Watermarking and Information-Hiding

Shivani Khurana

Abstract- **Watermarking is the process of embedding a watermark into host signal that can be in the form of Audio, Video, and Image .The watermark can be embedded as Logo, Text, and String. The main objective of embedding watermark is to protect the data from unethical hackers over Internet. This watermarking scheme can be embedded in different domains which can be referred as Spatial and Transform domain. Further Transform domain is divided into different types which are DCT, DWT, DFT. Watermarking can also be said as Information-Hiding, because the main factor is to hide the original details from the people who are sitting on internet.**

Keywords- **Watermarking, Audio, Image, Spatial- Domain, Transform-Domain**

I. INTRODUCTION

The need for watermarking of images has gained importance in the past years, due to the rapid growth of digitized media over the internet. Images can copied and distributed, therefore, watermarking schemes are needed in order to serve as copyright systems. A watermark is a secret code carrying identification information about the owner. Generally, a watermark is embedded such that it is invisible. Different types of watermarks like robustness, imperceptible, fragile, source-based etc can be applied. These watermarked video are highly susceptible to pirate attacks such as statistical analysis, frame averaging, frame dropping etc.

INFORMATION HIDING

Information hiding in host data, watermarking, is considered as application of digital media in which the hidden information is transferred via a channel where the noise includes the host and stems from other sources. The amount of information which is hidden is referred as Payload. At the extraction side the watermark should be extracted with confidence. The maximum number of bits which the watermark will carry is called as payload and is important watermarking

2. WATERMARKING AND INFORMATION HIDING PROCESS

In order to see the different aspects of the watermarking problem, depending on the particular applications and the applications requirements, we have to refine the general watermarking model and have a closer look at the successive stages of the watermarking process. These stages comprise:

- Embedding stage
- Extraction stage
- Distribution stage

1) Embedding

Except for some very early watermarking schemes such as patchwork approach, all robust watermarking algorithms operate in transform domain that offers access to the frequency components of the host image. In the embedding stage, the host image is transformed to a domain that facilitates embedding.

2) Distribution

The watermarked image is then distributed – for example published on a web server or sold to a customer.

3) Extraction

Eventually, after the watermarked image has undergone severe distortion, one would like to extract the embedded signature from the host data. This can be done by the party that embedded the watermark, In the first case, the secret key is used to embed the watermark as well as the original image might be available. This tremendously facilitates the watermarking system and makes watermark detection relatively straightforward..

3. TYPES OF WATERMARKING AND INFORMATION HIDING

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

TABLE 1 Classification of Watermarking

Sr. No	Classification Criteria	Types of Watermarking
1.	Media	Text, Image, Audio, Vide
2.	Perceptibility	Visible, Invisible
3.	Robustness	Robust, Fragile, Semi-fragile
4.	Watermark	Noise, Information Tagging, Image
5.	Embedding Domain	
	Spatial domain	LSB, Image Checksum, Patchwork, Random function
	Frequency domain	DCT, DWT, DFT
	Compression domain	MPEG-1.MPEG-2,MPEG-4,JPEG2000
	Hybrid	Visual-Audio, different watermarks & watermarking schemes
6.	Extraction Process	Private, Semi-Private, Public

4. TECHNIQUES OF WATERMARKING {LITERATURE SURVEY}

As a method of intellectual property protection, a digital watermark has recently stimulated significant interest and has become a very active area of research. Although watermarking is a recent field of research, many algorithms have already been proposed both in the academic as well as in the industry. Various techniques are applied in watermarking algorithms.

4.1 Existing methods

Many digital watermarking schemes have been proposed in the literature for still image and videos. Most of them operate on uncompressed videos, while others embed watermarks directly into compressed video. Recently, researchers tend to investigate video watermarking techniques that are robust and invisible. These schemes can be distinguished in terms of the domain that the watermark being embedded or detected, their capacity, real-time performance, the degree to which all three axes are incorporated, and their resistance to particular types of attacks. A classification map of the existing video watermarking techniques is presented. They can be divided into 3 main groups based on the domain in which the watermark is embedded; they are the Spatial domain, the Frequency domain and the MPEG coding structure based method

1. Spatial domain
2. Frequency domain

1. Spatial Domain: In spatial domain the pixels are manipulated directly. No transformations are applied to the host signal during watermark embedding process.

- Correlation based techniques
- Least significant bit modification

In correlation based techniques the correlation properties are more exploited by adding pixels, random noise in video, frame are in still image.

In least significant bit modification technique-: This technique is not much robust because the least significant bits can be replaced by random number of bits which can easily remove the watermark applied to the video.

2. Frequency Domain: It is also referred as transform domain. These are more robust than spatial domain techniques. It can be represented in three forms:

- DCT- Discrete Cosine Transformation
- DFT- Discrete Fourier Transformation
- DWT- Discrete Wavelet Transformation

Discrete Cosine Transformation- In case of DCT it allows an image to be broken up into different frequency bands because becomes very easy to embed watermark information into middle frequency bands. The middle bands are chosen so as to avoid the most visual important parts of the image which have low frequencies.

Discrete Fourier Transformation- It is considered in the field of watermarking because it controls the frequency of the host signal. It enables the schemes further to embed the watermark with the magnitude of its coefficients. The DFT is useful for watermarking purposes because it helps in selecting the adequate parts of the image for embedding in order to achieve the highest invisibility and robustness.

Discrete Wavelet Transformation-: **A**nother method is Discrete Wavelet transformation. It divides an image into different approximations that is (ll), Horizontal {hl), Vertical (lh), and Diagonal (hh).

Watermark based on MPEG coding structures-: These types of structures are basically used to reduce over-all real-time video processing complexity. The main objective of MPEG is motion compensated hybrid coding.

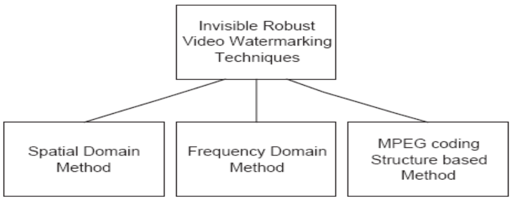
Invisible Robust Video Watermarking Techniques
Spatial Domain Method
Frequency Domain Method
MPEG coding Structure based Method

Fig 1 Classification map of existing Watermark Techniques

5. WATERMARKING AND INFORMATION-HIDING PROPERTIES

There are a number of papers that have discussed the characteristics of watermarks. Some of the properties discussed are robustness, tamper resistance, fidelity, computational cost, and false positive rate.

1. Accuracy -: Watermark detection should be accurate. False positives, the detection of a non-marked image, and false negatives, the non-detection of a marked image, should be few.

2. Robustness-: It must be stable. Robustness of watermark can be best evaluated by frame-dropping, frame-averaging, Statistical-analysis and lossy- compression.

3. Imperceptibility-: The quality of video should not be degraded. A watermark must be imperceptible that means it must prove its uniqueness. If an attacker wants to attack the watermark so it must be strong enough so as it cannot be broken easily.

4. Universal –: The same watermarking algorithm should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products.

5. Unobtrusive-: The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

6. Tamper Resistance-: Tamper-resistance is the most difficult measure we have. It is not easy to be estimated.

7. False Positive Rate -: It can be measured as number of detections successful which indicates the presence of Watermark. It can be estimated as the probability that a false positive will occur in a given detection.

6. WATERMARKING AND INFORMATION HIDING ATTACKS

To extract watermark different attacks can be applied. So as to prove robustness and imperceptibility the watermark should be unique enough and it must be taken into consideration that watermark should be robust enough.The different attacks which are mainly found are frame dropping, statistical analysis, collusion, forgery attacks etc.

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

2. Unintentional attacks –: Typically it includes degradation that occurs during lossy- copying. It may be considered as digital to analog conversion performed by recording of analog tapes, which may alter the document by low- pass filtering..

3. Intentional Attack-: Intentional attacks include direct water mark, desynchronisation in order to prevent its correct detection.

4. Collusion Attack-: Collusion attack is used to extract the watermark from the watermarked video. Collusion attack uses different watermarks on different scenes of the same video using same key.

5. Cryptographic Attack-: These types of attacks are based on the security. For this encryption/decryption of host signal is very important. This kind of attacks requires high computational complexity.

6. Protocol Attack-: This type of attacks mainly targets the entire concept of watermarking application. In this type of attack the attacker subtracts his own watermark from the watermarked information and proves ownership of data

7. Removal Attack-: As the word substitute's removal is basically to remove the watermark form the cover signal. This type of attacks are based on denoising, quantization, D/A or A/D conversions.

8. Active Attack –: Here the attacker tries to remove the watermark or make it detectable. Here the hacker tries to remove the watermark or make it undetectable. This type of attack is critical for many applications, including owner identification, proof of ownership, fingerprinting, and copy control, in which the purpose of the mark is defeated when it cannot be detected.

Table 2 Watermarking Attacks

Attack	Classification
Collusion attack	Removal attacks
Inversion attack	Ambiguity attacks
Affine transformation attack	Detection-disabling attacks
Attack	**Classification**
Noise attack, Compression attack	Simple attacks
Detector observation attack	Removal attacks
Inserter observation attack	Removal attacks
Collusion attack	Removal attacks
DVD tampering attack	Removal attacks
DVD scrambling attack	Removal attacks
Non-linear filtering attack	Removal attacks
Counterfeit attack	Ambiguity attacks
Attack operators	Simple attacks
Stir Mark attack	Simple attacks, Detection-disabling attacks
Echo attack	Removal attacks
Mosaic attack	Detection-disabling attacks
Detector observation attack	Removal attacks
Unzign attack	Simple attacks, Detection-disabling attacks

7. CONCLUSION AND FUTURE SCOPE

Watermarking is a copy protection system that allows tracking back illegally produced copies of the protected multimedia content. The main advantage of watermarking is that the watermark is embedded permanently in visual data. Most data hiding systems take advantage of human perceptual weaknesses, but have weaknesses of their own. In areas where cryptography and encryption are being outlawed, citizens are looking at "Steganography" to circumvent such policies and pass messages covertly. Commercial applications of "Steganography" in the form of digital watermarks are currently being used to track the copyright and ownership of electronic media. A generic watermarking framework has been designed and implemented as a plug-in for an existing open source multimedia streaming library. .

For practical use, several improvements should be made. Firstly, the embedding process should be optimized to preserve the former bit-rate of the video sequences. In order to increase robustness against direct removal attack, the watermark should be embedded into textured areas only. Textured areas provide more non-zero coefficients in the residual than uniform areas.

8. REFERENCES

[1] Vivek Kumar Aggarwal, A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of M. Tech. "Perceptual Watermarking of digital video using the variable temporal length 3D, DCT"

[2] Mohd Shahidan Abdullah, Azizah Abd Manaf ,"An Overview of Video Watermarking Techniques"

[3] Chan Pik Wah pwchan@cse.cuhk.edu.hk "Multimedia Security Digital Video Watermarking" Term Paper (Fall 2002)

[4] Matt L. Miller Ingemar J. Cox Jean-Paul M.G. Linnartz Ton Kalker Signafy Inc. NEC Research Institute Philips Research 4 Independence Way 4 Independence Way Prof. Holstlaan 4 Princeton, NJ 08540 Princeton, NJ 08540 5656 AA Eindhoven USA The Netherlands "A Review of Watermarking Principles and Practices"

[5] Ingemar J. Cox, Matt L. Miller and Jeffrey , "Water marking Applications and their Properties"

[6] Ingemar J. Cox, "A Secure, Robust watermark for Multimedia"

[7] Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review, 1999

[8] Fabien A. P. Petit colas, Ross J. Anderson and Markus G. Kuhn Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999. "Information Hiding Survey"

[9] Sabu M Thampi Assistant Professor, Department of Computer Science & Engineering LBS College of Engineering, Kasaragod Kerala-671542, S.India smtlbs@yahoo.co.in "Information Hiding Techniques: A Tutorial Review"

[10] Shuichi Shimizu IBM Japan, Tokyo Research Laboratory 1623-14 Shimotsuruma, Yamato-shi, Kanagawa 242-8502, Japan shue@jp.ibm.com, "Performance Analysis of Information Hiding"