of digital watermarking in both traditional and novel areas

A wide range of applications such as digital watermarking can be used for:

Copyright Protection - for the protection of the intellectual property, the data owner can embeded a watermark representing copyright information in the data. Embedded watermark can be used as a proof, example in a court if someone intentionally infringed the copyrights. Source Tracking (different recipients have different watermarked content) Broadcast Monitoring (Television news often international agencies including the watermarked video)

Fingerprinting: to trace the source of illegal copies, the owner can use fingerprinting technology. In this case, the owner can embed different watermarks in the copies of the data that are supplied to various customers. Fingerprinting can be compared to embedding a serial number that is related to the customers identified in the data. This enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.

Copy protection: the information stored in watermark can directly control digital recording devices for copy protection purposes. In this case watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not.

Broadcast monitoring: by embedding a watermark in commercial advertising, an automated monitoring system can verify whether the advertisements are broadcasted as contracted. Broadcast monitoring can protect not only the commercials but also the valuable TV products.

Data authentication: the so called fragile watermarks can be used to check the authenticity of data. A fragile watermark indicates whether the data has been altered. Further it offers the information in which part the data are being altered.

Medical safety: embedded the date and the patient‟ s name in medical images could be a useful safety measure.

Data Hiding: watermark techniques can be used for the transmission of secret messages. Since various governments restrict the use of encryption services, people can hide their messages in other data.

3.6.1 Application of watermarking in traditional area

It is essential to communicate our copyright ownership and usage rights no matter we are global media corporations or freelance photographers. Digital content is travelling quicker and further than ever before since the combination of access and new equipment. Digital has become a primary means of expression and communication. We are imperceptible watermark which can be embedded digital data that can include proprietary information, contact details, usage rights and we choose anything. For people who are looking for an efficient way to monitor, manage and monetize to their digital assets, the digital watermarking is an effective way and is mostly used today. Digital watermarking can ensure our ownership and contact information are attached for our material, and can add to enhance the automated license revenues, automated remind us when there is an unauthorized use.

3.6.1.1 Protection for audio and video content

In global entertainment industry, piracy of film, music and video is a multi-billion dollar big problem. The digital watermarking can help limit the unauthorized copy and redistribute, it can provide an added layer of protection to the content protection. The digital watermarking can communicate copyright ownership and rights of usage, protect the content against common threats of piracy like camcorder recording, Peer to Peer to share, copy, format

conversion and other forms of reprocessing. We can enjoy our entertainment experience without any difference even if the content has embedded watermarks.

3.6.2 Application of watermarking in novel area

3.6.2.1 Locating content online

Since we rely more and more on the Internet for information sharing, customer engagement, communication and research, we have to upload more content for the Web. For example, if you are a photographer or artist, you would like to share is a huge content on the web.

3.6.2.2 Rich media enhancement for mobile phones

To most of us, mobile phones are no longer merely for talking or texting. We find greater use of mobile phones assistance, information and entertainment. Thousands of popular media companies want to make their products like newspapers and magazines. The watermark can be embedded in all forms of easily media, it is a good way for companies to engage consumers by enriching their media experiences on their mobile phones with protected media content. Digital watermarking can be help companies engage and retain consumers, bring, build brand preference and loyalty traditional printed like newspaper and magazines to the Internet.

3.7 POSSIBLE ATTACKS

The attacks can be both intentional and unintentional. They can be broadly classified as
Jitter attack
Stirmark attacks

Mosaic attack: overlapping various parts of a photograph or different images to create a new one

Filtering attacks: applying median filter, blurring and so on.
Cropping: Leaving other areas to cut crop just the interesting areas of the image.

3.8 DISCRETE WAVELET TRANSFORM

DWT is the discrete variant of the wavelet transform. Wavelet transform represents valid alternative to the cosine transform used in standard JPEG. The DWT of images is a transform based on the tree structure with D levels that can be implemented by using an appropriate bank of filters. Essentially it is possible to follow two strategies that differ from each other basically because of the criterion used to extract strings of image samples to be elaborated by the bank of filters. Most image watermarking schemes operate either in the Discrete Cosine Transform (DCT) or the Discrete Wavelet Transform (DWT) domain. A few watermarking algorithms employ more exotic transforms such as the Fourier-Mellin Transform and the fractal transform. The DWT domain is better suited for image watermarking than the DCT and other transform domains for several reasons:

1. The DWT offers excellent space-frequency localization of salient image features such as textures and edges. In particular, the high frequency content of the image corresponds to large coefficient in the detail sub bands. Hence, watermark encoders operating in the wavelet domain can easily locate the high-frequency features of an image and embed most of the watermark energy there. Such embedding will result in implicit visual masking of the watermark since the Human Visual System (HSV) has a limited ability to detect high frequency signals [41].
2. The wavelet transform‟ s multi-resolution representation of images facilitates progressive transmission of image data and hierarchical decoding of nested watermarks. The DWT provides superior modeling of the HVS. The dyadic frequency decomposition of the wavelet transform resembles the pyramid decomposition of the hypothetical Cortex Transform [14] which models the human visual system. As a result, the DWT allows the different perceptual bands of the HVS to be excited individually.
3. The wavelet transform is computationally efficient. The DWT can be computed in linear fashion.
4. The DWT is very flexible: there are infinitely many wavelet filters. The multitude of possible filters and filter bank configurations enables highly customized processing of individual images. The flexibility in the choice of wavelet filters can also be exploited to increase the security of the watermarking schemes operating in the wavelet domain.

3.8.1 Haar wavelets

The first DWT was invented by the Hungarian mathematician Alfréd Haar. For input represented by a function, pairing, rotate repeated scale: finally resulting in 2n-1 differences and one final sum.

3.8.1.1 Daubechies wavelets

The most commonly used set of discrete wavelet transforms was formulated by the Belgian mathematician Ingrid Daubechies in 1988. The construction is based on the use of recurrence relations to generate progressively finer discrete samplings of an implicit mother wavelet

function; each resolution is twice that of the last scales. In his seminal paper, Daubechies the family of wavelets, the first of which is wavelet defeat. Interest in this field has after the explosion, and Daubechies' original forms of wavelets were developed.

3.8.1.2 The Dual-Tree Complex Wavelet Transform

It is invariant and directionally selective in two and high amplitude. It achieves this with redundancy factor of only 2^d for undecimated is significantly lower than the d-dimensional signals, DWT. The multidimensional (M-D) dual-tree ℂWT is nonseparable but is based on a computationally separable filter banks.

3.8.1.3 Others

Other forms of discrete wavelet transform include the non- or undecimated wavelet transform (where down sampling is omitted), the Newland transform (where an orthonormal basis of wavelets is formed from appropriately constructed top-hat filters in frequency space). Wavelet packet transform belong to the discrete wavelet transform. The complex wavelet transform is another form.

3.8.2 DWT AND FILTER BANKS

3.8.2.1 Multi-Resolution Analysis using Filter Banks

Filters are one of the most widely used signal processing tasks. Walking can be realized by wavelets filters with rescaling. One indication of the resolution measure of the amount of detail information in a sign is determined by the filtering operation, and scale up the sample is determined by and down sampling (sub sampling) operations.

The DWT is computed by successive low pass and high pass filtering of the discrete time- domain signal as shown in figure 3.8.1. This is called the Mallet algorithm or Mallet-tree decomposition. Its significance in the manner it connects the continuous-time mutiresolution to discrete-time filter. In the picture, the signal is denoted by the where n is an integer sequence x[n]. Low pass filter is denoted by G0 while the high pass filter is denoted by H0. At each level, high-pass filters detail information, d[n], is associated with low-pass filter, while scaling function produces coarse approximate, a[n].

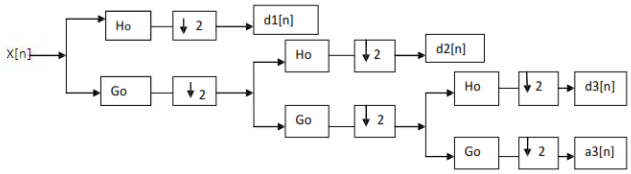


Figure 3.8.2 Three-level wavelet reconstruction tree

Figure 3.8.2 shows the reconstruction of the original signal from the wavelet coefficients. In fact,the reverse reconstruction process of decomposition. Approximation and detail coefficients at every level are two upsampled, passed through low pass and high pass synthesis filters and then added.

This process is continued through the same number of levels as in the decomposition process to obtain and the original signal. The Mallat algorithm works equally good, if a good analysis filter is used. In most Wavelet Transform application, it is necessary that the original signal be synthesized from the wavelet coefficients. To obtain accurate reconstruction analysis and synthesis filters have to satisfy some conditions. Let G (z) and G (z) be the low pass analysis and synthesis filters, respectively and H (z) and H (z) high pass analysis and synthesis filters respectively. The filter has to satisfy the following two conditions as given in[22].

The first condition implies that the reconstruction is aliasing-free and the second condition implies that the amplitude distortion has one of the dimensions. It can be seen that the reconstruction condition does not change if we switch the analysis and synthesis filters.

There are a number of filters which satisfy these conditions. But not all of them give accurate wavelet transforms, especially when filter coefficients are quantized. The accuracy of Wavelet Transform be determined after reconstruction by calculating the Signal to Noise Ratio (SNR) signal. Some applications such as pattern recognition do not need reconstruction and in such applications, the above conditions need not apply.

3.8.3 CLASSIFICATION OF WAVELETS

We can be classify wavelets into two classes:

(a) Orthogonal and

(b) Biorthogonal.

Based on the application can also be made of them.

3.8.3.1 Characteristics of orthogonal wavelet filter banks

The coefficients of orthogonal filters are the actual number. The filter consists of the same length and are not symmetric. Low pass filter, G0 by and the high pass filter, H0 are connected to each other[20,34].

The two filters are alternated flip each other. Flip turn automatically gives double-shift orthogonality between the low pass and high i.e, the scalar product of the filter, the filter pass a shift by two is zero. i.e., Sum(G(k)H[k * 21]) , where these are known as Conjugate Mirror Filters (CMF). Perfect reconstruction is possible with alternating flip.

3.8.3.2 Characteristics of biorthogonal wavelet filter banks

In the case of the biorthogonal wavelet filter, low pass and high pass filter do not have the same length. Low pass filter is always symmetric while the high pass filter could be either symmetric or anti-symmetric. The filter coefficients are then real numbers or integers. Perfect reconstruction, biorthogonal to filter bank has all odd length or all even length filter. Two analysis filters can be symmetric with odd length or one symmetric and the other anti symmetric even with length. In addition, two sets of analysis and synthesis filters should be double. Linear phase filters are biorthogonal the most popular filters for data compression applications.

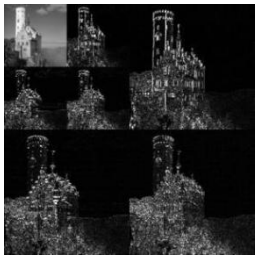


Fig 3.8.3:- An example of the 2D discrete wavelet transform that is used in JPEG2000.

The original image is three large drawings, each describing yield high pass filter local changes in brightness (details) in the original image.It is a low pass filter and produce an approximation image downscaled, the image is high-pass filtered to produce the three smaller Larger images, and low-pass filter for final output approximation image in the upper-left. The first DWT was invented by Hungarian mathematician Alfred defeat. Represented by a list of numbers for each input, storage and sum up the difference just passing wavelet transform the input values can be considered for the pair. Finally differences and resulting in a final amount. The amount pairing process to provide the next scale, rotate repeated. Dual- Tree Complex Wavelet Transform (ℂ WT), with significant additional benefits , discrete wavelet transform (DWT) to the relatively recent growth is almost invariant and directionally selective in two and higher dimensions change.

Fig 3.8.4 A wavelet

The wavelet analysis is done similar to the STFT analysis. To be analyzed signal is multiplied with a wavelet function just as it is multiplied with a window in STFT function, and is then calculated for each change Generated section. However, STFT contrast, the wavelet transform, wavelet function, changes the width of with each spectral component. At higher frequencies wavelet transforms, gives good time resolution and bad frequency resolution, at low frequencies, the wavelet transform gives good frequency resolution and poor time resolution.

Therefore, it's hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT changed. Then it can carry more good hiding watermarking signal and effect.

3.8.4 WAVELET FAMILIES

There are a number of basic functions that can be used as the mother wavelet for Wavelet Transform. Since the mother wavelet produces all wavelet functions used in the transformation through translation and scaling, it determines the characteristics of resulting Wavelet Transform.

Therefore, the details of the particular application should be taken into account and the appropriate mother wavelet should be chosen in order to use the Wavelet Transform.

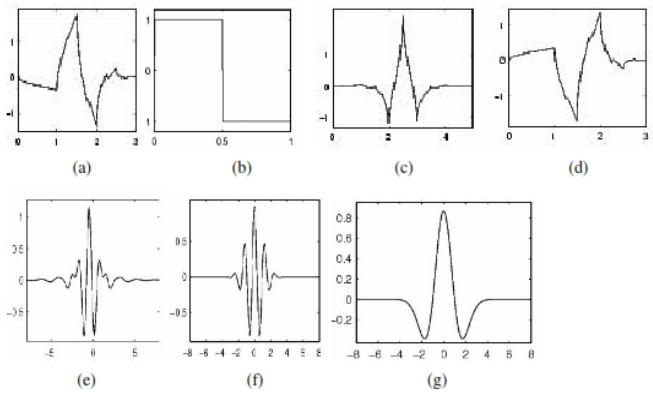


Figure 3.8.5. Wavelet families (a) Haar (b) Daubechies4 (c) Coiflet1 (d) Symlet2 (e) Meyer (f) Morlet (g) Mexican Hat.

Figure 3.8.5 illustrates some of the commonly used wavelet functions. Defeat the oldest and most simple wavelet. Therefore, any discussion of wavelets starts with the Haar wavelet. Daubechies wavelets are the most famous wavelets. They represent the foundations of wavelet signal processing and are used in numerous applications. It is also called as wavelets Maxflat their frequency responses have maximum flatness at frequencies 0 and π. This is very desirable property in some applications. The Haar, Daubechies, Sym lets and Coif lets are compactly supported orthogonal wavelets. These wavelets along with Meyer wavelets are capable of perfect reconstruction. The Meyer, Morlet and the Mexican Hat wavelets are symmetrical in shape. Wavelets are chosen based on their size and their ability to analyze the signal in a particular application.

3.8.4.1 PROPERTIES

We must be able to reconstruct the signal from its wavelet transform. This property involves the resolution of identity, the energy conservation in the time-scale space and the wavelet admissible condition. Any square integral function which has finite energy and satisfies the wavelets admissible condition can be a wavelet. The second basic property is related to the fact that wavelet transform should be a local operator in both time and frequency domains. Hence, the regularity condition is usually imposed on the wavelets. The third basic property is related to the fact that the wavelet transform is a multi resolution signal analysis.

The Haar DWT illustrates the desirable properties of wavelets in general. First, it can be performed in operation, second, it not only captures a notion of frequency content input, test it on a different scale, but also from floating materials, ie times at which frequencies occur. Combination of these two properties make the Fast wavelet transform (FWT) an alternative to the conventional Fast Fourier Transform (FFT).

3.8.4.2 TIME ISSUES

Due to the rate-change operators in filter bank, discrete time-invariant but not Watchtower actually very sensitive to the alignment of the signal in time. To solve the problem of the time- varying wavelet transforms, Mallet and Zhong proposed a new algorithm for wavelet representation of a signal, which is invariant to time shifts. [23] According to this algorithm, which is known as TI-DWT, only the scale parameter is sampled along the dyadic sequence 2^j. (j∈Z) and the wavelet transform is calculated for each point in time. [24][25].

3.8.4.3 APPLICATIONS

The discrete wavelet transform has a huge number of uses in science, engineering, and mathematics and computer science. Mostly, it is used for signal coding, represent a discrete signal in a more often as a prerequisite for data compression is unnecessary. Practical applications can also be found in signal processing of accelerations for gait analysis, [26] in digital communications and so on. [27] [28][29].

Wavelets also find application in speech compression, which reduces transmission time in mobile applications. They denoising, edge detection is feature extraction, speech recognition, echo cancellation etc. They are very promising for real time audio and video compression applications. Wavelets also have many applications in digital communication. The Orthogonal Frequency Division Multiplexing (OFDM) is one of them. Wavelets are also used in bio-imaging. For example, the measured ECG signals the heart, analyzed using wavelets or compressed for storage. The popularity of Wavelet Transform is increasing because of its ability to reduce distortion in the reconstructed signal while retaining all the significant features present in the signal. It is shown that discrete wavelet transform (discrete in scale and shift, and time constant) is successfully implemented as analog filter bank in biomedical signal processing for design of low-power pacemakers and also in ultra-wideband (UWB) wireless communication[30].

3.9 IMAGE SEGMENTATION

The simplest method of image segmentation is called the thresholding method. This method is based on threshold value to convert in to a gray-scale image into a binary image. Optimum threshold separates different objects from background.

Threshold selection in a image segmentation is a very difficult task. It provides important information about image and play important role in segmentation of image. Several different methods for choosing a threshold exist; users can manually choose a threshold value, or a thresholding algorithm can calculate a value automatically, which is called automatic thresholding. A simple method would be to choose the means or median value, the rationale being that if object pixels are brighter than background, they should be even brighter than average. A more sophisticated approach might be to create a histogram of the image pixel intensities and valley point is used as a threshold.

Various threshold selection techniques are well known in the literature.

a) Basic Global Thresholding.
b) Clustering methods
c) Histogram-based method
d) Region growing method

3.9.1 BASIC GLOBAL THRESHOLDING

This method is relatively simple, and does not require much specific knowledge image, and the image is robust against noise following iterative method:

1. An initial threshold is chosen, this can be done randomly or according to any other method desired.
2. The image is segmented into object and background pixels as described above, creating two sets

   (a) $G_1 = f\ m,n : f\ m,n > T$ (Foreground pixels)

   (b) $G_2 = f\ m,n : f\ m,n \leq T$ (Background pixels) ($f\ m,n$ is the value of the pixel located in the m^{th} column, n^{th} row)
3. Compute the average intensity values m_1 and m_2 for the pixels in regions G_1 and G_2 , respectively.
4. A new threshold is created that is the average of m_1 and m_2

$$T' = \frac{m_1 + m_2}{2}$$

5. Go back to step two, now using the new threshold computed in step four, keep repeating until convergence has been reached.

3.9.2 CLUSTERING METHODS

K-means algorithm is an iterative technique that is used to partition an image into K clusters. The basic algorithm is:

1) Pick K cluster centers, either randomly or based on some heuristic.
2) Assign each pixel in the image to the cluster that minimizes the distance between the pixel and the cluster center.
3) Re-compute the cluster centers by averaging all of the pixels in the cluster.
4) Repeat steps 2 and 3 until convergence is attained (e.g. no pixels change clusters).

In this case, distance is the squared or absolute difference between a pixel and a cluster center. The difference is based on pixel color, intensity, texture, and location, or a weighted combination of these factors. K can selected manually, randomly, or by a heuristic method.

3.9.3 HISTOGRAM BASED METHODS

Histogram-based methods are very efficient when compared to other image segmentation methods because they typically require only one pass through the pixels. In this method, a histogram is computed from all of the pixels in image, and the peaks and valleys in the histogram are used to locate the clusters in the image. A refinement of this technique is to recursively apply the histogram-seeking method to clusters in the image in order to divide them into smaller groups. This is repeated with smaller and smaller clusters until no more clusters are formed. One disadvantage of the histogram demand method is that it may be difficult to identify significant peaks and valleys in the image.

3.9.4 REGION GROWING METHODS

Region growing is a procedure that group pixels or sub-region into larger regions based on predefined criteria for growth. The basic approach is to start with a set of "seed" points and from these grow regions by appending to each seed those neighboring pixels that have predefined properties similar to the seed. The first region growing method was the seeded region growing method. This method takes set of seeds as input along with the image. Seed marks each of the items to fragment. Regions are grown iteratively by comparing all unallocated neighboring pixels to the regions. The difference between a intensity of pixel value and the region's mean is used as a measure of equality. The pixel with the smallest difference measured this way is allocated to the respective region. This process continues until all pixels are allocated to a region.

3.9.5 IMAGE SEGMENTATION BASED ON ENTROPY MEASURES

The different entropy measures which are used in this thesis for a comparative study in image segmentation problems. The methodology of image segmentation using the graylevel co-occurrence matrix (C) and Shannon entropy measure is discussed. n this thesis we extend this methodology using the co-occurrence matrix with non-Shannon entropy measures (such as Renyi, Havrda-Charvat, Kapur and Vajda entropy) on color images.

The basic steps of the algorithm are copy here for the sake of convenience:

1) Calculate the GLCM gray level co-occurrence matric $C(m_1,m_2)$, individualy for all possible neighbourhood directions and add them concatively.
2) Calculate $p(m_1,m_2)$,Probability matrix = $C(m_1,m_2)$ / (Total No. of pixels in image).
3) Apply individual entropy function on thus generated probab matrix.
4) Calcuate the minimal regional minima amomg all possible regional minimums in the entropy(t) function. Corrsponding t value is the threshold value

3.9.5.1 DIFFERENT ENTROPY MEASURES:-

A. SHANNON ENTROPY:

Shannon's entropy measure provides an absolute limit on the best possible losslesscompression of a signal under certain constraints [3]. It is defined as:

$$H_s \quad p_{m_1,m_2} \quad = -\sum_{m_1}\sum_{m_2} p_{m_1,m_2} \log p_{m_1,m_2} \quad ,$$

where probabilty distribution associated with the 2-D random variable. In this major project thesis, we have computed the values from the entries of the graylevel co-occurrence matrix[5],[6] of the given image as given by the relation:

$$p_{m_1,m_2} = C_{m_1,m_2} / (MN) \quad ,$$

where , represents the image dimensions along x and y directions respectively. The entropy function for the purpose of the calculation of threshold for image segmentation is then computed from the expression given as:

$$Entropy(t) = -\sum_{m_1=0}^{t}\sum_{m_2=t+1}^{L-1} p_{m_1,m_2} \log p_{m_1,m_2} - \sum_{m_1=t+1}^{L-1}\sum_{m_2=0}^{t} p_{m_1,m_2} \log p_{m_1,m_2}$$

where, L represents the maximum number of gray level present in a particular image and $m_1, m_2 \in [0,1,2,....,L-1]$ $t \in [0,1,2,....,L-2]$.

B. KAPUR ENTROPY:

Kapur's entropy of given order and type defined as [3], [8]:

$$H_k \quad p_{m_1,m_2} \quad = \left(\frac{\sum_{m_1}\sum_{m_2} p^{\alpha+\beta-1}_{m_1,m_2}}{\sum_{m_1}\sum_{m_2} p^{\beta}_{m_1,m_2}} - 1 \right) (2^{1-\alpha} - 1)^{-1} \quad ,$$

and the corresponding entropy function is given by

$$Entropy(t) = \sum_{m_1=0}^{t}\sum_{m_2=t+1}^{L-1} \left(\frac{p^{\alpha+\beta-1}_{m_1,m_2}}{p^{\beta}_{m_1,m_2}} - 1 \right) (2^{1-\alpha} - 1)^{-1}$$

$$+ \sum_{m_1=t+1}^{L-1}\sum_{m_2=0}^{t} \left(\frac{p^{\alpha+\beta-1}_{m_1,m_2}}{p^{\beta}_{m_1,m_2}} - 1 \right) (2^{1-\alpha} - 1)^{-1}$$

.

C. VAJDA ENTROPY:

Vajda entropy measure is a special case of Kapur's entropy where B=1 is taken. It provides the advantage of faster calculations over Kapur's entropy measure and is defined as [3]:

$$H_v \quad p_{m_1,m_2} \quad = \left(\frac{\sum_{m_1}\sum_{m_2} p^{\alpha}_{m_1,m_2}}{\sum_{m_1}\sum_{m_2} p_{m_1,m_2}} - 1 \right) (2^{1-\alpha} - 1)^{-1}$$

and the corresponding entropy function is given by

$$Entropy(t) = \left(\frac{\sum_{m_1=0}^{t}\sum_{m_2=t+1}^{L-1} p^{\alpha}_{m_1,m_2}}{\sum_{m_1=0}^{t}\sum_{m_2=t+1}^{L-1} p_{m_1,m_2}} - 1 \right) (2^{1-\alpha} - 1)^{-1}$$

$$+ \left(\frac{\sum_{m_1=t+1}^{L-1}\sum_{m_2=0}^{t} p^{\alpha}_{m_1,m_2}}{\sum_{m_1=t+1}^{L-1}\sum_{m_2=0}^{t} p_{m_1,m_2}} - 1 \right) (2^{1-\alpha} - 1)^{-1}$$

D. RENYI ENTROPY:

The Rényi entropy which is a generalization of Shannon entropy is one of a family of functionals for quantifying the diversity, uncertainty or randomness of a system. It is defined as [3], [10];

$$H_r(p_{m_1,m_2}) = \frac{\log \sum\sum p_{m_1,m_2}^{\ \alpha}}{1-\alpha}, \alpha \neq 1, \alpha > 0$$

and the corresponding entropy function is given by

$$Entropy(t) = -\sum_{m_1=0}^{t}\sum_{m_2=t+1}^{L-1} \frac{\log\left(\sum\sum\left(p_{m_1,m_2}\right)^{\alpha}\right)}{1-\alpha} - \sum_{m_1=t+1}^{L-1}\sum_{m_2=0}^{t} \frac{\log\left(\sum\sum\left(p_{m_1,m_2}\right)^{\alpha}\right)}{1-\alpha}$$

E. HAVRDA-CHARVAT ENTROPY:

The Havrda–Charvát entropy of degree introduced by Havrda and Charvát and later on modified by Daróczy is often used in statistical physics and is defined as follows [3]:

$$H_{hc}(p_{m_1,m_2}) = \frac{\sum\sum p^{\alpha}_{m_1,m_2} - 1}{2^{1-\alpha} - 1}$$

and the corresponding entropy function is given by

$$Entropy(t) = \frac{1}{2^{1-\alpha}-1}\left(\sum_{m_1=0}^{t}\sum_{m_2=t+1}^{L-1} p^{\alpha}_{m_1,m_2} - 1\right) + \frac{1}{2^{1-\alpha}-1}\left(\sum_{m_1=t+1}^{L-1}\sum_{m_2=0}^{t} p^{\alpha}_{m_1,m_2} - 1\right)$$

The above mentioned entropy functions are calculated for each t for a given image to be segmented using the probabilty distribution which in turn is calculated from its gray and color component level co-occurrence matrix. The numbers of minima points are determined from the entropy function versus gray level and color component level plot. The gray level and color component level corresponding to the smallest minima may be taken as a threshold for image segmentation problems.

Quantitative evaluation of the quality of the enhanced images is also an important issue. Several measures have been proposed in the literature for this purpose [23]. In this thesis, we propose and investigate the use of different entropy measures for quantitative evaluation of the quality of enhanced images. Simulation results of quantitative evaluation of the quality of the enhanced images using different entropy measures are also presented.

IV. EXPERIMENTAL SETUP AND RESULT ANALYSIS

4.1 MATLAB: COMPUTATION TOOL

Image Processing Toolbox provides a comprehensive set of reference standard algorithms, functions, and image processing apps, analysis, visualization, and algorithm development. You can do image enhancement, image deblurring, features detection, noise reduction, image segmentations, geometric transformations, and image registration. Many tools are multithreaded box functions to take advantage of multicore and multiprocessor computers. Supports a variety of image processing toolbox set high Dynamic Range, gigapixel image types, including resolution, embedded ICC profile, and topographic. Visualization functions let you explore an image, examine region of pixels, adjust in contrast, shape or form histogram, and manipulation regions of interest (ROIs). With toolbox algorithms you can restore degraded images, facilities, and measures to detect, analyze shape, textures, and adjust color balance.

4.1.1 Key Features

- Image enhancement, filtering, and deblurring
- Image analysis, including segmentations, morphology, feature extraction, and measurement.
- Geometric transformation and intensity-based image registration methods.
- Image transforming, including FFT, DCT, Radon, and fan-beam projection.
- Workflows for processing, displaying, and navigation arbitrarily large images.
- Image Viewer and Video Viewer apps.
- DICOM files import and export.

4.2 ALGORITHM FOR WATERMARKING USING DWT

Algorithm 1:

a) Embedding Procedure

Step 1. Apply 1-Level DWT on an M*N host image.

Step 2. Divide the HL and LH sub band into non-overlapping blocks of size 2*2 and select blocks in even columns of HL and blocks in odd columns of LH for embedding watermark.

Step 3. For each selected block B(m, n) and a watermark bit w.

Calculate mean value M(m, n) of four coefficients in B(m, n)

$$M(m,n) = \frac{\sum_{i=0}^{1}\sum_{j=0}^{1}(x_{m+i,n+j})}{4}$$

Embed watermark bit w

R := M(m, n) mod 6;

for i := 0 to 1

for j := 0 to 1

if $0 \le R < 3$ then

if w = 1 then xm+i,n+j := xm+i,n+j + (3-R);

if w = 0 then xm+i,n+j := xm+i,n+j - R;

if $3 \le R < 6$ then

if w = 1 then xm+i,n+j := xm+i,n+j + (3-R);

if w = 0 then xm+i,n+j := xm+i,n+j + (6-R);

Step 4. Perform IDWT on the embedded image to obtain a stego image.

b) Extraction Procedure

Step 1. Apply 1-Level DWT on an M*N stego image.

Step 2. Divide the HL and LH subband into non-overlapping blocks of size 2*2 and select blocks in even columns of HL and blocks in odd columns of LH for extracting watermark.

Step 3. For each block B(m, n) . Calculate mean value M(m, n) of four coefficients in B(m, n)

Extract watermark bit w

R := M(m, n) mod 6 ;

if $0 \leq R < 1.5$ then w:= 0;

if $1.5 \leq R < 4.5$ then w:= 1;

if $4.5 \leq R < 6$ then w:= 0;

4.3 VERIFICATION OF THE RESULT

The MSE (Means Square Error) and NC (Normalized Coefficients) values are calculated for the watermarking procedure. And the criterion of good watermarking technique is, lower should be the MSE value and higher should be the NC value. MSE represent the similarity index of original image in comparison to watermarked image. While NSE represent the index that shows the detoriation or damage of extracted watermark when compared to original watermark which was used for hiding in the previous stage. Resemblance of watermarked image or attacked frame to cover (original image). Better is resemblance better is watermarking scheme

(A) PSNR: The Peak-Signal-To-Noise Ratio (PSNR) is used to evaluate deviation of the attack of the watermarked and the original frame video frames and is defined as:

PSNR := 10 Log10 (2552 / MSE) , measured in dB(decibels) units.

Where, MSE (mean squared error) between original and distorted frames (size m x n) is defined. MSE is sum of squared difference between original and watermarked frame.

(B) The Normalized Coefficient (NC): gives a measure of the robustness of watermarking. NC can be ranged between 0 to1: W and W' represent the original and extracted watermark respectively.

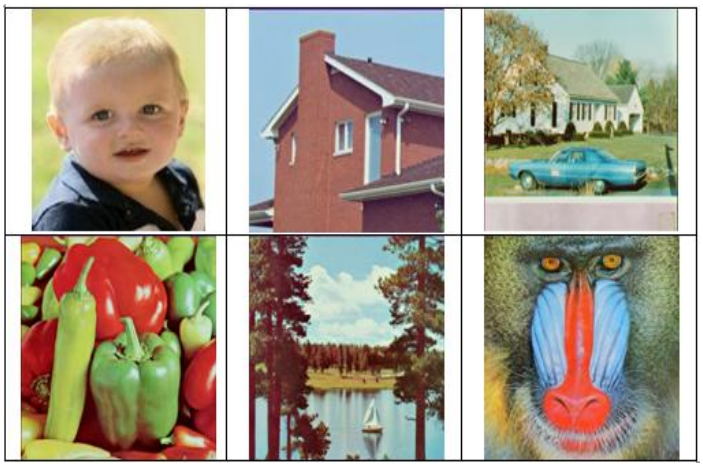
$$NC = \frac{\sum W_{i,j} * \sum W'_{i,j}}{\sqrt{\sum (W_{i,j})^2 * \sum (W'_{i,j})^2}}$$

4.4 RESULTS AND PARAMETERS

Digital watermarking technology is an emerging field in computer science, cryptology, signal processing and communications. The watermarking research is more exciting as it needs collective concepts from all the fields along with Human Psychovisual analysis, Multimedia and Computer Graphics. The watermark may be of visible or invisible type and each has got its own applications.

The experiment is conducted on a 4Ghz I5 processor, with the discussed algorithm simulated in MATLAB2013A running on Windows& Platform.

The Fig.4.4.1 (a) & (b) represents the cover images and watermark images set.



(a) Cover Images

(b) Message / Watermark Images

Fig.4.4.1 Cover and Message Image set

The segmentation result for the message images using Otsu method is depicted as below:

Fig. 4.4.2 The binary conversion of watermark images

The watermarked images resulted from embedding algorithm applied individually on 6 messages is represented by below figure, where binary message bits are embedded into LH and HL band of cover images,

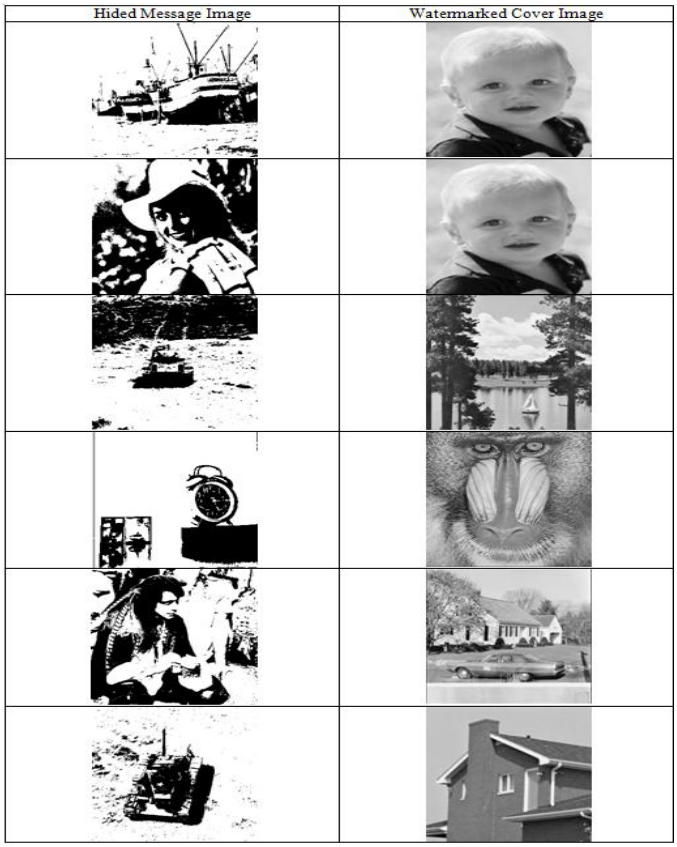


Fig. 4.4.3 The watermarked cover images

Extracted watermarks at user end using Algorithm2 is depicted by below figure:-

Fig 4.4.4 The extracted watermark or message at user-end.

The PSNR and NC values calculated using the watermarked images of fig4.4.3 and extracted watermarks of fig.4.4.4 is tabulated as below:

TABLE: Peak Signal to Noise Ration (PSNR) and Normalized Coefficient (NC)

PSNR	NC
103.1837	0.970634
103.9979	0.9816
104.6117	0.989
104.9977	0.98756
105.1966	0.9865
105.1901	0.98212
104.8139	0.9940657
104.4167	0.9862318
104.0099	0.98907
103.583	0.99049

V. CONCLUSION AND FUTURE SCOPE

As a future scope the concept of Cryptography and Digital Watermarking can be combined to implement more secure Digital Watermarking system. We can use the watermarking technique in the frequency domain for various applications. We can also implement in other spatial domain techniques and cryptography algorithms for most advanced encryption technique to encrypt the messages.

As a future work the video frames can be subject to scene change analysis to embed an independent watermark in the sequence of frames formation of a scene, and repeat this process for all scenes within a video, this can result into invisible digital video embedding. A number of companies, such as the Dig marc Corporation, Sony and IBM have introduced digital watermarking software applications that allow individuals to imbed watermarks within image, audio and video files to be protected them from copyright infringement. Watermarks may be viewed with software and can reveal either a unique identification code that can be traced to the copyright owner or specific information about the copyright owner. Companies are also offering on-line tracking

services so that the copyright owner can see how the owner's materials are used via the Web. These processes will continue to help fight against electronic copyright infringement.

REFERENCES

[1] Yeo and M.M. Yeung,: 'Analysis and synthesis for new digital video application,' icip, International Conference on Image Processing(ICIP97),vol. 1,pp.1,1997.

[2] M. Natarajan, G. Makhdumi1,: 'Safeguarding the Digital Contents: Digital Watermarking,' DESIDOC Journal of Library & Information Technology,vol.29,May 2009,pp. 29-35.

[3] C.I. Podilchuk, E.J. Delp,: 'Digital watermarking: algorithms and applications,' Signal Processing Magazine, vol. 18,pp. 33-46, IEEE, July 2001.

[4] G. Doerr, J.L. Dugelay,: 'Security Pitfalls of Frame-by-Frame Approaches to Video Watermarking,' Signal Processing, IEEE Transactions, vol. 52,pp. 2955-2964, 2004.

[5] M. K. Thakur, V. Saxena, J.P.Gupta,: 'A Performance Analysis of Objective Video Quality Metrics for Digital Video Watermarking,' Computer Science and Information Technology (ICCSIT),2010, 3rd IEEE International Conference, vol. 4,pp. 12-17,2010.

[6] S. Voloshynovskiy, S. Pereira, T. Pun,: ' Watermark attacks,' Erlangen Watermarking Workshop 99, October 1999.

[7] G. Langelaar, I. Setyawan, and R. Lagendijk,: ' Watermarking Digital Image and Video Data: A State of - Art Overview,' IEEE Signal Processing Magazine, vol.,pp. 20-46, Sep. 2000.

[8] F. Hartung and B. Girod ,: ' Watermarking of uncompressed and compressed video,' Signal Processing, 1998,vol. 66, no. 3,pp. 283-301.

[9] J. Lee et al, A survey of watermarking techniques applied to multimedia, IEEE International Symposium on Industrial Electronics, vol. 1,pp. 272-277, 2001.

[10] Cox et al,: ' Digital watermarking: principal and practice,' Morgan Kaufmann,2002.

[11] J. Meng, and S. Chang,: 'Embedding Visible Video Watermarks in the Compressed Domain', International Conference on Image Processing, ICIP 98,Proceedings, vol.1,pp. 474-477, 1998.

[12] Meggs, Philip B.,: ' A History of Graphic Design (Third ed.)', John Wiley & Sons, Inc. pp.58. ISBN 978-0-471-29198-5, 1998.

[13] F. Hartung and M. Kutter,: 'Multimedia watermarking techniques', Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[14] Xiangwei Kong, Yu Liu, Hua jian Liu, Deli Yang,: ' Object watermarks for digital images and video'. Image and Vision Computing. 2004, 22(08): 583-595.

[15] Sourav Bhattacharya, T. Chattopadhay and Arpan Pal,: ' A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC'.

[16] Gwena. El Do. Err, Jean- Luc Dugelay,: ' A guide tour of Video watermarking', Signal Processing: Image Communication 18,pp.263-282.2003.

[17] Vivek Kumar Agarwal,: ' Perceptual watermarking of digital video using the variable temporal length 3D-DCT,' IIT, Kanpur, 2007.

[18] C. Navya Latha, K. Sumanth,: ' Digital Video Watermarking'.

[19] Fernando Perez- Gonzalez and Juan R. Hernandez,: ' A tutorial on Digital Watermarking'.

[20] Y. R. Lin, H. Y. Huang and W. H. Hsu,: 'An embedded watermark technique in video for copyright protection', 18thInternational Conference on Pattern Recognition-ICPR '06,20-24 August 2006,pp. 795-798, Hong Kong.

[21] Nisreen I. Yassin 1, Nancy M. Salem2 and MohamedI. El Adawy National Research Centre, Cario, Egypt,: ' Block Based Video Watermarking Scheme Using Wavelet Transform and Principal Component Analysis,'IJCSI International Journal of Computer Science Issues,vol. 9, Issue 1, no. 3, January 2012.

[22] X. Kang, WenjunZeng, J. Huang,: ' A Multi- band Wavelet Watermarking Scheme'. International Journal of Network Security, vol.no. 2,pp. 121-126,Mar 2008.

[23] T. Khatib, A. Haj, L. Rajab, H. Mohammed,:' A Robust Video Watermarking Alogrithm,: 'Journal of Computer science, vol.4,pp.910-915, 2008.

[24] S.K. Amirgholipour, a. r.. naghsh- Nilchi,: 'Robust Digital Image Watermarking Based on joint DWT-DCT', International Journal of Digital Content Technology and its Applications ,vol.3. Number 2,pp. 42-54, June 2009.

[25] Martin Zlomek, Charles University in Prague, Faculty of Mathematics and Physics, Department of Software and Computer Science Education, Video Watermarking.

[26] M. Chandra, S. Pandey,: ' A DWT Domain Visible Watermarking Techniques for Digital Images', International Conference on Electronics and Information Engineering,pp. v2-421- v2-427, 2010.

[27] Salwa A. K. Mostafa, A. S. Tolba, F. M. Abdelkader, Hisham M. Elhindy,: ' Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform', IJCSNS International Journal of Computer Science and Network Security,vol.9, no.8, August2009.

[28] R. Reyes, C. Cruz, M. Nakano-Miyatake, Member IEEE and H. Perez- Meana, Senior Member IEEE,: 'Digital Video Watermarking in DWT Domain Using Chaotic Mixtures, IEEE Latin America Transactions,vol. 8, no. 3, June2010.

[29] Xiaoli Li, Student Member, IEEE, Sridhar (sri) Krishnan, Senior Member, IEEE, and Ngok-Wah Ma, Senior Member, IEEE, A Wavelet-PCA- Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing, IEEE Transactions on Information Forensics and Security,vol. 5, no. 3, September 2010.

[30] Xiangui Kang, Jiwu Huang, Senior Member, IEEE, Yun Q. Shi, Senior Member, IEEE, and Yan Lin,: 'A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression', IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, August 2003.

[31] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty,Department of Computer Science & Engineering, St Thomas, College of Engineering and Technology, Kolkata, India, : 'Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis, International Journal of Wisdom Based Computing, vol. 1(2), August 2011.

[32] Abdi H. & Williams, L.J., 'Principal Component Analysis', Wiley Interdisciplinary Reviews: Computational Statistics,pp, 433-459, 2010.

[33] Shaw P. J. A.,: 'Multiviariate Statistics for the Environmental Sciences, Holder-Arnold. ISBNO-340-80763-6, 2003.

[34] Barnott, T.P., and R. Preisendorfer,: ' Origins and levels of monthly and seasonal forecast Skill for United States Surface air temperatures determined by canonical correlation analysis.' Monthly weather Review 115, 1987.

[35] Hsu, Daniel, Sham M. Kakade, and Tong Zhang,: 'A Spectral Algorithm for learning hidden markov models,' 2008.

[36] Jolliffe I.T,: 'Principal Component Analysis.' Series in Statistics.

[37] Kriegel, H.P.,: Kroger P. Schubort, E., Zimek, A .: ' A General Framework for Increasing the Robustness of PCA-Based correlation Clustering Algorithm,2008.