Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery

Term Paper (Spring 2003)

Chan Pik Wah
pwchan@cse.cuhk.edu.hk

Supervised by
Prof. Michael R. Lyu

Department of Computer Science and Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong

Abstract

With the rapid growth of the Internet and multimedia systems in distributed environments, it is easier for digital data owners to transfer multimedia documents across the Internet. Therefore, there is an increase in concern over copyright protection of digital content. However, current technology dose not protect their copyright properly. In the early days, encryption and control access techniques were used to protect the ownership of media. They do not protect against unauthorized copying after the media have been successfully transmitted and decrypted. Recently, the watermark techniques are utilized to maintain the copyright. In this paper, we focus on using the digital watermarking techniques to protect digital multimedia intellectual copyright and propose a new algorithm for video watermarking. We present a novel DWT-based blind digital video watermarking scheme with scrambled watermark. Our scheme embeds different parts of a signal watermark into different scenes of a video under the wavelet domain. To increase robustness of the scheme, the watermark is refined by the error correcting code, which is embedded as watermark in the audio channel. The features of our video watermarking algorithm are: (1) it allows blind retrieval of embedded watermark which does not need the original video; (2) the watermark is perceptually invisible; (3) it is robust against the attack of frame dropping, averaging and statistical analysis; (4) it is resistant to lossy compression; and (5) visual-audio watermark is applied. The algorithm design, evaluation, and experimentation of the proposed scheme are described in this paper.

Table of content

Abstract 2
1 Introduction 4
1.1 Motivation 4
1.2 Research objective 5
1.3 Report overview 6
2 Background 7
2.1 Multimedia Security 7
2.2 Cryptography 8
2.3 Digital Watermarking 10
2.4 Literature Review 19
3 Novel Video Watermarking Algorithm.....29
3.1 Video Preprocess..... 31
3.2 Watermark Preprocess 36
3.3 Watermark Embedding 41
3.4 Watermark Detection.....45
4 Experimental Result & Discussion.....48
4.1 Experimental Results.....48
4.2 Discussion 52
5 Future Direction 55
6 Conclusion 56
7 Acknowledgement 56
8 References 57
9 Appendix 64
9.1 Audio Watermark.....64
9.2 Image watermarking in spatial domain 66
9.3 Image watermarking in transformed domain 68
9.4 Video watermarking 69

1 Introduction

The past few years have seen an explosion in the Internet and the use of digital media; digital data owners are now easier to transfer multimedia documents across the Internet. This leads to wide interest of multimedia security and multimedia copyright protection and it has become a great concern to the public in recent years. Industry is marking significant investments to deliver digital audio, image, and video information to consumers and customers. In the early days, encryption and control access techniques were used to protect the ownership of media. Recently, the watermark techniques are utilized to keep the copyrights. In this report, it will focus on using digital watermarking technique to protect the digital multimedia intellectual copyright and a new algorithm of video watermarking is proposed.

1.1 Motivation

Multimedia and network security issues are classically handled through cryptography; however, cryptography ensures confidentiality, authenticity, and integrity only when a message is transmitted through a public channel such as an open network. It does not protect against unauthorized copying after the message has been successfully transmitted. Digital watermarking is an effective way to protect copyright of multimedia data even after its transmission. Watermarking is a concept of embedding a special pattern, *watermark*, into a document so that a given piece of information, such as the owner's or authorized consumer's identity, is indissolubly tied to the data. This information can later prove ownership, identify a misappropriating person, trace the marked document's dissemination through the network, or simply inform users about the rights-holder or the permitted use of the data.

Digital watermarking remains a largely untested field and only very few large industrial consortiums have published requirements against which watermarking algorithms should be tested. Different interesting watermarking approaches have been proposed in these few years, most of them focus on digital image watermarking. As the research area of image watermarking becomes mature, researchers gradually change their target to video watermarking. Most of them based on the techniques of the image watermarking and applied to raw video or compressed video. However, current image watermarking scheme are not capable of adequately protecting video data. Video watermarking introduces

some issues not present in image watermarking. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks, including frame averaging, frame dropping, frame swapping, statistical analysis, etc. Applying a fixed image watermark to each frame in the video leads to problems of maintaining statistical and perceptual invisibility. Furthermore, such an approach is necessarily video independent; as the watermark is fixed while the frame changes. Applying independent watermarks to each frame also presents a problem. Regions in each video frame with little or no motion remain the same frame after frame. Motionless regions may be statistically compared or averaged to remove independent watermarks. In addition, video watermarking schemes must not use the original video during watermark detection as the video usually is in very large size and it is inconvenient to store it twice. We propose a new video watermarking scheme to overcome these problems.

1.2 Research objective

As video copyright protection is strongly concerned, a robust video watermarking scheme is necessary. In order to design a robust, invisible, blind and not removable video watermarking scheme, a survey and investigation has been done on multimedia security issues and multimedia watermarking scheme. Various watermarking scheme schemes are compared and evaluated. Base on these, a new approach and procedures for multimedia security based on watermarking are proposed.

A blind discrete wavelet transform based video watermarking scheme with scrambled watermark is proposed. In this scheme, the watermark is decomposed into different parts and embedded in the frames of different scenes in the video. As identical watermark is used within each motionless scene and independent watermarks are used for successive different scenes, the proposed method is robust against the attack of frame dropping, averaging, swapping, interpolation and lossy compression. The scheme allows blind retrieval of embedded watermark which does not need the original video. The details of the scheme are described in chapter 4.

Experiment has been done on this novel video watermarking scheme to test and show its robustness. Further improvement will be done on it to maximize the strength of this scheme.

Video watermarking is not a standalone technology. It can be associated with different applications to achieve a sophisticated system. This research can be continuous by applying this new developed scheme to specific environment or application and examine its usefulness.

1.3 Report overview

This paper is organized into 6 chapters. The next chapter introduces the issues related to multimedia security and different multimedia watermarking techniques and a literature review of different audio, image and video watermarking scheme is provided. Novel video watermarking scheme is described in chapter 3 and the experimental results are shown in chapter 4. Chapter 5 would state the further improvement of this scheme. Finally, a conclusion would be given in chapter 6.

2 Background

Watermarking technique is a particular embodiment of multimedia security. Let first have an overview of state-of-the-arts technologies in multimedia security and a literature review of current audio, image and video watermarking scheme.

2.1 Multimedia Security

Internet, today, provides an environment where miscreants can easily re-transmit multimedia data on a large scale and without detection. Security has become one of the most significant and challenging problems for spreading new information technology.

The multimedia security requirements are essentially the same as standard information commerce systems:

- Both content provider and the client need to authenticate each other at the beginning of a transaction.
- The content need to be authentic i.e. that it has really been published by the provider and that the content is unaltered.
- The authenticity and integrity requirements should not only be on the content but also on the contract. The content provider should be able to prove that a client has accepted some terms while the client should be able to prove that certain set rights have been acquired.
- Privacy of the client may also be important. Sometimes, it may be desirable that no one, not even the content provider, be able to figure out the identity of the client.

Currently there are numbers of different techniques that researcher target on, including cryptography, digital watermarking, and secure delivery protocol. Different of techniques fall into different research area. The following sessions will have a brief introduction on them.

2.2 Cryptography

The first technology content owners turn to is cryptography. Cryptography is probably the most common method of protecting digital content. It is certainly one of the best developed as a science. The content is encrypted prior to delivery, and a decryption key is provided only to those who have purchased legitimate copies of the content. The encrypted file can then be made available via the Internet, but would be useless to a pirate without appropriate key. In Cryptography, the structure of the message is changed to make it meaningless and unintelligible unless it is decrypted.

There are two kinds of cryptosystems: *symmetric* and *asymmetric*. Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Asymmetric cryptosystems are also called *public key* cryptosystems.

Symmetric cryptosystems have a problem: how do you transport the secret key from the sender to the recipient securely and in a tamperproof fashion? If you could send the secret key securely, then, in theory, you wouldn't need the symmetric cryptosystem in the first place -- because you would simply use that secure channel to send your message. Frequently, trusted couriers are used as a solution to this problem. Another, more efficient and reliable solution is a public key cryptosystem, such as RSA, which is used in the popular security tool

For example, Alice and Bob want to communicate in secret, while Eve wants to eavesdrop. Alice and Bob could be military jets, on-line businesses or just friends trying to have a private conversation. They can't stop Eve listening to their radio signals, so they can keep communication by using cryptography.

One solution is use symmetric cryptosystem as shown in Figure 2.1. Alice and Bob exchange a digital key, so they both know it, but it's otherwise secret. Alice uses this key to encrypt messages she sends, and Bob reconstructs the original messages by decrypting with the same key. The encrypted messages are useless to Eve, who doesn't know the key, and so can't reconstruct the original messages. With a good encryption algorithm, this scheme can work well, but exchanging the key while keeping it secret from Eve is a problem.

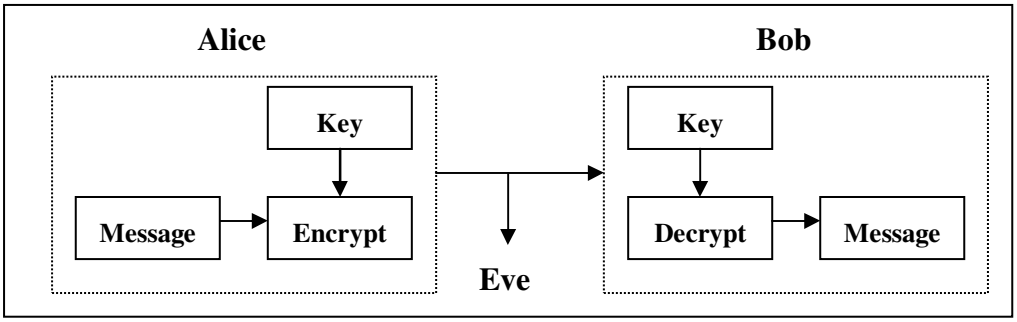


Figure 2.1

Asymmetric cryptosystems (public key encryption, shown in figure 2.2) is different, because it splits the key up into a public key for encryption and a secret key for decryption. It's not possible to determine the secret key from the public key. In the diagram, Bob generates a pair of keys and tells everybody (including Eve) his public key, while only he knows his secret key. Anyone can use Bob's public key to send him an encrypted message, but only Bob knows the secret key to decrypt it. This scheme allows Alice and Bob to communicate in secret without having to meet.

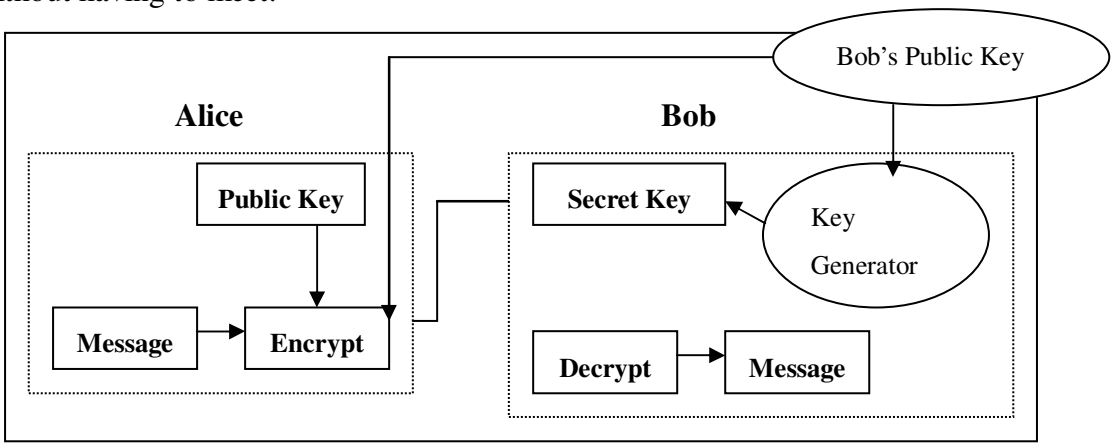


Figure 2.2

Unfortunately, encryption cannot help the owner monitor how a legitimate customer handles the content after decryption. Pirates can actually purchase the product, use the decryption key to obtain an unprotected copy of the content, and then proceed to distribute illegal copies. In order words, cryptography can protect content in transit, but once decrypted, the content has no further protection.

Thus there is a strong need for an alternative or complement to cryptography: a technology that can protect content even after it is decrypted. Watermarking has the potential to fulfill this need because it places information within the content where it is never removed during normal usage. Decryption, re-encryption, compression, digital-to-analog conversion, and file format changes – a watermark can be designed to survive all of these processes. This is going to discuss in the following session.

2.3 Digital watermarking

A Digital Watermark is a digital signal or pattern inserted into a digital data, which can also be referred to as a digital signature. Watermarking is a key process in the protection of copyright ownership of electronic data, including image, videos, audio, etc. The term watermarking comes from the invisible ink used to write secret messages. Watermarking has the additional requirement of robustness. Even if it is known that a watermark exists, as is the case in public watermarking schemes, it should be ideally impossible for an attacker to destroy the embedded watermark. There should be no way of removing the embedded information without rendering the cover object unusable. Generally, watermark has three distinct properties imperceptible, inseparable from the works, and undergoes the same transformation as the work.

A simple watermarking idea is shown in figure 2.3. Watermark is a design of the watermark signal ***W*** to be added to the host signal. The watermark signal, apart from depending on the watermark information ***W',*** may also depend on a key ***K*** and the host data ***I*** into which it is embedded.

$$W = f_0(I, K, W')$$

In watermarking algorithm, stego-image ***I*** is input to the marking algorithm and the algorithm watermark the image with a watermark $\tilde{I} = g(I, \tilde{I}, K)\,\boldsymbol{W}$ and output the watermarked image $\tilde{I}$ with the following equation:

$$I \oplus W \longrightarrow \tilde{I}$$

Verification algorithm is a design of the corresponding extraction method that recovers the watermark information from the signal mixture, perhaps with the help of the key and the original.

$$\tilde{I} = g(I, \tilde{I}, K)$$

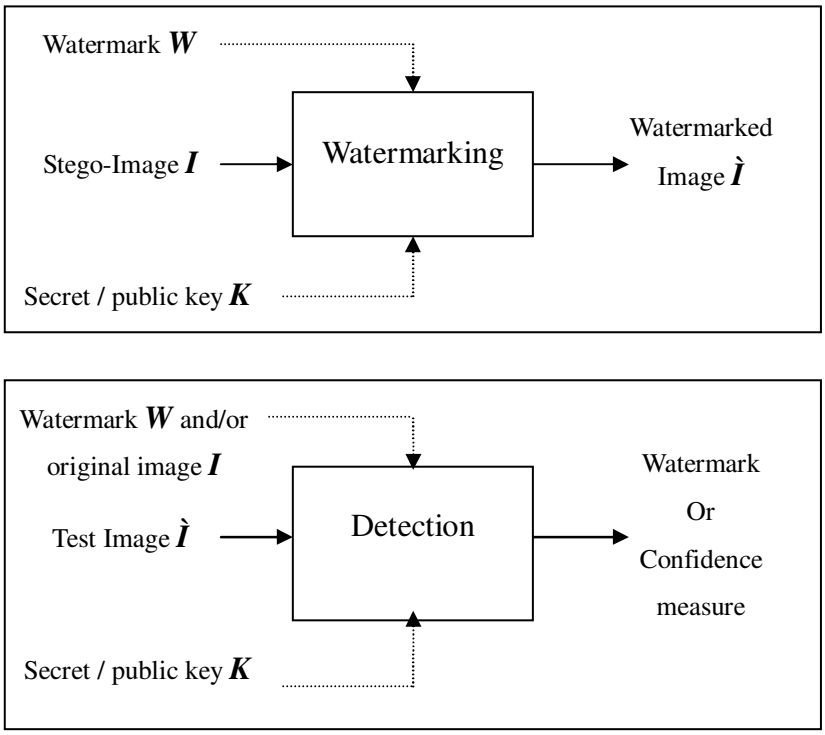

Watermark W
Stego-Image I
Watermarking
Watermarked
Image Ì
Secret / public key K
Watermark W and/or
original image I
Test Image Ì
Detection
Watermark
Or
Confidence
measure
Secret / public key K

Figure 2.3

2.3.1 Requirements of watermarking

Watermarking systems can be characterized by a number of defining properties including embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, robustness, security, cipher and watermark keys, modification and multiple watermark, cost, tamper resistance, unobtrusiveness, ready detection, unambiguous, sensitivity, and scalability. The relative importance of each property is dependent on the requirement of the application and the role the watermark will play. Some of them are common to most practical applications. In this section, such general requirements will be listed and briefly discussed and focus will put on image watermarking and video watermarking.

A general consensus is that embedded watermarks should be invisible, robust, and have high capacity.

Perceptual Transparency

Invisibility is that degree that an embedded watermark remains unnoticeable when a user views the watermarked contents. So far researchers have tried to hide the watermark in such a way that it is impossible to be noticed. However this requirement conflicts with other requirements such as tamper resistance and robustness, especially against lossy compression algorithms. Compression algorithms currently used still permit such a goal to be reachable, however, this may be no more possible in the future, thus to survive the next generation of compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer which is asked to compare the original and the marked version of the document.

Robustness

Robustness is the resilience of an embedded watermark against removal by signal processing. The use of music, images and video signals in digital form, commonly involves many types of distortions, such as lossy compression, or, in the image case, filtering, resizing, contrast enhancement, cropping, rotation and so on. For watermarking to be useful, the mark should be detectable even after such distortions occurred. It is a common opinion [book] that robustness against signal distortion is better achieved if the watermark is placed in perceptually

significant parts of the signal. This depends on the behavior of lossy compression algorithms, which operate by discarding perceptually insignificant data not to affect the quality of the compressed image, audio or video.

Consequently, watermarks hidden among perceptually insignificant data are likely not to survive compression. In the image watermarking case, the resistance to geometric manipulations, such as translation, resizing, rotation and cropping is still an open issue, yet such operations are very common and a solution needs to be found before watermarking techniques are successfully applied to image copyright protection.

Most of Video watermarking scheme base on the techniques of the image watermarking. But video watermarking introduces some issues not present in image watermarking. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks, including frame averaging, frame dropping, frame swapping, statistical analysis, interpolation etc.

Capacity

Capacity is that amount of information that can be expressed by an embedded watermark. Theoretical capacity of embedded watermarks has been examined using information-theoretic concepts. Depending on the application at hand, the watermarking algorithm should allow a predefined number of bits to be hidden. General rules do no exist here, however, in the image case, the possibility of embedding into the image at least 300-400 bits should be granted. In any case, system designers should keep well in mind that the number of bits could be hidden into data is not unlimited; but very often is fairly small.

Low error probability

Even in the absence of attacks or signal distortions, the probability of failing to detect the watermark (false-negative) and of detecting a watermark when, in fact, one does not exist (false-positive), must be very small. Usually, statistically based algorithms have no problem in satisfying this requirement; however such ability must be demonstrated, if watermarking is to be legally credible.

2.3.2 Attacks on watermarking

Watermarking is potential method for protection of ownership right on digital data. Many people try to attack the watermarked data and benefit from it. In this session, overview of the state-of-the-art watermarking attack would be given.

There are different possible attacks on watermark. Here a list of attacks against watermarking system could be judged is proposed, but the different between intentional and unintentional processing is not made.

Removal Attacks

Removal attacks aims at the complete at the watermark information from the watermarked data without cracking the security of the watermarking algorithm. That is, no processing, even prohibitively complex, can recover the remark information from the attacked data. The category include denoising, quantization, compression, multiple watermark and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly.

Jpeg and Mpeg are currently one of the most widely used compressions algorithms for images and video respectively and any watermarking system should be resilient to some degree of compression.

As most of the energy of the image is concentrated at the low frequency band, if the watermark falls into the high frequency regions, the watermark may be distorted by compression.

Geometric Attacks

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is gained. However, the complexity of the required synchronization process might be too great to be practical.

The most common attack is rotation, cropping, scaling, deletion of lines or columns, shearing and other signal processing techniques. For video watermarking, there are more attack, including frame averaging, frame dropping,

frame swapping, statistical analysis, interpolation etc.

Cryptographic Attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermark. One such technique is brute-force search for the embedded secret information.

Protocol Attacks

Protocol attacks at attacking the entire concept of the watermarking application. The main threat addressed in the literature is an attack by pirate who tries to remove the watermark directly. As a consequence, the definition commonly used for robustness includes only resistance to signal manipulation. Craver *et al.* show that this is not enough by exhibiting a "protocol" level attack.

The basic idea is that many schemes provided no intrinsic way of detecting which of two watermarks was added first: the process of marking is often additive, or at least commutative. So if the owner of the document ***D*** encodes a watermark ***W*** and publishes the marked version ***Y***

$$Y = D + W$$

and has no other proof of ownership, a pirate who has registered his watermark as w' can claim that the document is his and that the original unmarked version of it was

$$X = D + W - W'$$

One solution is to time stamp ***D*** when it is creates. Then, the owner with the earliest-dated original is the true owner. A watermark that is a function of a non-invertible (one-way) function of ***D*** would also securely determine ownership. Let ***H*** be the hash of ***D***.

$$H = H(D)$$

A time stamp ***S*** would then be used as the seed for generating ***W. T*** is the time of ***X***'s creation, and ***U*** is the owner name.

$$S = (H, T, U)$$

$$Y = D + W(S)$$

If is computationally infeasible to obtain the correct watermark without knowing ***S***. to successfully steal ***Y***, one must find an ***X*** such that

$$X = Y - W(S)$$

Since ***W (S)*** depends on ***X***, this task is unrealistic.

Another attack is that with traditional watermarking based fingerprinting techniques is that the watermark is inserting solely by seller. A buyer whose watermark has been found in unauthorized copies can claim that the unauthorized copy was created by the seller! Research has proposed a new protocol, which called Buyer-seller watermarking Protocol. The seller dose not get to know the exact watermarked copy the buyer receives. Hence the seller cannot create copies of the original content containing the buyer watermark.

2.3.3 Applications of watermarking

Watermarking can be used in a wide variety of application. In general, if it is useful to associate some additional information with a work, this metadata can be embedded as a watermark.

There are several actual watermarking applications such as Broadcast Monitoring, Owner Identification, Proof of Ownership, Transaction Tracking, Content Authentication, Copy Control, Device Control, Data augmentation, and automatic monitoring of copyrighted material on the Web. The watermark property is dependent on the requirement of the application and the role the watermark will play.

For watermarking for copyright protection, it embeds information about the owner of the object and uses for resolving rightful ownership. It requires a very high level of robustness For fingerprinting for traitor tracking, each object have unique watermark identifying for example the buyer of an object, so copies can be traced. Following session will give examples from different papers.

Examples from pervious researches

Watermarking of Streaming Video for Fingerprinting Application by Fengming Huang *et al*

In this paper, it proposes a real time watermarking paradigm for fingerprinting streaming videos over the Internet or a private video-on-demand network. Their paradigm is based on a 3-tier architecture which runs a proxy server in between the video server and the client's video player. They adopt the proxy approach, as they do not wish to modify the video server/player. The proxy server intercepts the client's request and the video data transmitted by server, embeds a watermark into the video data based on the client/transaction information, and re-encapsulate the video data within the transport packets. This prototype is capable of fingerprinting Mpeg4 streaming video using standard video streaming protocols.

Watercasting: Distributed Watermarking of Multicast Media by Ian Brown *et al*

This is a scheme, which encrypted multicast audiovisual data, and the data may be watermarked by lightweight active network components in the multicast tree.

Every recipient receives a slightly different version of the marked data, allowing those who illegally re-sell that data to be traced. Groups of cheating users or multicast routers can also be traced.

Enabling Hierarchical and Bulk-Distribution for Watermarked Content by Germans Carurini *et al*

These are two mechanisms that allow the preparation and distribution of tagged data in a more scalable way than existing approaches. The first one, called hierarchical tagging, is preferable for online multi-level distribution, where producer and customer are or in direct contract, but intermediate agents provide distribution channels and sales platforms. The second method is well suited to per-produced bulk-media distribution, with only small amount of online information being transferred to each consumer.

Digital Right Management and Watermarking of Multimedia Content for M-commerce application by Fengming Huang *et al*

With the increasing popularity of wireless data service, especially in high-rate mobile networks like GPRS and UMTS, mobile e-commerce is also becoming increasingly important. An important ingredient of m-commerce is wireless media download and streaming. Unlike in the fixed Internet, mobile terminals provided much more reliable information about the identity of the user. The mobile terminal serial number and, even more, the phone number or identity are usually tightly bound to an individual user known to the network provider. This information can be used for watermarking and data identification purposes, thus avoiding a weakness of Internet digital right management systems.

2.4 Literature Review

Though watermarking is a recent field of research, many techniques have already been proposed both in the academic as well as in the industry fields. Various techniques have applied in watermarking algorithm and they can be classified into different type from the point of view of the offered functionality's. In this paper, we have a brief review of the current discussion of audio, image and video watermarking schemes.

2.4.1 Introduction

A digital document may be authenticated with what is known as a digital watermark. A watermark is a secret code or image incorporated into an original content which acts to verify both the owner and content of the document. The use of perceptually invisible watermark is one of image authentication. A watermarking algorithm consists of three parts: watermark, marking algorithm and verification algorithm.

Each owner has a unique watermark. The marking algorithm incorporates the watermark into the image or video. The verification algorithm authenticates the content, determining both the owner and the integrity of the content.

A variety of imperceptible watermarking schemes have been proposed over the last few years. The state-of-the-arts algorithm would be introduced in this chapter and the table listing their details, their advantages and disadvantages is attached in the appendix.

2.4.2 Audio watermarking

Comparing with the development of digital video and image watermarking, digital audio watermarking provides a special challenge because (1) data hiding must not be audible since otherwise it will mask the original audio signal it will be easily tampered with and removed, (2) the human auditory system (HAS) operates over a wide dynamic range between 20 Hz to 20 kHz, making it difficult to embed outside this rage, (3) there is a limited area of embedding the data. Currently, audio watermarking techniques mainly focus on four aspects: low bit coding, phase coding, spread spectrum-based coding and echo hiding.

Low-Bit Coding — The basic idea in low-but coding techniques is to embed the watermark in an audio signal by replacing the least significant bit of each sampling point by a coded binary string corresponding to the watermark

Phase Coding –A hidden datum is represented by a particular phase or phase change in the phase spectral. Phase coding is one of the most effective coding schemes in term of the signal-to-noise ratio because experiments indicate that listeners might not hear any difference caused by a smooth phase shift, even though the signal patterns may change dramatically.

Spread Spectrum – The basic spread spectrum technique is designed to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible. It turns out that may spread spectrum techniques adapt well to data hiding in audio signals.

Echo Hiding – Echo hiding is a method for embedding information into an audio signal. It seeks to do so in a robust fashion, while not perceivably degrading the original signal. Echo hiding embeds data by introducing an echo. The value of a hidden datum corresponds to the time delay of the echo and its amplitude. The echo delays are selected to be less than the detectable hearing limited

Here is some developed audio watermarking schemes that applied the above techniques.

Affine Resistant Digital Audio Watermarking Using Template Matching

This is an approach for embedding a digital watermark inaudibly into an audio clip, in the time domain, according to the difference between two half blocks of each block. The proposed scheme does not require any host-related information for watermark extraction. The embedded watermark is robust to common audio signal manipulations, such as MP3 compression, time shifting, cropping, time scaling, D/A A/D conversion, insertion, deletion, re-sampling, re-quantization and filtering.

Two kinds of information are hidden in the audio: the owner's information and a synchronization template. The owner's information is a binary image provided by the copyright owner, which can be words, numbers, a signature, a personal seal

or an organization's logo. The synchronization template is generated by a random number generator controlled by a secret key and is used for synchronizing the signal skew caused by time shifting, cropping and time scaling attacks. The two kinds of information are combined together and dispersed by another secret key before embedding. The proposed technique can be applied to automatically search for a protected audio from an audio database (or from the World Wide Web) by first matching the synchronization template, and then show the owner's information if it is claimed to have been watermarked.

Digital Audio Watermarking Based-on Multiple-Bit Hopping and Human Auditory System

To optimally balance in-audibility and robustness when embedding and extracting watermarks, the embedding scheme is high related to audio content by making use of the properties of human auditory system and multiple-bit hopping technique. The watermark embedding design is based on audio content and HAS. With content-adaptive embedding scheme, the embedding parameter for setting up the embedding process will vary with the content of the audio signal..

In broad term, this techniques involves segmenting an audio signal into frames in time domai, classifying the rames as belongs to one of several known classes, ad then encoding each frame with an appropriate embeddin scheme. To echace the robustnes and taper-resistace of the embedded watermark, a multiple-bit hopping technique is employed. Instead of embedding one bit into an audio frame, multiple bits with different time delay can be embedded into eac audio sub-frame

Muteness-Based Audio Watermarking Technique

This audio watermarking approach bears certain similarities with the open space text watermarking. The audio counterparts of text spaces are periods of silence. In audio signal, a mute period offers the following advantages: (1) a mute period is an integral part of any audio signal. It cannot be omitted since it represents and integral part of the studio signal. (2) It occurs randomly in audio signal, which is generated by the music process. (3) A mute period represents a real time interval that will not be decreased when compressed.

The audio watermarking technique presented in this scheme is a muteness-based, which offers the following features: (1) It extends the mute periods in an audio

signal without any perceptual difference to the average human auditory system. (2) The extension of mute periods carries the same amplitude so it will blend with the original and will not attract any attention. (3) It dose not require the original signal to extract the watermark.

2.4.3 Image watermarking

One early watermarking method obtains a checksum of the image data, then embeds the checksum into the LSB of randomly chosen pixels. Others add a modified maximal length linear shift register sequence to the pixel data. They identify the watermark by using spatial cross correlation function of the modified sequence and part of the watermarked image. Watermarks also can modify the image's spectral or transform coefficients directly. These algorithms often modulate DCT, DFT or DWT coefficients according to a sequence known only to the owner. Watermarking techniques may be image dependent. These techniques increase the security level of the watermark in the image while maintaining the imperceptibility of the mark. One method incorporate feature from most of the above techniques. Its wavelet implementation lends itself to watermarking data rate-scalable video. Visible watermarks also exist; IBM has developed a proprietary visible watermark to protect images that are part of the digital Vatican library project. The watermarking itself is only a small part of any controlled access and distribution scheme; a method for secure distribution would combine encryption with digital watermarking. The following part introduce numbers of current proposed image watermarking schemes.

2.4.3.1 Spatial domain

Spatial method analyzes a data from the spatial point of view. A watermarking method based on the spatial domain, scatters information to be embedded to make the information hardly detectable. It uses minor change of the value of pixel directly. This technique has an advantage which is strong to cropping and translation, but weak to attack like noise and compression. For spatial domain techniques, different approaches have be proposed, checksum techniques, two-dimensional spatial watermark and spread spectrum approach.

Checksum Technique

This watermark is formed from the checksum value of the seven most significant

bits of all pixels. A checksum is the modulo-2 addition of a sequence of fixed-length binary words; it is a special type of hash function. The final checksum is fifty-six bits. The technique then randomly chooses the locations of the pixels that are to contain one bit of the checksum. The pixel locations of the checksum, together with the checksum itself, form the watermark, *W*. The last bit of each chosen pixel is changed (if necessary) to equal the corresponding checksum bit. *W* must be kept secret. To verify this watermark the checksum of a test image *Z* is obtained, and compared to the ideal version in W. The advantages of this technique are these; first, embedding *W* only changes half of the pixels covered by *W*., this is not only reduces visual distortion but also increases security. Second, an image may hold many *W* as long as they do not overlap. The disadvantage is that this watermarking method is fragile. Any change to either the image data itself or the embedded checksum can cause the verification procedure to fail. An attacker could remove the entire watermark by replacing the LSB plane.

Basic M-sequence Approach

This watermark is based on using a modified m-sequence. A linear feedback shift register with n stages can form pseudorandom binary sequences with periods as large as *2n - 1*. M-sequences achieve this maximum period, and have a very desirable autocorrelation and randomness properties. Two types of sequences may be formed from an m-sequence *unipolar* and *bipolar*. This watermark is robust to small amounts of noise introduced in the image. Multiple watermarks can overlap; successive watermarks treat the previously watermarked image as a new *X*. However, the last two bit planes could be removed and replaced. An attacker can deduce *W* if *2n* consecutive bits in *W* are known. This method does not specifically protect the DC value of the pixels covered by an individual block.

Secure Spread Spectrum Watermarking for Multimedia

This scheme inserts a watermark into the spectral components of the data using techniques analogous to spread spectrum communication, hiding a narrow band signal in a wideband channel that is the data. The watermark is difficult for an attacker to remove; even when several individuals conspire together with independently watermarked copies of the data. It is also robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital

conversion, resampling, and requantization, including dithering and recompression and rotation, translation, cropping and scaling. The same digital watermarking algorithm can be applied to all three media under consideration with only minor modifications, making it especially appropriate for multimedia product. Retrieval of the watermark unambiguously identifies the owner, and the watermark can be constructing to make counterfeiting almost impossible.

2.4.3.2 Frequency Domain

Generally DCT, FFT and wavelet transform are used as the methods of data transformation. In these methods, a watermark that one wishes to embed inn distributed in overall domain of an original data, and the watermark, if it is once embedded, is hardly to be deleted. For transformed domain techniques, they have Hierarchical watermarking with Discrete Cosine Transform, sub-band watermarking techniques, modifying coefficient value in wavelet domain or after Discrete Fourier Transform.

Hierarchical Watermarking Depending on Local Constraints

In this paper it proposes a new watermarking technique where the watermark is embedded according to two keys. The first key is used to embed a code bit in a block of pixels. The second is used to generate the whole sequence of code bits. The watermark is embedded in spatial domain by adding or subtracting a random digital pattern to the given image signal depends on the local energy distribution. The embedding depth level depends on the spectral density distribution of DCT coefficients and on the JPEG quantization table and inserts the watermark in the low frequency component. The label consists of a set of bits which are embedded locally in a rectangular set of blocks and it is repeated over the entire image. After detecting individual bits, the retrieve label is verified by performing a XOR operation to the watermark code.

Watermark to Wavelet Transformed image

Watermarking and compression algorithm are jointly considered. Present the watermarking algorithm in the wavelet domain without compression. The watermark algorithm is integrated within a zero-tree type DWT. It is robust if engraved at high compression ratio. (Robust watermark must be put in the most significant components.) It is also transparency. There is only little difference

brought by signature engraving and difference smaller when compression ratio is higher.

A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image

This scheme first inserts the watermark into the middle-frequency range. Filter banks are very important and have to be saved for the watermark embedding and the middle-frequency band to insert the watermark is also chosen the coefficient in that band of the image is replace by the watermark. This achieve both spatial and frequency localization. It is both perceptual invisibility and robustness to compression. It is robustness to noise, image processing techniques, median filter, geometric transform.

2.4.3.3 Hybrid Watermarking

Watermark not only can be embedded into one domain, they can be inserted into both spatial and frequency domain or apply different techniques onto one watermark, i.e. the hybrid techniques.

A Hybrid Watermark for Tamper Detection in Digital Image

A hybrid image authentication watermark obtained as a combination of fragile and a robust watermark is presented. The fragile watermark has good localization and security properties but cannot be used to distinguish malicious changes from innocent image processing operations. The hybrid watermark can be used to accurately pinpoint changes as well as distinguish malicious tamper from innocent operations. The authentication can be done without accessing any information about the original image.

Effective Hybrid Digital Watermarking Scheme Using Direct Sequence-Spread Spectrum Method

The proposed scheme is that produced watermark image using personal ID of copyrighter is inserted into the original images, and the watermark image is detected from the watermarked image. That is an extension of the spread-spectrum watermarking which combine key with logo method. Binary image is used as watermark image, and degradation of image quality between

original image and watermarked image in order to confirm required invisibility in watermark system and watermark robustness to protect a attack from the outside are analyzed using the values of PSNR and recovered rate of the watermark image.

2.4.4 Video Watermarking

Most of the proposed video watermarking scheme based on the techniques of the image watermarking and applied to raw video or the compressed video. As some issue in video watermarking is not present in image watermarking, such as video object and redundancy of the large amount video data, researchers have make use of those characteristics to develop different schemes,. The details of some schemes would be discussed in the following section.

A Robust Watermarking Approach for Raw Video

This approach first extracts the brightness of the to-be-marked frame, computing its full-frame DFT and then taking the magnitude of the coefficients. The watermark is composed of two alphanumerical strings. The DFT coefficient is altered, then IDFT. Only the first frame of each GOP is watermarked, which was composed of twelve frames, leaving the other ones uncorrupted. It is good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping. Decide to watermark one or more frames in GOP, a trade-off between time spent for marking and the degree of robustness needed for the sequence can be achieve

A New Wavelet-Based Digital Watermarking for Video

This paper proposes a method of embedding a digital watermark image in video. In the watermarking, the decomposed watermark image with different resolution is embedding in the corresponding resolution of the decomposed video by means of multiresolution signal decomposing. The proposed method is robust against the attack of frame dropping, averaging and lossy compression.

Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation

The watermark consists of static and dynamic temporal components that are generated from a temporal wavelet transform of the video scenes. To generate the watermark, the resulting wavelet coefficient frames are modified by a perceptually shaped pseudo-random sequence representing the author. The noise-like watermark is statically undetectable to thwart unauthorized removal. Furthermore, the author representation resolves the deadlock problem. The multiresolution watermark may be detected on single frames without knowledge of the location of the frames in the video scene.

Combating Geometrical Attacks in a DWT Based Blind Video Watermarking System.

This scheme is a high capacity blind video watermarking system invariant to geometrical attacks such as shift, rotation, scaling and cropping. A spatial domain reference watermark is used to obtain invariance to geometric attacks by employing image registration techniques to determine and invert the attacks. A second, high capacity watermark, which carries the data payload, is embedded in the wavelet domain according to a human visual system model.

Scrambling Technique for Video Object Watermarking Resisting to Mpeg-4

This paper presents a so-called scrambling technique which allows to adapt any classical spread spectrum watermarking scheme operating in the spatial domain to the Mpeg-4 requirements concerning VO manipulation. This technique can be easily added to the embedding and detection schemes without changing the watermarking algorithm. It modifies some predefined pairs of quantized DCT coefficient in the luminance block of pseudo-randomly selected MBs. It is based on spread-spectrum techniques. Dividing the image into blocks of equal size, them binary sequence is generated using secret key, and then adds to the image. Special decomposition of mpeg-4 include the fact that VO have significant value Watermark information has to present in each VO

Object-Based Transparent Video Watermarking

It presents a watermarking procedure to embed copyright protection into video sequences. To address issues associated with video motion and redundancy, individual watermarks are created for objects within the video. Each watermark is created by shaping an author and video dependent pseudo-random sequence according to the perceptual masking characteristics of the video. As a result, the watermark adapts to each video to ensure invisibility and robustness. Furthermore, the noise like watermark is statistically undetectable to prevent unauthorized removal.

Video Object-based Watermarking: A Rotation and Flipping Resilient Scheme

Video object is very important concept in Mpeg4 standard. Video object may be purposely cut and pasted for illegal use. In this paper, a robust watermarking scheme foe video object protection is proposed. For each segmented video object, a watermark is embedded by a new technology designed based in the concept of communication with side information. To solve the asynchronous problem caused by object placement, it proposes to use eigenvectors of a video object for synchronization of rotation and flipping.

Direct Sequence Watermarking for Digital Video using m-frames

This scheme applies a direct sequence spread spectrum model to the watermarking of the digital video. First, video signal is modeled as a sequence of bit planes arranged along the time axis. Watermarking of this sequence is a two layer operation. A controlling m-sequence first establishes a pseudorandom order in the bit plane stream for later watermarking. Watermark, defined as m-frames, supplant the tagged bit planes. Moreover, attempts in corrupting the image to destroy the watermark render the video useless before damaging the seal itself. The watermarked video is also robust to video editing attempts such as subsampling, frame reordering etc. The watermark is also identifiable from very short segment of video. Individual frames extracted from the video will also contain the copyright information.

3 New Video Watermarking Algorithm

With the rapid growth of the Internet and multimedia systems in distributed environments, it is easier for digital data owners to transfer multimedia documents across the Internet. Therefore, there is an increase in concern over copyright protection of digital content. In the early days, encryption and control access techniques were used to protect the ownership of media. They do not protect against unauthorized copying after the media have been successfully transmitted and decrypted. Recently, the watermark techniques are utilized to maintain the copyright. In this paper, we focus on using the digital watermarking techniques to protect digital multimedia intellectual copyright and propose a new algorithm for video watermarking.

Video watermarking introduces some issues not present in image watermarking. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks, including frame averaging, frame dropping, frame swapping, statistical analysis, etc. Applying a fixed image watermark to each frame in the video leads to problems of maintaining statistical and perceptual invisibility. Furthermore, such an approach is necessarily video independent; as the watermark is fixed while the frame changes. Applying independent watermarks to each frame also presents a problem. Regions in each video frame with little or no motion remain the same frame after frame. Motionless regions may be statistically compared or averaged to remove independent watermarks. In video, apart from the video channel, is also has a audio channel. It can be used to increase the robustness of the video watermarking scheme. In addition, video watermarking schemes must not use the original video during watermark detection as the video usually is in very large size and it is inconvenient to store it twice.

In order to overcome these problems, a new approach and procedures for multimedia security based on watermarking is proposed. Figure 3.1 shows an overview of the scheme, which we describe in detail in the following sections.

Audio-aided DWT-based Video Watermarking Scheme with Scramble Watermark is proposed. The watermark scheme we propose is based on Discrete Wavelet Transform. In our scheme, a watermark is decomposed into different parts and they are embedded in corresponding frames of different

scenes in the original video. An identical watermark is used within each motionless scene, independent watermarks are used for successive but different scenes, and these watermarks are embedded in the middle frequency sub-band of the frames. With this, the proposed method is robust against the attack of frame dropping, averaging, swapping, and lossy compression. The error correcting code for the watermark is extracted and embedded in the audio channel as audio watermark. In detection phase, it will be used to refine the watermark extracted from the video channel. The scheme consists of different parts, including: video preprocess, watermark preprocess, watermark embedding, and watermark detection. The scenario of the scheme would be described in this chapter.

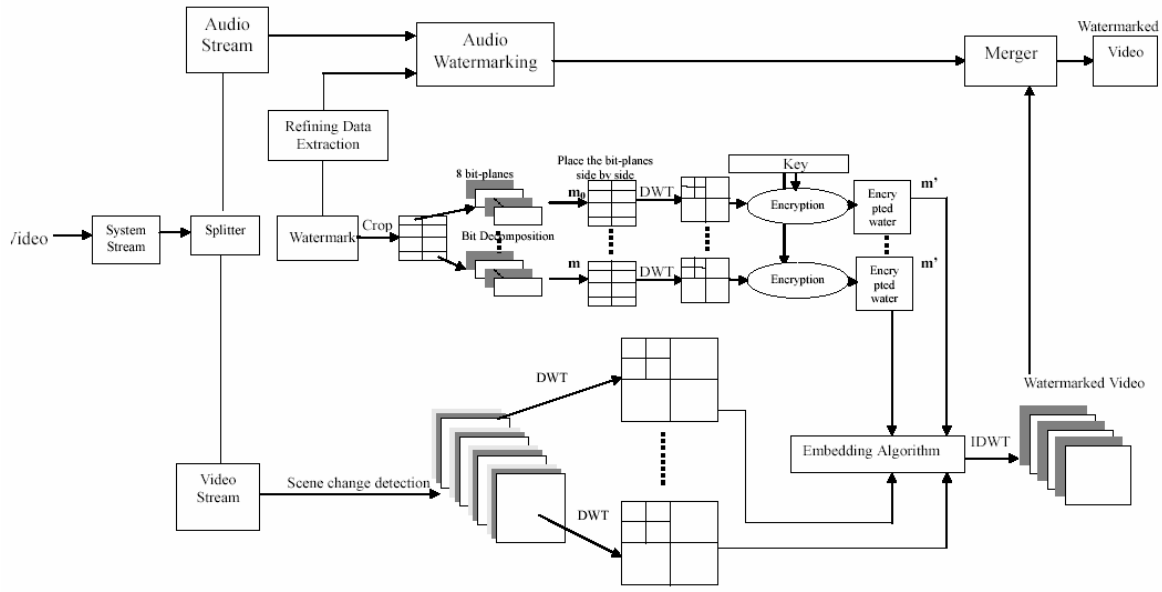


Figure 3.1 Overview of the watermarking process

3.1 Video preprocess

Video preprocess consists of 3 parts: splitter, discrete wavelet transform and scene change detection and they are described in detail in this section.

3.1.1 Splitter

The input video is split into video stream and audio stream and the watermarks are embedded in each channel separately. After embedding, two streams will be merged and output the watermarked video

3.1.2 Discrete Wavelet Transform

This watermark scheme is based on 4 levels Discrete Wavelet Transform (DWT).

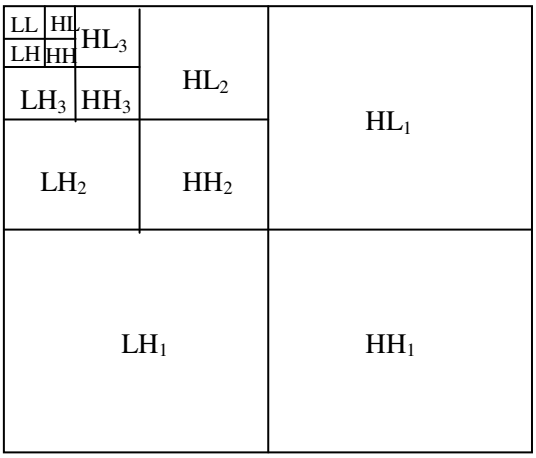


Figure 3.2

All frames are transformed to wavelet domain with 4 levels. A 4 level DWT diagram is shown in Figure 3.2. DWT is a kind of transform that convert a signal into coarse and detail signals by “averaging and differencing” on the coefficients. Wavelet transform breaks down the signal into a coarse coefficient (DC component) and a hierarchical of detail coefficients (AC components).
Wavelet transform is a sequence of low pass and high pass filtering, which has shown detail in figure 3.3. Filtered signal is down sampled by 2 at each level and filtering is recursively applied on the lower passed signal

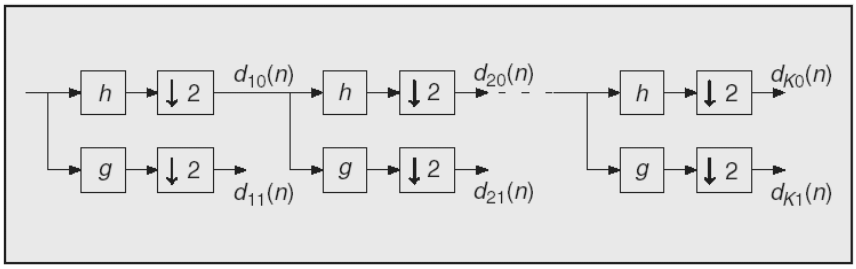


Figure 3.3

h - low pass filter, *g* - high pass filter, d_{ij} detail coefficients

2D Separable wavelets allow 2D DWT to be done by 2 passes of 1D DWT. Detail is shown in Figure 3.4.

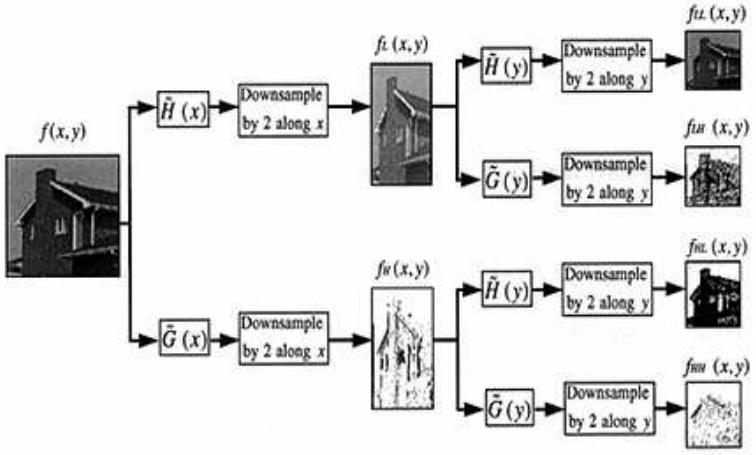


Figure 3.4

Figure 3.5

Next, the low and high pass filtering is applied to the low-passed image (i.e. ***fLL(x,y)***). The process repeats 4 times, until it obtain an image with structure in

figure3.2, and the result is shown in figure 3.5. Later the DWT coefficient would be modified according to the watermark.

DWT is chose as it is more computationally efficient than the sinusoidal based discrete transform. The speed is faster than DCT and DFT as only sum or different of the pixel have to be calculated.
With DWT, it takes lots of advantage to resist the attacks on the watermarked frames:

- Achieving both spatial and frequency localization
- Achieve both perceptual invisibility and robustness to compression.
- Robustness to noise, image processing techniques, and median filter (which can be consider as a case of pixel permutation, it course destroys the synchronization.).
- Resist to geometric transform (lots of existing algorithm may not survive)
- Resilience to counterfeit attempts.

The scheme is robust against format conversions because the watermark is inserted before compression. Otherwise, the drawback of the techniques is that, since the code is directly embedded into the compressed stream such as mpeg-4, the copyright information is lost if the video file is converted to a different compression standard, such as mpeg-2

Apart from DWT, video has to be divided into different scene before embedding the watermark into the video stream. So, scene change detection will be performed and the details are described in the next section.

3.1.3 Scene Change Detection

Scene changes are detected from the video by applying the histogram difference method on the video stream. Independent watermarks are embedded in frames of different scenes. Within a motionless scene, an identical watermark is used for each frame. As shown in figure 3.6, watermark m_1 is used for the first scene (first nine frames). When there is scene change at 10th frame, another watermark m_3 is used for the next scene (10th to 20th frame). The watermark for each scene is chosen with pseudo-random permutation.

$m_0, m_1 ...$ are different part a single watermark. The watermark is preprocessed and cropped into $m_0, m_1 ...$ and the detail of the watermark preprocess is described in the next session.

Histogram difference method is used for scene change detection. Each frame is coded in 24-bit image, eight bits for each color (red R, green G, blue B). Consequently, each pixel is checked and classified into different classes. For efficiency purpose, only the most significant two bits for each color are considered. Then, the total difference of the whole histogram (H) calculated, which is:

$$H = \sum_{i,j=0}^{63} [P_a(i) - P_b(j)]^2$$

If H > threshold (T), we consider there is a scene change.

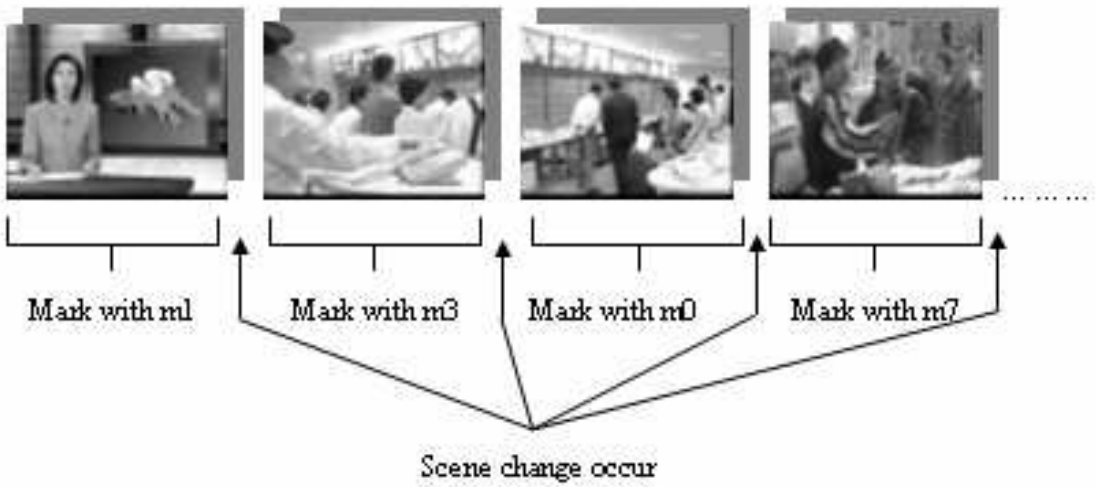


Figure 3.6

As each scene is embedded with same watermark, it can prevent attackers from removing the watermark by frame dropping. If they try to remove the frames with same watermark, they need to remove the whole trunk of frame (i.e. the whole scene) and this would lead to significant damage to the video.

Identical watermark is used within a scene can also prevent attackers from taking advantage of motionless regions in successive frames to remove the watermark by comparing and averaging the frames statistically. Moreover, similar frames use same watermark make the scheme resist to statically analysis of the video to get the watermark.

Independent watermark used for successive different scene can prevent attackers from colluding with frames from completely different scenes to extract the watermark.

3.2 Watermark Preprocess

Watermark is processed before it is embedded in the video. Two watermarks are embedded in the video. (one in the video channel, one in the audio channel).

3.2.1 Video watermark

The watermark is cropped in small images, which use as different independent watermarks which mention in the last section, shown as figure 3.7. In the detection phase, the watermark is reconstructed with these small images.

The watermark must be a 256-grey-level image, so 8 bits can represent each pixel. It is first scaled to a particular size with the following equation

$$2^n \le m \qquad \textbf{, n>0}$$

$$p + q = n \qquad \textbf{, p and q > 0}$$

where m is number of scene changes and n, p, q are integers. And the size of the watermark should be

$$64 * 2^p \; X \; 64 * 2^q$$

Then the watermark is divided into $\mathbf{2^n}$ small images with size 64 X 64. Figure 3.7 shows the procedure of watermark preprocess with
m = 10, n = 3, p = 1, and q = 2.

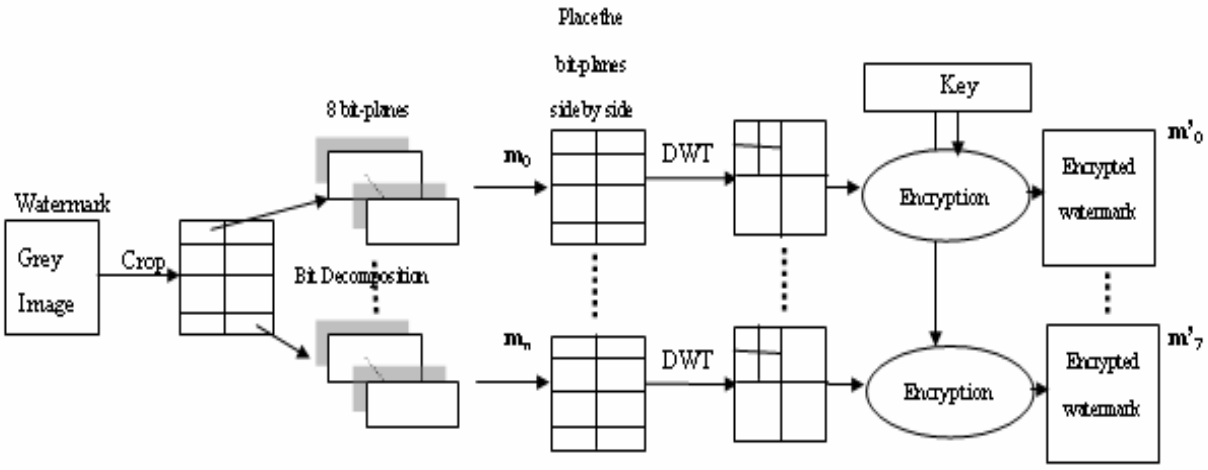
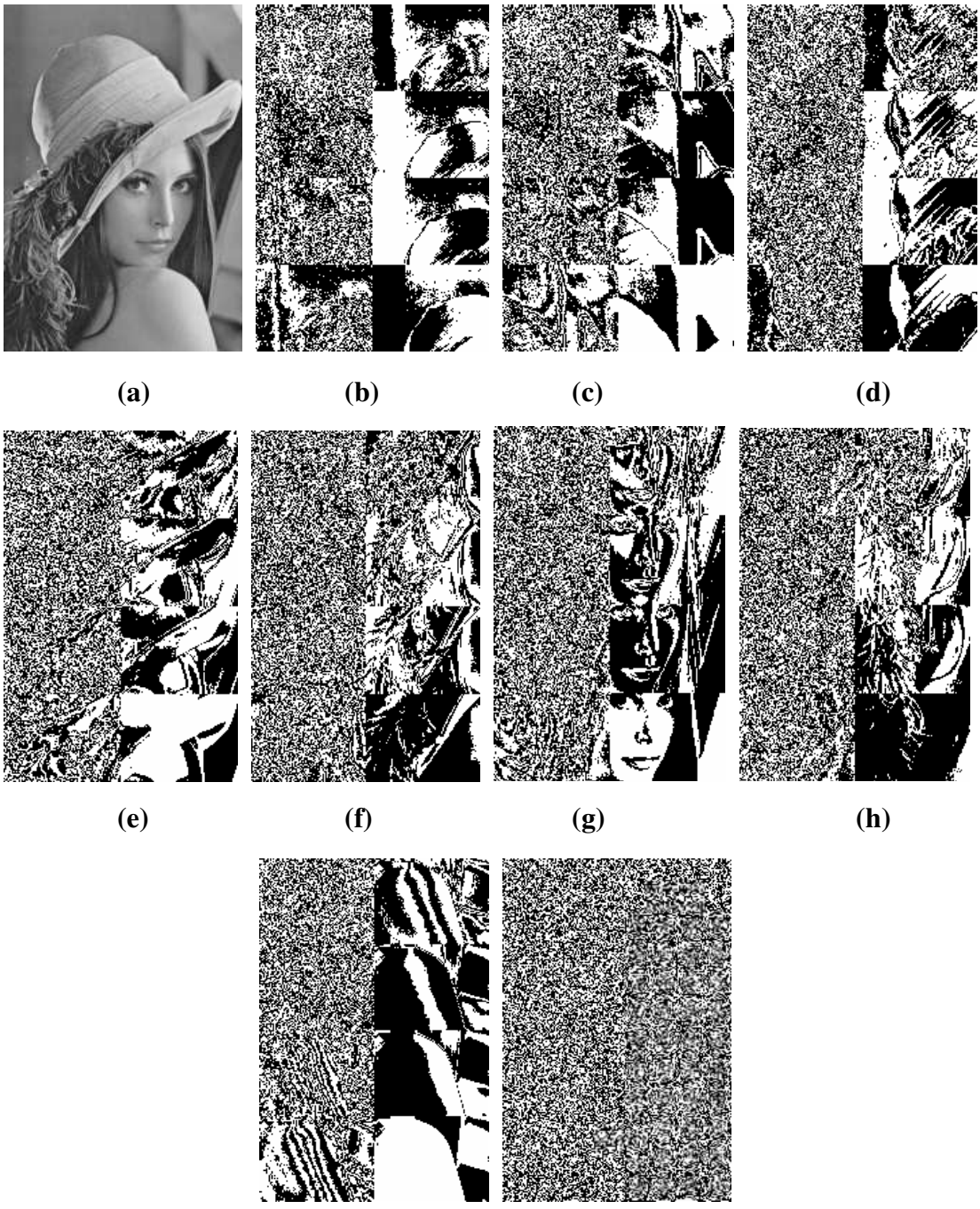


Figure 3.7 Preprocessing the watermark



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j)

Figure 3.8 (a) Original watermark (b-i) preprocessed watermark m_0-m_7 (j) encrypted watermark m'_0

Watermark is cropped into pieces and embedded in different frame can make the watermarks resistant to attacks by frame averaging. As the watermark is scramble, it is hard for the attackers to reconstruct the watermark without the knowledge. It prevents unauthorized embedding of watermark and harder for removing the watermark and increases the watermark security.

In the next step, each small image is decomposed into 8 bit-planes, and a large image m_n can be obtained by placing the bit-planes side by side only consisting of 0's and 1's. These processed images are used as watermarks, and totally 2^n independent watermarks are obtained. Watermarks in spatial domain m0 to m7 are shown in figure 3.8(b)-(i). To make the scheme more robust, the processed watermarks m are transformed to the wavelet domain and encrypted. Each DWT coefficient of watermark is embedded to corresponding frequency in the video frame. Sample preprocessed watermarks are shown in figure 3.8, where (a) is the original watermark, (b)-(i) represent the scrambled watermarks in the spatial domain, and (j) shows the encrypted watermark of (b), *i.e.,* m'_0.

3.2.2 Audio watermark

Error correcting code is extracted from the watermark image and embedded in audio channel as an audio watermark. This watermark can provided the error correction and detection capability for the video watermark. In detection phase, it would be extracted and used for refining the video watermark.

Different error correcting coding techniques can be applied such as Reed-Solomon Coding Techniques and Turbo Coding. Error correcting codes are a kind of safety net-mathematical insurance against the vagaries of an imperfect material world.

The key to error correction is redundancy. Indeed, the simplest error correcting code is simply repeated everything times. However, in order to keep the audio watermark to be inaudible, we cannot embed too much information into the audio channel. In our scheme, we applied averaging to achieve the error code. Since pixels of an image are likely to have similar values with the neighbor pixels, average value of a small region can be used to estimate the pixels within that particular region. The average value of each region is calculated as follow:

$$Avg_k = \sum_{i=0}^{x} \sum_{j=0}^{y} W_{j*w+q*x+p*y*w+i}$$

k = kth block of the average image
p = y-coordinate of region k
q = x- coordinate of region k
x*y = size of block

This concept is visualized in figure 3.9 and the video and audio watermark are shown.

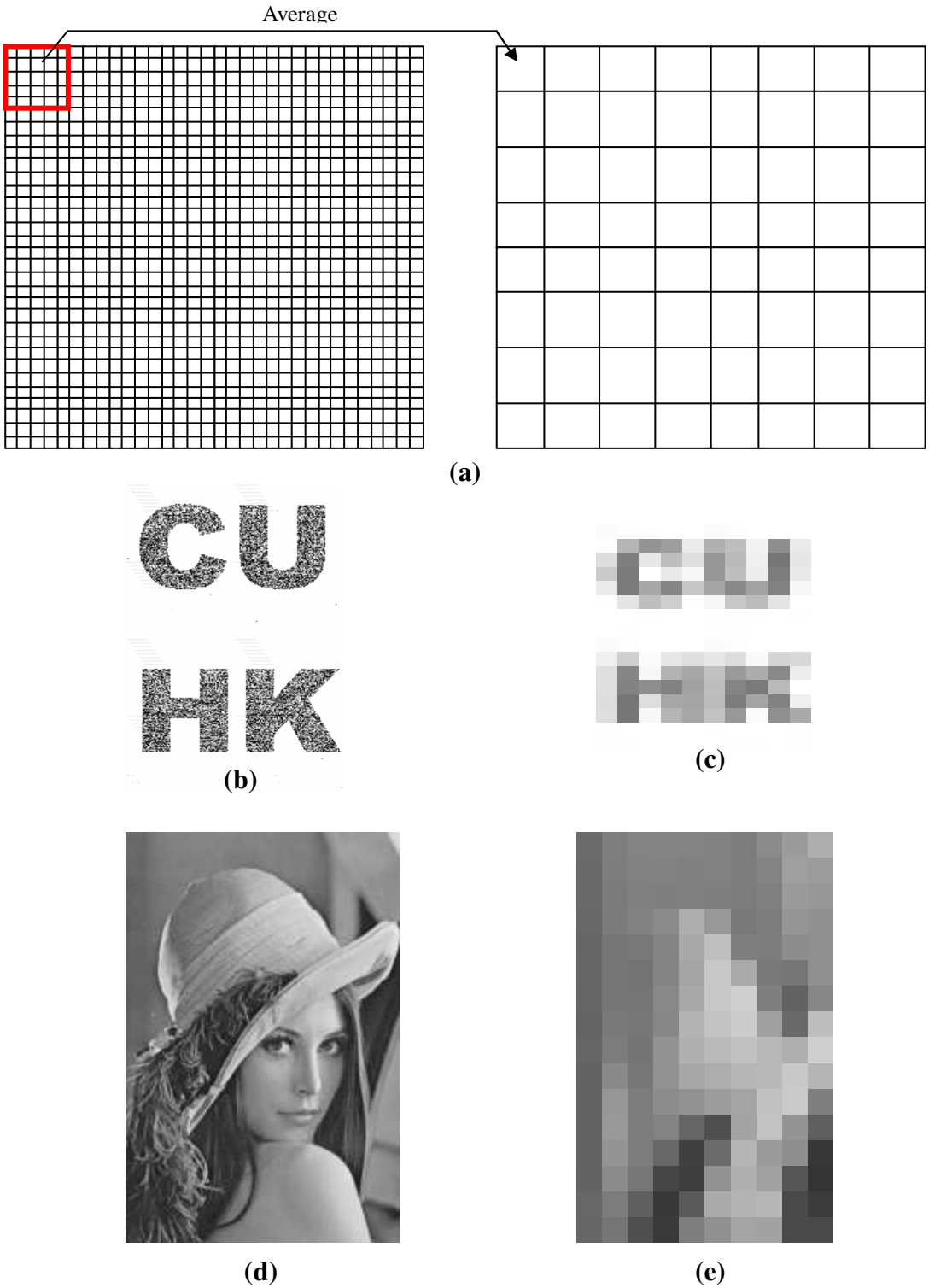


Figure 3.9 (a) visualization of averaging (b) original video watermark (c) audio watermark (average of (c)) (d) video watermark would be used in the following sections (e) audio watermark of d

After all things are prepared, what's next? It should be embedding watermark in the video frames. The details are stated in the coming session.

3.3 Watermark Embedding

Two watermarks have to be embedded in video channel and audio channel. The overview of the watermarking procedures is shown in figure 3.10.

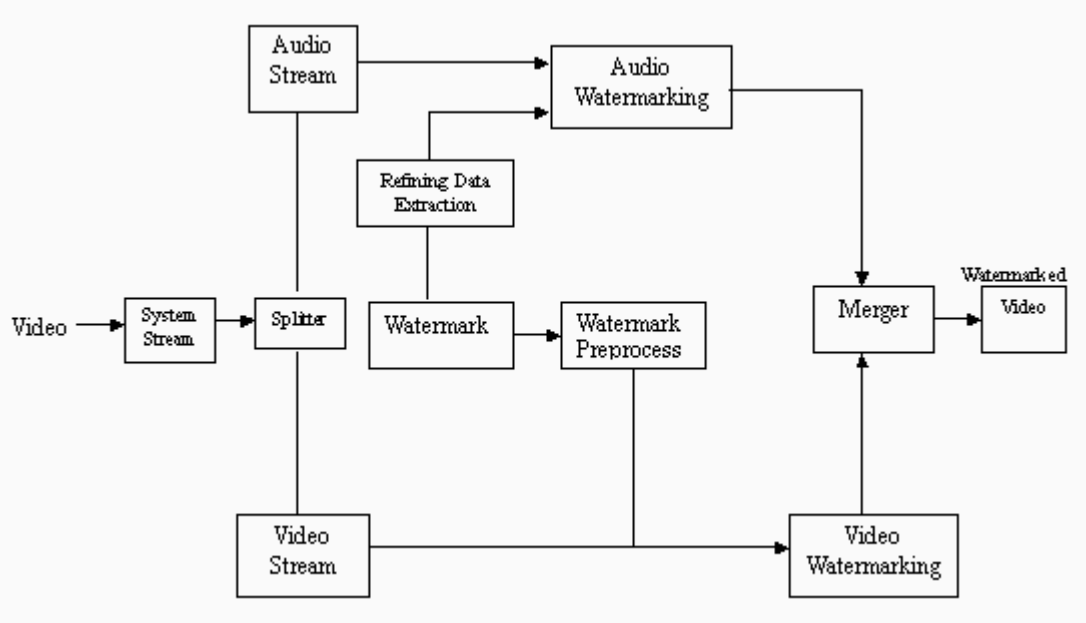


Figure 3.10 Overview of the watermarking process

The details are described in this section.

3.3.1 Video Watermark

The watermark is added to the frames by altering the magnitude of some DWT coefficients. The condition is shown as follow:

if W[j] = 1,
Exchange C[i] with max(C[i], C[i+1], C[i+2], C[i+3], C[i+4])
else
Exchange C[i] with min(C[i], C[i+1], C[i+2], C[i+3], C[i+4])

where **C[i]** is the i^{th} DWT coefficient of a video frame, and **W[j]** is the j^{th} pixel of a certain watermark. The sequence of watermark coefficients used is stated in figure 3.11, where higher frequency coefficients are embedded to higher frequency part of the video frame. Also, only the middle frequency wavelet coefficient of the frame (middle frequency sub-band) is watermarked, i.e., DWT

coefficients of HL_1, LH_1, HL_2, LH_2, HL_3, LH_3, HL_4 and LH_4 are watermarked. Details are shown in figure 3.11. As an example, the original and the watermarked frames are shown in figure 6(a) and 6(b) later.

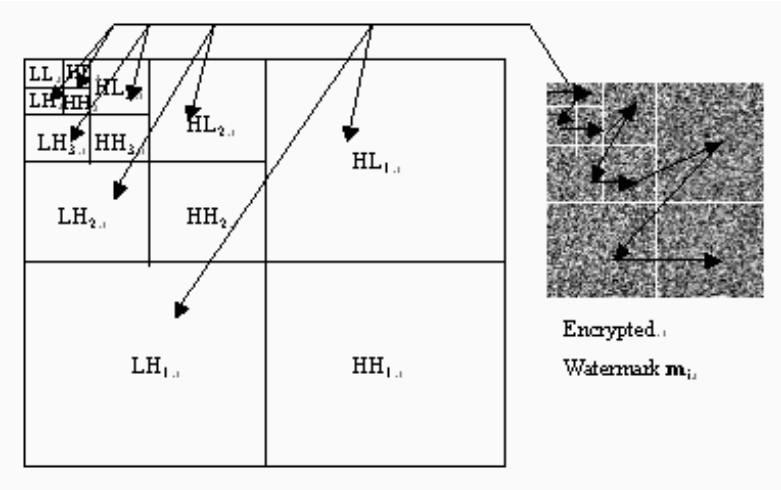


Figure 3.11 Embedding watermarks in a frame

Coefficients of LL (i.e. the low frequency sub-band) are not watermarked, as video energy is concentrated on lower frequency wavelet coefficient. If they are altered, it will affect perceptual quality. Only alter LL coefficients make the hidden mark not perceptible under domestic condition.

Coefficients of HH (i.e. the high frequency sub-band) are also not watermarked. It can make the watermark survive MPEG lossy compression as lossy compression removes the details (i.e. the high frequency components) of the image.

After watermark is embedded in the video frames in wavelet domain, Inverse Discrete Wavelet Transform (IDWT) is applied to obtain the watermarked frames and output the watermarked video stream

3.3.2 Audio Watermark

The emphasis of this scheme is video watermark and audio watermark is used to help the video watermark to be more robustness. Audio watermark is used for refining the video watermark in detection phase, so the error coding code is store in the audio channel. We have applied the audio watermarking technologies of Communication and Multimedia Lab of Department of Computer Science and Information Engineering in National Taiwan University to do this part.

A novel approach for embedding a digital watermark inaudibly into an audio clip, in the time domain, according to the difference between two half blocks of each block is proposed by CMLAB. The proposed scheme does not require any host-related information for watermark extraction. The embedded watermark is robust to common audio signal manipulations, such as MP3 compression, time shifting, cropping, time scaling, D/A A/D conversion, insertion, deletion, re-sampling, re-quantization and filtering.

We have applied it in our video watermark scheme. Two kinds of information are hidden in the audio: the error correcting code and a synchronization template. The error correcting code is described in the pervious section. The synchronization template is generated by a random number generator controlled by a secret key and is used for synchronizing the signal skew caused by time shifting, cropping and time scaling attacks. The two kinds of information are combined together and dispersed by another secret key before embedding.

After both video and audio watermark are embedded, the video and audio stream are merged and the watermarked video is output.

3.4 Watermark Detection

In the detection phase, video is checked for the mark presence. There are two, somehow related, ways to look at watermark extraction, first is "Whose watermark is this?" or second is "Is this watermark X?" The watermark can be thought of as a signal embedded in noise. The optimal detector is maximum likelihood or, equivalently, a correlation receiver. Ours is a blind video watermarking scheme, it do not need the original video while detecting the watermark. Watermark is detected through the following process, and the overview is shown in figure 3.12. and details are shown in figure 3.14

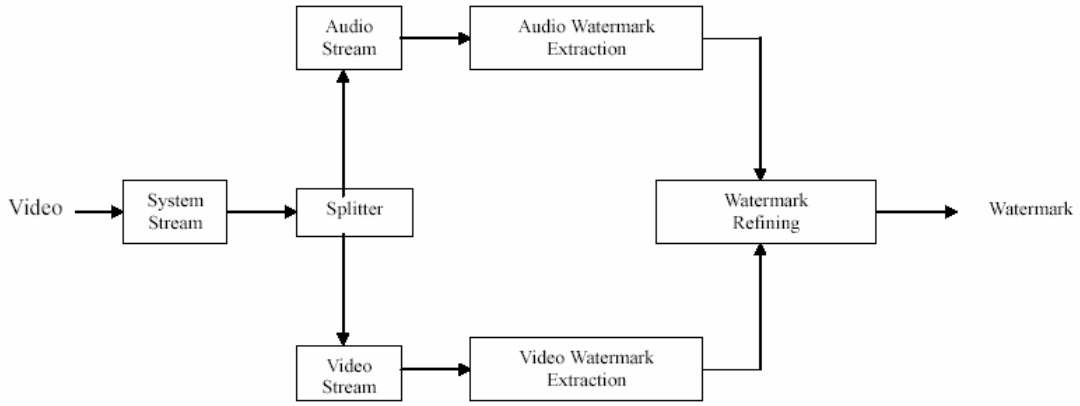


Figure 3.12

The test video is split into video stream and audio stream and the watermarks are extracted separately by audio watermark extraction and video watermark extraction.

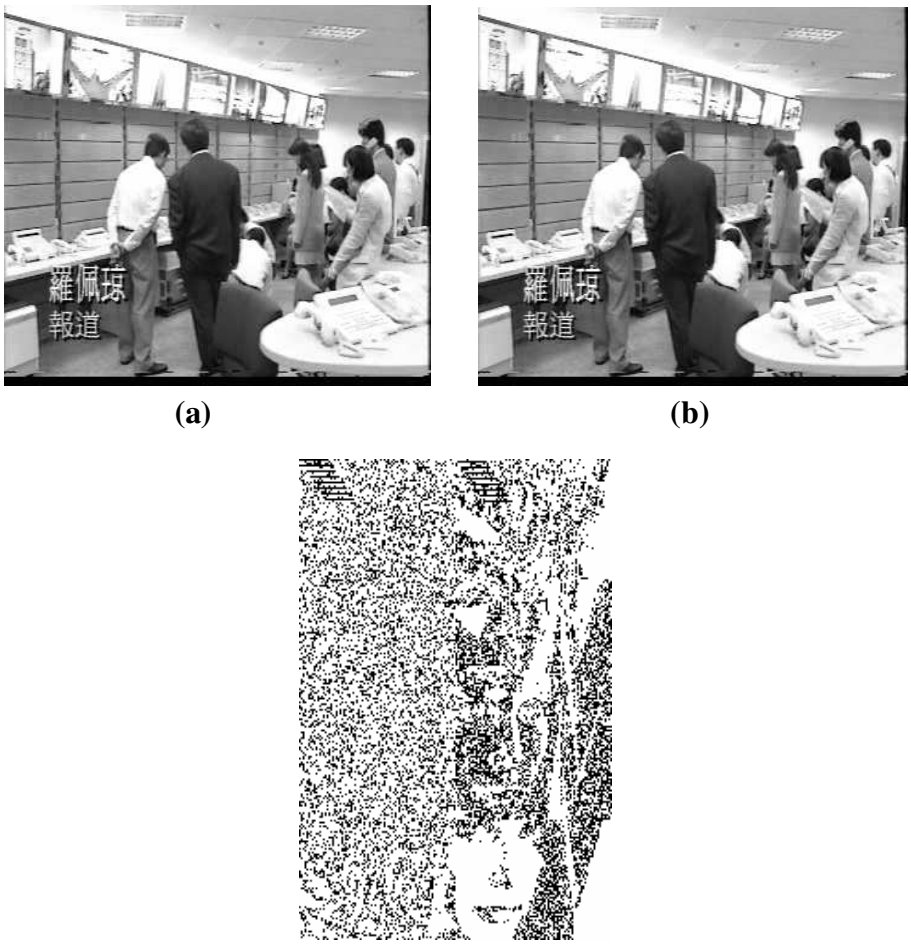
The video stream will be processed to get the video watermark. First, scene changes are detected from the video. Also, each video frame is transformed to the wavelet domain with 4 levels. Then the watermark is extracted with the following condition:

if WC[i] > median(WC[i], WC[i+1], WC[i+2], WC[i+3], WC[i+4])
W[j] = 1
Else
W[j] = 0

where **WC[i]** is the i^{th} DWT coefficient of a watermarked video frame, and **W[j]** is the j^{th} pixel of an extracted watermark.

As an identical watermark is used for all frames within a scene, multiple copies of each part of the watermark may be obtained. The watermark is recovered by averaging the watermarks extracted from different frames. This reduces the effect if the attack is carried out at some designated frames. Then we can combine the 8 bit-planes and recover the 64 X 64 size image, i.e., $1/2^n$ part of the original watermark.

If enough scenes are found and all parts of the watermark are collected, the original large watermark image can be reconstructed. The extracted watermark from a sample frame is shown in figure 3.13. However, if some of the watermark part is lost, the watermark can still survive. We will show this later.



(a) **(b)**

(c)

Figure 3.13(a) Original frame (b) Watermarked frame (c) Extracted watermark corresponding to figure 3.13(a)

The error correcting code is extracted from the audio stream and the video watermark extracted is refined by this information with the following equation

$$\widehat{W}_{ij} = (\widehat{W}_{ij} * P + Avg_k * Q)/(P+Q) \qquad \text{if } \left|W_{ij} - \widehat{W}_{ij}\right| \geq T$$

$$\widehat{W}_{ij} = \widehat{W}_{ij} \qquad \text{Otherwise}$$

k = kth block of the average image

i = x- coordinate of video watermark

j = y-coordinate of video watermark

T = Threshold that the pixel need to correct

P: Q = the ratio of importance of extracted watermark to average

After extracting and refining the watermark, the user can compare the results with the referenced watermarks subjectively. However, since the subjective measurement will be affected by the factors of the image size, expertise of the observers, and the experimental conditions, etc., a quantitative measurement is required to provide objective judgment of the extracting fidelity. Therefore, a similarity measurement of the extracted and the referenced watermarks can be defined as:

$$\text{Normalized correlation: NC} = \frac{\sum_i \sum_j W(i,j)\widehat{W}(i,j)}{\sum_i \sum_j [W(i,j)]^2}$$

which is the cross-correlation normalized by the reference watermark energy to give unity as the peak correlation. We will use this measurement to evaluate our scheme in our experiment.

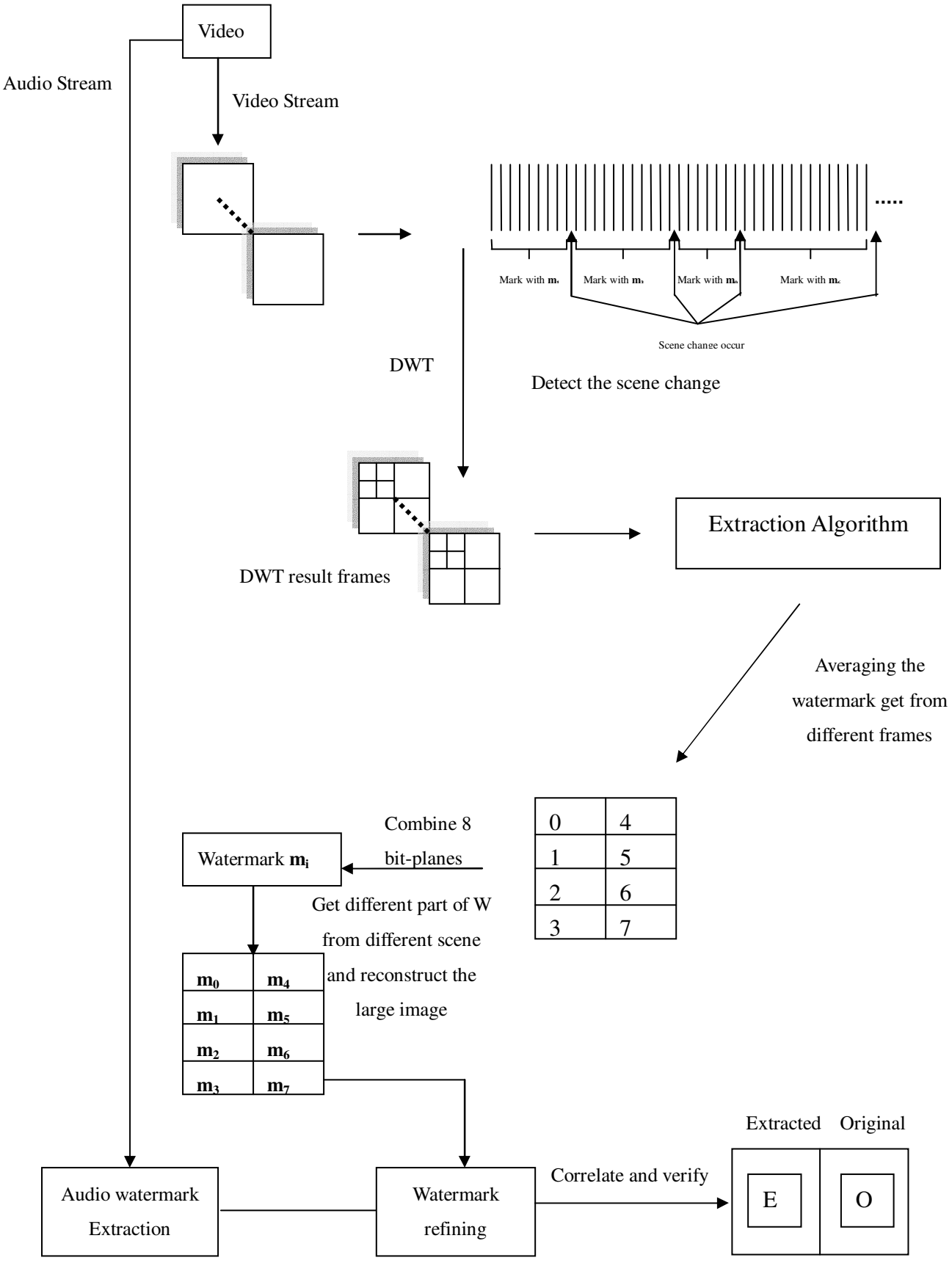

Video
Audio Stream
Video Stream
Mark with m1
Mark with m3
Mark with m5
Mark with m7
Scene change occur
DWT
Detect the scene change
DWT result frames
Extraction Algorithm
Averaging the watermark get from different frames
0 4
1 5
2 6
3 7
Combine 8 bit-planes
Watermark mi
Get different part of W from different scene and reconstruct the large image
m0 m4
m1 m5
m2 m6
m3 m7
Extracted Original
E
O
Audio watermark Extraction
Watermark refining
Correlate and verify

Figure 3.14

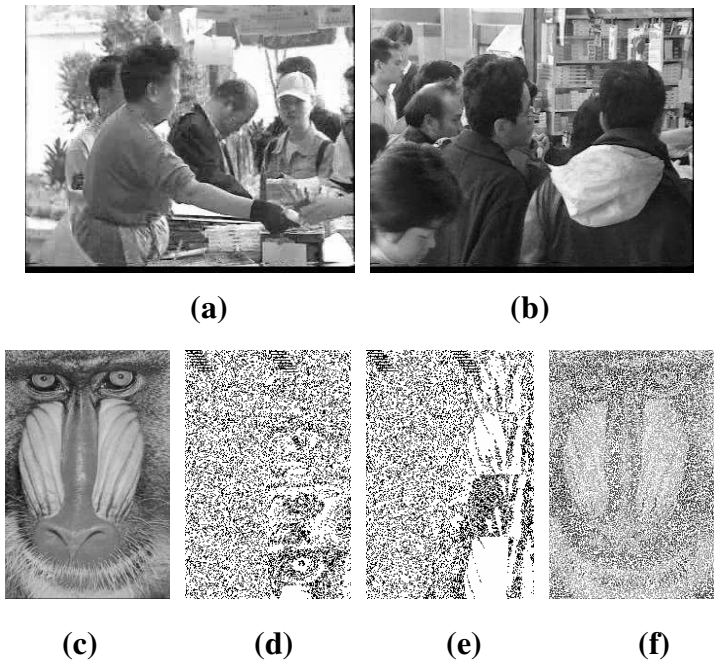
4 Experimental Results & Discussion

4.1 Experimental Results

Simulations are performed to evaluate the performance of the algorithms mentioned above. Two videos are used for the experiment.

Video 1

A video news clip with 1328 frames of size 352 X 288 is used for testing. The video consists of 8 scene changes. The video frames are all normalized to 256 X 256 before the watermark is embedded and the DWT coefficients of the middle frequency sub-band are modified according to the watermarking scheme. Different parts of the watermark are extracted from the watermarked video for reconstructing the whole watermark. As illustration, the extracted watermarks of the 2nd scene and the 3rd scene, as well as the recovered watermark are shown in figure 3.15.



(a) **(b)**

(c) **(d)** **(e)** **(f)**

Figure 3.15 (a) Watermarked 2nd scene (b) Watermark 3rd scene (c) Original watermark (d) Extracted watermark from 2nd scene (d) Extracted watermark from 3rd scene (e) recovered watermark from all video frames

To test the frame dropping and averaging attack, 700 random frames are dropped. The missing frames are replaced by the average of the two neighboring frames. Figure 3.16(a) shows the extracted watermark under this attack. Figure 3.16(b) demonstrates the extracted watermark from the video under by MPEG compression. Figure 3.16(c) and (d) depict the watermarks extracted from the video clip whose the frames are under image processing attacks. Figure 3.16(e) shows the recovered watermark when all frames in the 5th scene are dropped. The experimental results illustrate the effectiveness of our scheme.

Then the extracted watermark is compared with the original watermark and the NC values are calculated. It is found that the watermark is very robust against attack by frame dropping and frame averaging, which get the highest NC values (9.56). The scheme is also robust against change of brightness, cropping and partial watermark dropping; their NC values are greater than 8. However, the scheme is not very good when compression is applied, where NC is 5.6 and it is not satisfactory.

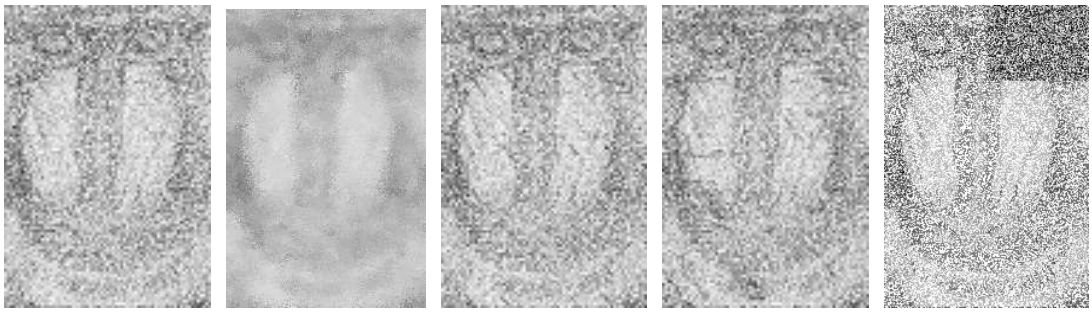


Figure 3.16 Extracted watermark from different attacks (a) Dropping and averaging (b) Compression (c) Increase brightness (d) Cropping some regions (e) Dropping all frames with the 5th part of watermark

Video 2

A video news clip with 1526 frames of size 352 X 288 is used in our experiment. The video consists of 10 scene changes. The video frames are first normalized to 256 X 256, and then the watermark is embedded in it. As an illustration, the extracted watermarks of the 4th scene and the 6th scene, as well as the recovered watermark are shown in figure 3.17.

(a) **(b)**

(c) **(d)** **(e)** **(f)**

Figure 3.17 (a) Watermarked 4th scene (b) Watermark 6th scene (c) Extracted watermark from 4th scene (d) Extracted watermark from 6th scene (e) recovered watermark from all video frames (f) Dropping all frames with the 5th part of watermark

To test the robustness, different attacks are applied to the watermarked video, including frame dropping, frame averaging, lossy compression, brightness increasing, area cropping, and partial removal of the watermark.

To test the frame dropping and averaging attack, 650 random frames are dropped. The missing frames are replaced by the average of the two neighboring frames. The NC value is the lowest when the video is under attack by MPEG compression. With DWT, our scheme takes the major advantages in resisting the

attacks on the watermarked frames. The results also show our scheme is robust against different image processing attacks. The experimental results illustrate effectiveness of our scheme.

After getting the result from these two videos, NC values of the extracted watermarks are calculated. The NC values are retrieved and shown in figure 3.x when the watermarked video is under different attacks.

In figure 3.18, 2 curves are shown in the graph. One of them is without correction with audio watermark. Another one is corrected with audio watermark. It is found that video watermark is improved by audio watermark as the NC values are increased.

The NC value of the pure audio watermark is 0.92. When video watermark is refined by the audio watermark, the NC value of cropping is improved from 0.914 to 0.943 and the NC value of dropping is improved from 0.946 to 0.965. The NC values of the refined watermarks are higher; it shows that the visual-audio watermark can improve the robustness of the watermark scheme.

However, when the watermark is under compression and sharpening, the NC value of the watermarks are increased but they are lower than the pure audio watermark.

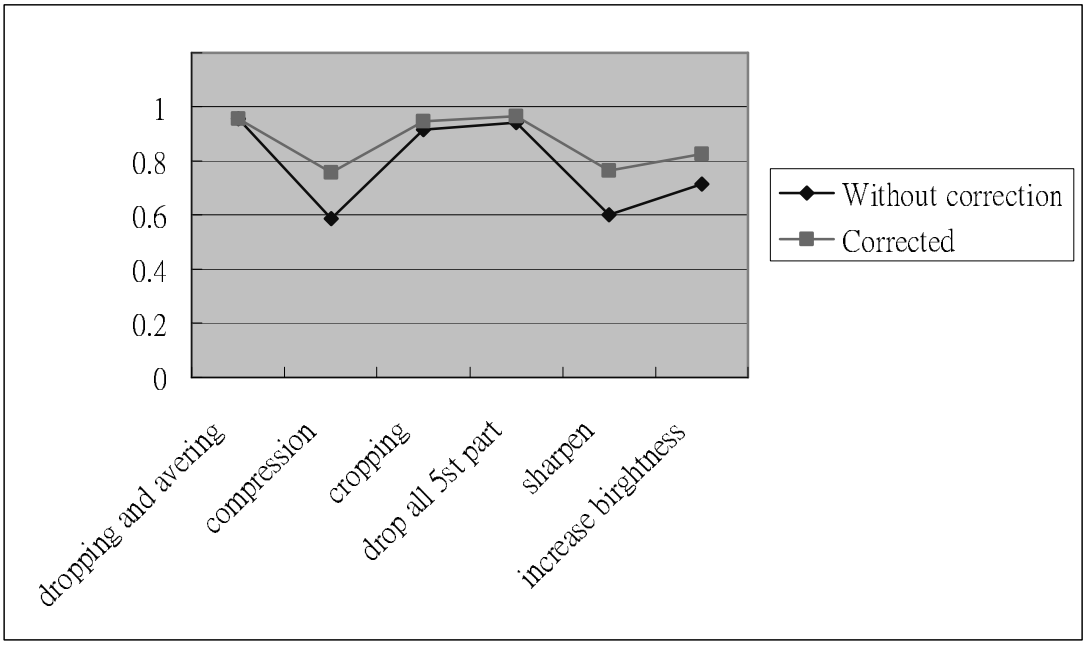


Figure 3.18 NC values under different attacks

4.2 Discussion -- Evaluation on the robustness of the watermark scheme

The video watermarking scheme supposes to be robust against the attack of frame dropping, averaging, lossy compression and novel attack on image watermarking.

Frame dropping

As each scene is embedded with same watermark, it can prevent attackers from removing the watermark by frame dropping. If they try to remove the frames with same watermark, they need to remove the whole trunk of frame (i.e. the whole scene) and this would lead to significant damage to the video.

Frame averaging

Watermark is cropped into pieces and embedded into different frame can make the watermarks resistant to attacks by frame averaging to extract the watermark

Identical watermark is used within a scene can prevent attackers from taking advantage of motionless regions in successive frames to remove the watermark by comparing and averaging the frames statistically. Also, similar frames used same watermark make the scheme resistant to statically analysis of the video.

Statistical analysis

Independent watermark used for successive different scene can prevent attackers from colluding with frames from completely different scenes to extract the watermark.

Lossy compression

Coefficients of HH (i.e. the high frequency sub-band) are also not watermarked. It can make the watermark survive MPEG lossy compression as lossy compression removes the details (i.e. the high frequency components) of the image. However, after experiment, it is found that the scheme is not very robust against lossy compression.

Attacks on watermarked frame

With DWT, it takes lots of advantage to resist the attacks on the watermarked frames. It achieves both spatial and frequency localization, both perceptual invisibility and robustness to compression. It robust to noise, image processing techniques, and median filter (which can be consider as a case of pixel permutation, it course destroys the synchronization.). DWT also make the watermark to be resistant to geometric transform (lots of existing algorithm may not survive)

The scheme is robust against format conversions because the watermark is inserted before compression. Otherwise, the drawback of the techniques is that, since the code is directly embedded into the compressed stream such as mpeg-4, the copyright information is lost if the video file is converted to a different compression standard, such as mpeg-2

This scheme also survive after resizing as the video are normalized in both insertion and detection phase

Invisibility

Coefficients of LL (i.e. the low frequency sub-band) are not watermarked, as video energy is concentrated on lower frequency wavelet coefficient. If they are altered, it will affect perceptual quality. Only alter LL coefficients make the hidden mark not perceptible under domestic condition.

Blind watermarking scheme

Retrieval of embedded watermark does not need the original video. It is important for increasing the performance of the scheme because the size of video is large and it takes long time to transmit and process.

Visual-audio watermark

The video watermarking scheme is improved by including both video and audio watermark. The error correcting code is extracted from the video watermark and embedded in the audio channel. And it is used to refine the video watermark in detection phase. After including the audio watermark for refining, it increases the normalized correlation values of the video watermark.

Weakness

1. The capacity of the scheme is not calculated; the capacity can be improved by using different transform domain.
2. The error correcting code techniques applied is not very accurate
3. The watermark is not very robust against to lossy compression.
4. When the watermark is under compression and sharpening, the NC value of the watermarks are increased but they are lower than the pure audio watermark.

5 Future Direction

The novel video watermark scheme presented and experimental result is shown. It shows that the scheme is robust against the attack of frame dropping, averaging, statistical analysis and attack on image watermarking.

It is found that the watermark is not robust against lossy compression; we can improve the scheme in this direction. When the watermark is under compression and sharpening, the NC value of the watermarks are increased but they are lower than the pure audio watermark. It can be improved by change the way to combine the visual and audio watermark. It can use the concept of committee machine. The scheme can also be improved by making use of the information from the video, such as time information to increase the robustness of the watermark.

This DWT-based Video Watermarking Scheme with Scramble Watermark can be associated with different applications to achieve a sophisticated system. This research can be continuous by applying the new developed watermarking scheme to specific environment or application and examine its usefulness.

6 Conclusion

After noticing the importance of the multimedia security and video watermarking in nowadays Internet world and reviewing the state-of-the-arts technologies of the audio watermarking, image watermarking and video watermarking, a novel digital video watermarking scheme is proposed. Our scheme embeds different parts of a signal watermark into different scenes of a video under the wavelet domain. To increase robustness of the scheme, the watermark is refined by the error correcting code which is embedded as watermark in the audio channel. It is a scheme which not only robust to image watermark attacks, but also the additional issue addressed by video, that is frame averaging, frame dropping, frame swapping and statistical analysis. Experiment is carried out to prove this visual audio watermarking scheme's robustness.

7 Acknowledgement

Prof. Michael R. Lyu provides valuable suggestions and comments and these give significant direction to my research.

8 Reference

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

[2] Ahmet M. Eskicioglu, Edward J. Delp, "An overview of multimedia content protection in consumer electronics devices", Signal Processing: Image Communication 16 (2001) 681}699

[3] Boulgouris, N.V.; Koravos, F.D.; Strintzis, M.G.,"Self-synchronizing watermark detection for MPEG-4 objects", *Electronics, Circuits and Systems, 2001. ICECS 2001. The 8th IEEE International Conference* on , 2001, Page(s): 1371 -1374 vol.3

[4] Checcacci, N.; Barni, M.; Bartolini, F.; Basagni, S., "Robust video watermarking for wireless multimedia communications ", *Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE* , 2000, Page(s): 1530 -1535 vol.3

[5] Ching-Yung Lin and Shih-Fu Chang, "Issues and Solutions for Authenticating MPEG Video", *IEEE International Conference on Acoustics, Speach and Signal Processing*, 15-19 Mar 1999, pp 54-65.

[6] Chun-Shien Lu; Hong-Yuan Mark Liao, "Video object-based watermarking: a rotation and flipping resilient scheme", *Image Processing, 2001. Proceedings. 2001 International Conference* on , Volume: 2 , 2001, Page(s): 483 -486 vol.2

[7] Eugene T. Lin, Christine I. Podilchuk, Ton Kalker, and Edward J. Delp, "Streaming Video and Rate Scalable Compression: What Are the Challenges for Watermarking?" *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents III*, Vol. 4314, January 22 - 25, 2001, San Jose, CA.

[8] F. Hartung and B. Girod, "Watermarking of Uncompressed and Compressed Video", *Signal Processing*, vol. 66, no. 3 (Special issue on Watermarking), pp. 283-301, May 1998.

[9] Furon, T; Duhamel, P., "Robustness of asymmetric watermarking technique", *Image Processing, 2000. Proceedings. 2000 International Conference on, 2000*, Page(s): 21-24 vol.3

[10] Fengming Huang; Hosseni, H.M.; Hock Chuan Chu; Yong Liang Guan, "Watermarking of streaming video for finger-printing applications", on , Volume: 2 , 2002, Page(s): 452 -455

[11] Fridrich, J., "A hybrid watermark for tamper detection in digital images", *Signal Processing and Its Applications, 1999. ISSPA '99. Proceedings of the Fifth International Symposium* on , Volume: 1 , 1999 , Page(s): 301 -304 vol.1

[12] Hartung, F.; Ramme, F., "Digital rights management and watermarking of multimedia content for m-commerce applications", IEEE Communications Magazine , Volume: 38 Issue: 11 , Nov. 2000, Page(s): 78 -84

[13] Ian Brown, Colin Perkins, and Jon Crowcroft, "Watercasting: Distributed Watermarking of Multicast Media", *Networked Group Communication '99*

[14] Ikpyo Hong; Intaek Kim; Seung-Soo Han, "A blind watermarking technique using wavelet transform" *Industrial Electronics, 2001. Proceedings. ISIE 2001.* IEEE International Symposium on, Volume: 3 , 2001 Page(s): 1946 -1950 vol.3

[15] Jun-Zhao Sun; Howie, D.; Koivisto, A.; Sauvola, J., "A hierarchical framework model of mobile security ", *Personal, Indoor and Mobile Radio Communications, 2001 12th IEEE International Symposium* on , Volume: 1 , 2001, Page(s): A-56 -A-60 vol.1

[16] Lancini, R.; Mapelli, F.; Tubaro, S., "A robust video watermarking technique in the spatial domain ", *Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium* on VIPromCom , 2002 Page(s): 251 -256

[17] L. Qiao and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer 's rights," *Journal of Visual Communication and Image Representation 9*, pp. 194#210, September 1998.

[18] L. Qiao and K. Nahrstedt, "Watermarking method for mpeg encoded video:

Towards resolving rightful ownership," *IEEE Multimedia Computing and Systems*, June 1998.

[19] M.Ramkumar and A.N. Akansu, "Robust Protocols for Proving Ownership of Image" *IEEE Trans. on Multimedia*

[20] Piva, A.; Caldelli, R.; De Rosa, A., "A DWT-based object watermarking system for MPEG-4 video streams ", *Image Processing, 2000. Proceedings. 2000 International Conference* on , 2000 Page(s): 5 -8 vol.3

[21] Piva, A.; Bartolini, F.; Barni, M., "Managing copyright in open networks", *IEEE Internet Computing* , Volume: 6 Issue: 3 , May-June 2002, Page(s): 18 -26

[22] R. B. Wolfgang and E. J. Delp, "Overview of Image Security Techniques with Applications in Multimedia Systems," *Proceedings of the SPIE Conference on Multimedia Networks: Security, Displays, Terminals, and Gatweys,* Vol. 3228, November 2-5, 1997, Dallas, Texas, pp. 297-308.

[23] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents*, vol. 3657, January 25 - 27, 1999, San Jose, CA, pp. 40-51.

[24] R. B. Wolfgang and E. J. Delp, "A Watermarking Technique for Digital Imagery: Further Studies," *Proceedings of the International Conference on Imaging Science, Systems, and Technology* June 30 - July 3, 1997, Las Vegas, pp. 279-287.

[25] Serdean, C.V.; Ambroze, M.A.; Tomlinson, M.; Wade, G., "Combating geometrical attacks in a dwt based blind video watermarking system", *Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium* on VIPromCom , 2002, Page(s): 263 -266

[26] Joo Lee; Sung-Hwan Jung, "A survey of watermarking techniques applied to multimedia", *Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE International Symposium* on, Volume: 1, 2001, Page(s): 272 -277 vol.1

[27] Sumit Gulwani, "A report on Security Issues in Multimedia" Department of

Computer Science & Engineering, Indian Institute of Technology Kanpur

[28] Sviatoslav Voloshynovskiy, Shelby Pereira, Alexander Herrigel Nazanin, “Generalized watermarking attack based on watermark estimation and perceptual remodulation”, In Ping Wah Wong and Edward J. Delp eds., *IS&T/SPIE's 12th Annual Symposium Electronic Imaging 2000: Security and Watermarking of Multimedia Content II*, Vol. 3971 of SPIE Proceedings, San Jose, California USA, 23-28 January 2000. (Paper EI 3971-34).

[29] T. P.-C. Chen and T. Chen, "A Framework for Optimal Public Watermark Detection", *Carnegie Mellon University Technical Report*: AMP01-03.

[30] Vassaux, B.; Nguyen, P.; Baudry, S.; Bas, P.; Chassery, J.-M., “Scrambling technique for video object watermarking resisting to mpeg-4”, *Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium* on VIPromCom , 2002 Page(s): 239 –244

[33] Xiamu Niu, Shenghe Sun, "A New Wavelet-Based Digital Watermarking for Video", *9th IEEE Digital Signal Processing Workshop*. Texas, USA, Oct. 2000

[34] Imprimatur, “Watermarking Technology for Copyright Protection: GeneralRequirements and Interoperability”

[35] Video watermark technique in motion vector *Jun Zhang; Jiegu Li; Ling Zhang;* Computer Graphics and Image Processing, 2001 Proceedings of XIV Brazilian Symposium on , Oct 2001 Page(s): 179 -182

[36] System issues in digital image and video watermarking for copy protection *Kalker, T.;* Multimedia Computing and Systems, 1999. IEEE International Conference on , Volume: 1 , Jul 1999 Page(s): 562 -567 vol.1

[37] Fast video transcoding architectures for networked multimedia applications *Jeongnam Youn; Jun Xin; Ming-Ting Sun;* Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on , Volume: 4 , 2000 Page(s): 25 -28 vol.4

[38] Media-independent watermarking classification and the need for combining digital video and audio watermarking for media authentication *Dittmann, J.; Mukherjee, A.; Steinebach, M.;* Information Technology: Coding and

Computing, 2000. Proceedings. International Conference on , 2000 Page(s): 62 -67

[39] Joint watermarking of audio-visual data *Dittmann, J.; Steinebach, M.;* Multimedia Signal Processing, 2001 IEEE Fourth Workshop on , 2001 Page(s): 601 -606

[40] Oblivious cocktail watermarking by sparse code shrinkage: a regional- and global-based scheme *Chun-Shien Lu; Liao, H.-Y.M.;* Image Processing, 2000. Proceedings. 2000 International Conference on , Volume: 3 , 2000 Page(s): 13 -16 vol.3

[41] Towards second generation watermarking schemes *Kutter, M.; Bhattacharjee, S.K.; Ebrahimi, T.;* Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on , Volume: 1 , Dec 1999 Page(s): 320 -323 vol.1

[42] Multi-level watermarking with independent decoding *Butman, M.; Hel-Or, H.Z.;* Image Processing, 2001. Proceedings. 2001 International Conference on , Volume: 2 , 7-10 Oct 2001 Page(s): 514 -517 vol.2

[43] Image refining technique using digital watermarking *Chuan-Fu Wu; Wen-Shyong Hsieh;* Consumer Electronics, IEEE Transactions on , Volume: 46 Issue: 1 , Feb 2000 Page(s): 1 -5

[44] Digital watermarks for audio signals *Boney, L.; Tewfik, A.H.; Hamdy, K.N.;* Multimedia Computing and Systems, 1996., Proceedings of the Third IEEE International Conference on , 17-23 Jun 1996 Page(s): 473 -480

[45] Practical challenges for digital watermarking applications *Sharma, R.K.; Decker, S.;* Multimedia Signal Processing, 2001 IEEE Fourth Workshop on , 2001 Page(s): 237 -242

[46] Multipurpose audio watermarking *Chun-Shien Lu; Hong-Yuan Mark Liao; Liang-Hua Chen;* Pattern Recognition, 2000. Proceedings. 15th International Conference on , Volume: 3 , 2000 Page(s): 282 -285 vol.3

[47]What can we reasonably expect from watermarks? *Craver, S.A.; Min Wu; Liu, B.;* Applications of Signal Processing to Audio and Acoustics, 2001 IEEE Workshop

on the , 2001 Page(s): 223 -226

[48] Digital audio watermarking and its application in multimedia database *Changsheng Xu; Jiankang Wu; Qibin Sun;* Signal Processing and Its Applications, 1999. ISSPA '99. Proceedings of the Fifth International Symposium on , Volume: 1 , 1999 Page(s): 91 -94 vol.1

[49] An adaptive audio watermarking system *Say Wei Foo; Theng Hee Yeo; Dong Yan Huang;* Electrical and Electronic Technology, 2001. TENCON. Proceedings of IEEE Region 10 International Conference on , Volume: 2 , 2001 Page(s): 509 -513 vol.2

[50] Muteness-based audio watermarking technique *Kaabneh, K.A.; Youssef, A.;* Distributed Computing Systems Workshop, 2001 International Conference on , Apr 2001 Page(s): 379 -383

[51] A robust digital audio watermarking technique *Changsheng Xu; Jiankang Wu; Qibin Sun;* Signal Processing and Its Applications, 1999. ISSPA '99. Proceedings of the Fifth International Symposium on , Volume: 1 , 1999 Page(s): 95 -98 vol.1

[52] Wireless image transmission using multiple-description based concatenated codes *Sachs, D.G.; Anand, R.; Ramchandran, K.;* Data Compression Conference, 2000. Proceedings. DCC 2000 , 2000 Page(s): 569

[53] Video image transmission via mobile satellite channels *Xiaohong Wang; Yong Liu; Blostein, S.B.;* Communications, 1995. ICC 95 Seattle, Gateway to Globalization, 1995 IEEE International Conference on , Volume: 1 , 18-22 Jun 1995 Page(s): 352 -356 vol.1

[54] Audio watermarking: features, applications and algorithms *Arnold, M.;* Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on , Volume: 2 , 2000 Page(s): 1013 -1016 vol.2

[55] Multimedia data-embedding and watermarking technologies *Swanson, M.D.; Kobayashi, M.; Tewfik, A.H.;* Proceedings of the IEEE , Volume: 86 Issue: 6 , Jun 1998 Page(s): 1064 -1087

[56] "To Improve the Image Distortion and Machine Motion Accuracy in Machine Vision Measuring System", Chih-Hung Tsai, Shiaw-Wen Tien, Yi-Chan Chung and Yu-Tang Lin, International Journal of The Computer, The Internet and Management, Vol. 10, No2, 2002, p 56 -80

[57] Compression tolerant watermarking for image verification *Bassali, H.S.; Chhugani, J.; Agarwal, S.; Aggarwal, A.; Dubey, P.;* Image Processing, 2000. Proceedings. 2000 International Conference on , Volume: 1 , 2000 Page(s): 430 -433 vol.1

[58] The choice of watermark domain in the presence of compression *Chuhong Fei; Deepa Kundur; Kwong, R.;* Information Technology: Coding and Computing, 2001. Proceedings. International Conference on, Apr 2001 Page(s): 79 -84

[59] An integrated algorithm with watermarking and compression *Shao Ya-fei; Zhang Li; Wu Guo-wei; Lin Xing-gang;* Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences on, Volume: 2 , 2001 Page(s): 797 -802 vol.2

9 Appendix

Table of different digital watermarking schemes

9.1 Audio Watermark

Audio Watermark	Method	Advatage	Detection
Affine Resistant Digital Audio Watermarking Using Template Matching	This is an approach for embedding a digital watermark inaudibly into an audio clip, in the time domain, according to the difference between two half blocks of each block. The proposed scheme does not require any host-related information for watermark extraction.	the embedded watermark is robust to common audio signal manipulations, such as MP3 compression, time shifting, cropping, time scaling, D/A A/D conversion, insertion, deletion, re-sampling, re-quantization and filtering.	When extracting watermark, our system detects all possible time shifts and time scales from -2% to +2%, and the extraction can be done in real time. The signal to noise ratio (SNR) is defined as follows: $SNR = 10\log_{10}\frac{\sum_n x^2(n)}{\sum_n [x(n)-y(n)]^2}$ where x(n) and y(n) are samples of the original and the watermarked audio clips, respectively. The SNR values in the brackets of Table 1 is calculated based on the adjustable blocks, i.e. where $x(n) \neq y(n)$, only.

Digital Audio Watermarking Based-on Multiple-Bit Hopping and Human Auditory System	the embedding scheme is high related to audio content by making use of the properties of human auditory system and multiple-bit hopping technique. The watermark embedding design is based on audio content and HAS. With content-adaptive embedding scheme, the embedding parameter for setting up the embedding process will vary with the content of the audio signal..	Robust to A/D and D/A conversion, niose adding,	The watermarked audio signal is segmented into frames using the same segmentation method as in embedding process. Then the bit detection is conducted to extract bit delays on a frame-by-frame basis. Because a single bit of the watermark is hopped into multiple bits through bit hopping in the embedding process, multiple delays are detected in each frame. This method is more robust against attackers compared with the single bit hiding technique. Firstly, one frame is encoded with multiple bits, and any attackers do not know the coding scheme. Secondly, the embedded signal is weaker and well hidden as a consequence of using multiple bits
Muteness-Based Adio Watermarking Techniqe	1) It extends the mute perods in an audio signal without any perceptual diferece to the average human auditory system. 2) The extension of mute periods carries the same amplitude so it will blend with the original and will not attract any attetion. 3) It dose not require the original signal to extract the watermark.	1) a mute period is an integral part of any audio signal. It cannot be omitted since it represets and integral part of the sudio signal. 2) It occours randomly in audio signal, which is generated by the music process. 3) A mute period represets a rel time iterval that will not be decreased whe compressed.	In order to detect the watermark in a audio signal. The owner needs to have only the original length of all mte periods fro the audio file. From the distributed copy, it ca extract all the mute period ad recover the watermark.

9.2 Image Watermark in Spatial domain

Watermarking Scheme	Method	Advantage	Disadvantage	Detection method
LSB encoding	Hiding data in a fixed number of LSBs of an image pixel	1. Good localization and security properties 2. Minimizing of degradation after insertion	1. Cannot be used to distinguish malicious change	Extracting using correlation
Checksum techniques	This watermark is formed from the checksum value of the seven most significant bits of all pixels. A checksum is the modulo-2 addition of a sequence of fixed-length binary words;	1. Embedding W only change half of the pixels covered by W. This not only reduces visual distortion but also increases security. 2. An image may hold many W as long as they do not overlap 3. fast	1. This watermarking method is fragile. Any change to either the image data itself or the embedded checksum can cause the verification fail 2. Checksum method dose not detect pixel swaps or similar attacks. 3. removed by replacing the LSB plane	Verify the watermark the checksum of the test image and compare with the ideal W
m-sequence approach	This watermark is based on using a modified m-sequence. M-sequences achieve this maximum period, and have a very desirable autocorrelation and randomness properties.	1. robust to small amount of noise 2. pixel swaps required knowledge of W 3. multiple watermark can overlap	1. last 2 bit planes could be removed and replaced 2. deduce W if 2n consecutive bits in W are known 3. not specifically protect the DC value of the pixel covered by individual block	
Spread spectrum	Delivers narrowband data through a noisy channel	1. Level of tolerance to change is user-determined by adjusting T 2. Verification algorithm. Is much less computationally intensive 3. changes in an image can be	Similar to m-sequence approach	Retrieval of the watermark unambiguously identifies the owner, and the watermark can be constructing to make counterfeiting almost impossible.

		localized to a certain block of image		
Hierarchical watermarking depending on local constraints	1. Embed a code bit in a block of pixels 2. Generate the whole sequence of code bits. The watermark is embedded in spatial domain by adding or subtracting a random digital pattern to the given image signal. 3. The embedding depth level depends on the spectral density distribution of the DCT coefficient and on the JPEG quantization table.	1. Resist to the common attack on the watermarked images include clipping and rotation.	The watermark is adapted to local changes in the image.	Find the location of the marker in order to determine the block where the label has been embedded. The decision is taken by thresholding the correlation of the marker with the edge map of the image.

9.3 Image Watermark in Transformed domain

Watermarking Scheme	Method	Advantage	Disadvantage	Detection method
Watermark to wavelet transformed image	Watermarking and compression algorithm are jointly considered. Present the watermarking algorithm in the wavelet domain without compression. The watermark algorithm is integrated within a zero-tree type DWT	1. Robust if engraved at high compression ratio. (Robust watermark must be put in the most significant components.) 2. Transparency	1. Little difference brought by signature engraving. 2. Difference smaller when compression ratio is higher.	Correlation between the watermark and the watermarked image.
A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image	1. Insert the watermark into the middle-frequency range 2. Filter banks are very important and have to be saved for the watermark embedding and the middle-frequency band to insert the watermark are also chosen 3. Replace the coefficient in that band by image achieved using the following method.	1. Achieving both spatial and frequency localization 2. Achieve both perceptual invisibility and robustness to compression. 3. Robustness to noise, image processing techniques, **median filter (which can be consider as a case of pixel permutation, it course destroys the synchronization.). 4. Resist to geometric transform (lots of existing algorithm may not survive) 5. Resilience to counterfeit attempts.		1. The watermarked image is decomposed into object with the stored filter banks, decomposition structure and embedded band information. Then extract the image in the select band. 2. Decompose the image into 4 bands and tile them into pattern, then descramble and perform normalization 3. Correlate the image with the original watermark. 4. Compare with the threshold

9.4 Video Watermark

Watermarking Scheme	Method	Advantage	Disadvantage	Detection method
Scrambling Technique for Video Object Watermarking Resisting to Mpeg-4	1. It modifies some predefined pairs of quantized DCT coefficient in the luminance block of pseudo-randomly selected MBs. 2. It is based on spread-spectrum techniques. Dividing the image into blocks of equal size, them binary sequence is generated using secret key, then add to the image. 3. Special decomposition of mpeg-4 include the fact that VO have significant value 4. Watermark information has to present in each VO	1. Resisting to mpeg-4, especial to video object manipulation 2. Adapt easily any classical spread spectrum watermarking scheme operating in the spatial domain to mpeg 4 format 3. Resist to eventual lossy compression of the segmentation mask due to mpeg4 4. Resist counter geometric attack such as rotations and scaling	According to the classical method used that use for watermarking the VO.	Correlation between S and each block of the watermarked image is calculated. The first step of the recovery scheme consists in summing the different of each pair; the value of the embedded bit is then given by the sign of the sum
A Robust Watermarking Approach for Raw Video	1. Extracting the brightness of the to-be-marked frame, computing its full-frame DFT and then taking the magnitude of the coefficients. 2. The watermark is composed of two alphanumerical strings, Alter the DFT coefficient, then IDFT 3. Watermarking the first frame of each GOP, which was composed of twelve frames, leaving the other ones uncorrupted.	1. Good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression. 2. Resist to geometric transformations as scaling, rotation and cropping.	Decide to watermark one or more frames in GOP, a trade-off between time spent for marking and the degree of robustness needed for the sequence can be achieve	The luminance of the image to be checked for watermark presence is extract again and the magnitude of its DFT is considered.

Object-Based Transparent Video Watermarking	1. Each segmented object is embedded with a unique watermark according its perceptual characteristics. In particular, each object in the video has an associated watermark. 2. As the object experiences translations and transformations over time, the watermark remains embedded with it. An inter-frame transformation of the object is estimated and used to modify the watermark accordingly. 3. If the object is modified too much, or if the watermark exceeds the TEL of the object pixels, a new object and new watermark are defined.	1. As it is object based, the algorithm may be easily incorporated into the MPEG-4 object-based coding framework. 2. In addition, the detection algorithm does not require information regarding the location (i.e., index) of the test frames in the video. 3. resist to video degradations including additive noise, MPEG compression, cropping, and printing and scanning	Affected by noise.	Detection of the watermark is accomplished via a generalized likelihood ratio test. For each frame or object R in the potentially pirated video sequence, the hypothesis test H0: X = R - F= N H1: X = R - F = W' + N is performed. Here F may be an original frame closest to R or may be a composite frame of objects from the object database. In the case when R is an object, F is the corresponding object from the object database. The term W' is the potentially modified watermark, and N is noise.

DWT-based objected watermarking	1. First, decomposed the image through DWT in four levels. 2. The watermark consisting of a pseudo-random binary sequence is inserted by modifying the wavelet coefficients 3. The Max tolerable level of disturb is added to each DWT coefficient. 4. IDWT and mixed watermarked image	Order to be robust against format conversions; the watermark has to be inserted before compression. Otherwise, the drawback of the techniques is that, since the code is directly embedded into the compressed mpeg-4 stream, the copyright information is lost if the video file is converted to a different standard	DWT is not invariant to translation, if the video object is placed in a different position of the new scene, the synchronization between the watermark and the VO is lost	1. Objects present in the scene are extracted frame-by-frame, obtaining s different image for each object. 2. DWT of each image is then computed 3. Correlation between the watermark and the DWT marked coefficients.
Direct sequence watermarking of digital video using m-frame	1. 2mX2m frames separated in time Tf = T/N union of b-bit planes separated in time Tb = Tf/b 2. The suppressed bit planes are candidates for later watermarking. The watermarked video can then be split into the union of two interleaved segment. 3. Extension to a 1-D m-sequence, m-frame, by reshaping the 1D sequence to a pattern.	1. Attempts in corrupting the image to destroy the watermark vender the video unless before damaging the seal itself 2. Watermarked video is also robust to video editing attempts such as sub sampling, frame recording 3. Identifiable from very short segment of video. Individual frames extracted from the video will also contain the copyright information.	The quick and effective way of disturbing a watermarked video is possibly the white noise storm. As a derivative of LSB watermarking, it is expected that the proposed scheme here to be vulnerable even to the smallest of noise attack.	Unknown video needs to be correlated with the expected watermark. Proper correlation, however, requires that the reference m-frames be in sync with the coming video.
Rotation and flipping resilient scheme	1. The DCT coefficient are scanned in a zig-zag order 2. Select the DCT coefficient with a 1-D sequence. The hidden watermark w is designed to have same length with the number of selected coefficient 3. Take the mean and	Synchronization of rotation Synchronization of flipping Synchronization of scale and shape		Let the watermarked image be first mean filtered. The mean filtered DCT coefficient at I is calculated. Recover the watermark and model the CDT coefficient.

	generate a new set of filtered coefficient. 4. To conceal a watermark like a communication process carrying side information, replace the DCT coefficient by a watermark.			
DWT based blind video watermarking	1. Determine the attack parameters and pass the image into the watermark decoder 2. Insert the DWT domain and capacity is maximized by embedding based on a HVS model 4. Use a SS reference watermark and the PN sequence used to embed the watermark corresponds to the "original image" and the watermark embedded in the unsynchronized marked video corresponds to noisy "attacked image". 5. Embed 2 different watermark, 1st is 1-bit watermark used only for geometric reference and is embedded in spatial domain. 2nd is multi-bit mark used for the data payload and embedded in DWT domain	1. Combating geometrical attacks 2. High capacity blind video watermarking system invariant to geometrical attacks such as shift, rotation, scaling and cropping. 3. Invariant a scaling up to 180%, rotation up to 70%, and arbitrary aspect ratio changes up to 200% on both axes 4. Combine the advantage of an algorithm based on the Fourier-Mellin transform (FMT) image registration techniques, with watermarking in the Discrete Wavelet Transform domain		Correlation