Volume : 2 | Issue : 1 | Jan 2013 • ISSN No 2277 - 8179

Research Paper

Engineering

KEYWORDS: Index Terms— Digital video Watermarking, DWT, Video Copy Protection, Digital Video Watermarking Techniques

A Survey on Digital Video Watermarking: Types, Applications & Techniques

Hitesh D. Panchal | Lecturer in E.C., Government Polytechnic for Girls, Ahmedabad, Gujarat, India

ABSTRACT

Digital Television offers many potential benefits in picture quality as it is able to store and copy material without losing the quality or fidelity; hence resulting in superior quality as compared to the analog form due to its noise-free transmission. At the same time, there has been tremendous growth in both network and performance of computers, which directly increases considerable challenges for copyright enforcement. However, the fact that an unlimited number of perfect copies can be illegally produced is a serious threat to the rights of the content owners. As such, there is a great desire for copyright system that can preserve both the economic value of digital data and the rights of the owners. This is a significant limitation and encryption alone may not be sufficient for any copyright protection. In fact, it is mainly concerned with secure communication but not the copyright protection. Digital watermarks have been proposed as a way to handle this challenging issue. A watermark can act as an invisible signature to discourage copyright violation.

1. INTRODUCTION

Watermarking compliments (and does not replace) encryption. A digital watermark is a piece of information that is hidden directly in the media content, in such a way that it is imperceptible to a human visual system (HVS) and always remains present, but easily detected by a computer. The principal advantage of this is that the content is inseparable from the watermark. This makes watermarks suitable for several applications.

In general, to give the video a sense of ownership or authenticity, the desirable properties of watermarking scheme should comply with the following requirements [1]:

- The digital watermark embedded into the video data should be invisible or at least hardly perceptible.
- A digital watermark should be statistically invisible so it cannot be removed by intentional or unintentional operations on the bit stream or on the decoded video without degrading the perceived quality of the video too much that it makes the video without any commercial value. This requirement is called robustness.
- Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation.
- Watermarking in the bit stream domain may not increase the bit-rate (at least for constant bit-rate applications).
- It can be assumed that incorporating a watermark into a compressed video has to obey much more constraints than incorporating a watermark into uncompressed video. Therefore, it is advantageous to do so in the domain of uncompressed video wherever possible.

2. DIGITAL WATERMARKING TYPES

The classification of Digital watermarking according to the different viewpoint is summarized in Table 1 [2].

Classification		Content
Inserted media category		Text Image Audio Video
Perceptivity of watermark		Visible Invisible
Robustness of watermark		Robust Semi-fragile Fragile
Inserting watermark type		Noise Information tagging Image
Processing method	Spatial domain	LSB Image checksum Patchwork Random function
	Frequency domain	Look-up table Spread spectrum: DCT, Wavelet (DWT), Fourier (DFT)
	Compression domain	MPEG1 MPEG2 MPEG4 JPEG2000
	Hybrid	Visual-audio Different watermarks Different watermarking scheme
Necessary data for extraction		Private Semi-private Public

Table :1 Classification of watermarking according to several viewpoints

Digital watermarking can be applied to many different types of documents, including text, audio, image and video. Watermark techniques can be classified into visible and invisible watermarks. In general, invisible watermarks are mostly used. The oblivious meaningful video watermarking remains a challenging problem since the original video is often unavailable due to videos' bulky volume. Watermarks, on the other hand, need robustness to protect the ownership from various attacks. They can be classified into three categories, robust, semi-fragile and fragile watermarks.

A watermark can be a random sequence with one information bit or multiple-bit meaningful information. The random sequence watermark is more robust in general; however, embedding meaningful watermark is more important in some applications. For image types, there are binary image, stamp, logo and label. Moreover, watermark processing methods are classified into four categories: spatial domain, frequency domain, compression domain and hybrid. Finally, watermark extraction methods can be classified as private, semi-private and public watermarking, according to the necessity of the original media.

1. VIDEO WATERMARKING APPLICATIONS

The following classification is based on the type of information conveyed by the watermark [3].

Application Class	Purpose of the embedded watermark	Application Scenarios
Protection of Intellectual Property Rights	Conveys information about content ownership and intellectual property rights	Copyright Protection, Copy Protection, Fingerprinting
Content Verification	Ensures that the original multimedia content has not been altered, and/or helps determine the type and location of alteration	Authentication Integrity Checking
Information hiding	Represents side-channel used to carry additional Information.	Broadcast Monitoring System Enhancement

Table: 2 Classification of video watermarking applications

3.1 DIGITAL WATERMARKING FOR COPYRIGHT PROTECTION

Copyright protection appears to be one of the first applications digital watermarking was targeted for. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. If users of digital content (music, images, and video) have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the

watermarked content. A copyright owner distributes his/her digital content with his/her invisible watermark embedded in it. In the case of a copyright ownership dispute, a legal owner should be able to prove his ownership by demonstrating that he owns the original work, and that the disputed work has been derived from the original by embedding a watermark into it.

3.2 DIGITAL WATERMARKING FOR COPY PROTECTION

The objective of a copy protection application is to control access to and prevent illegal copying of copyrighted content. It is an important application, especially for digital content, because digital copies can be easily made, they are perfect reproductions of the original, and they can easily and inexpensively be distributed over the Internet with no quality degradation. There are a number of technical and legal issues that need to be addressed and resolved in order to create a working copy protection solution. Those issues are difficult to resolve in open systems, and we are not aware of the existence of an open system copy protection solution.

3.3 DIGITAL WATERMARKING FOR FINGERPRINTING

There are some applications where the additional information associated with a digital content should contain information about the end user, rather than about the owner of a digital content. For example, consider what happens in a film making environment. During the course of film production, the incremental results of work are usually distributed each day to a number of people involved in a movie making activity.

Those distributions are known as film dailies, and they are confidential. If a version is leaked out, the studio would like to be able to identify the source of the leak. The problem of identifying the source of a leak can be solved by distributing slightly different copies to each recipient, thus uniquely associating each copy with a person receiving it.

3.4 DIGITAL WATERMARKING FOR FRAUD AND TAMPER DETECTION

When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated or falsified. This can be achieved by embedding a watermark in the data.

3.5 DIGITAL WATERMARKING FOR BROADCAST M-O-NIT-O-RING

Many valuable products are regularly broadcast over the television network: news, movies, sports events, advertisements, etc. Broadcast time is very expensive, and advertisers may pay hundreds of thousands of dollars for each run of their short commercial that appears during commercial breaks of important movies, series or sporting events. The ability to bill accurately is this environment is very important. It is important to advertisers who would like to make sure that they will pay only for the commercials which were actually broadcast. And, it is important for the performers in those commercials who would like to collect accurate royalty payments from advertisers.

3.6 Watermark Requirements

Nowadays, due to the highly developed technology of network, digital documents such as texts, images and videos can be distributed rapidly and widely via the World Wide Web in a cost-efficient way. As a result, documents can be easily duplicated and distributed without the owner's consent. Therefore it brings new challenges to security, to keep the distribution of digital multimedia work both profitable for the document owners and reliable for the customers.

The ideal watermark should have the following two properties:

- Invisibility: the watermark should keep imperceptible to avoid being overwritten.
- Robustness: the watermark must be difficult to be removed by adding noises.

4. DIGITAL VIDEO WATERMARKING TECHNIQUES

Many digital watermarking schemes have been proposed in theliterature for still images and videos. Most of them operate on uncompressed videos [4, 5], while others embed watermarks directly into compressed videos [6, 7]. 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 based on processing domain is shown in Figure 1. They can be divided into 2 main groups based on the domain that the watermark is embedded; they are spatial domain, frequency domain. Most of the proposed video watermarking scheme based on the techniques of the image watermarking and applied to raw video or the compressed video.

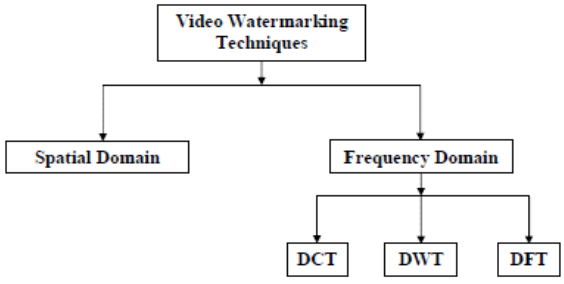

Figure: 1 Digital video watermark techniques

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. In the following sections, each class of algorithms is briefly described. Besides, we present the important idea, strength and limitation introduced by these schemes.

5.1 SPATIAL DOMAIN WATERMARKS

We first review the video watermarking techniques in the spatial domain. Algorithms in this class generally share the following characteristics:

- The watermark is applied in the pixel or coordinate domain.
- No transforms are applied to the host signal during watermark embedding.
- The watermark is derived from the message data via spread spectrum modulation.
- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal.

The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. As a result they have proven to be most attractive for video watermarking applications where real-time performance is a primary concern. However, they also exhibit some major limitations: The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks; lack of consideration of the temporal axis results in vulnerability to video processing and multiple frame collusion; and watermark optimization is difficult

using only spatial analysis techniques. The three methods that fall into this class can be distinguished by the dimensionality of the watermark pattern.

5.2 FREQUENCY DOMAIN WATERMARKS

Generally, three transformed domain methods DCT, DFT and DWT are used for watermarking. We discuss these methods in next section in detail with advantage and disadvantages of these methods. We also discuss some other methods recently used.

5.2.1 DCT DOMAIN WATERMARKING [9]

DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. The main steps of any block based DCT algorithm are as follows:

Steps in DCT Block Based Watermarking Algorithm
1) Segment the image into non-overlapping blocks of 8x8
2) Apply forward DCT to each of these blocks
3) Apply some block selection criteria (e.g. HVS)
4) Apply coefficient selection criteria (e.g. highest)
5) Embed watermark by modifying the selected coefficients.
6) Apply inverse DCT transform on each block

5.2.2 DWT DOMAIN WATERMARKING

In the last few years wavelet transform has been widely studied in signal processing in general and image compression in particular. In some applications wavelet based watermarking schemes outperforms DCT based approaches [8].

CHARACTERISTICS OF DWT

- The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely.
- Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution.
- Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL).
- The larger the magnitude of the wavelet coefficient the more significant it is.
- Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved.
- High resolution sub bands helps to easily locate edge and textures patterns in an image.

ADVANTAGES OF DWT OVER DCT

- Wavelet transform understands the HVS more closely than the DCT.
- Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution.
- Visual artifacts introduced by wavelet coded images are less evident compared to DCT because wavelet transform doesn't decompose the image into blocks for processing. At high compression ratios blocking artifacts are noticeable in DCT; however, in wavelet coded images it is much clearer.

DISADVANTAGES OF DWT OVER DCT

Computational complexity of DWT is more compared to DCT. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient.

5.2.3 DWT WATERMARKING

DWT based watermarking schemes follow the same guidelines as DCT based schemes, i.e. the underlying concept is the same; however, the process to transform the image into its transform domain varies and hence the resulting coefficients are different. Wavelet transforms use wavelet filters to transform the image. There are many available filters, although the most commonly used filters for watermarking are Haar Wavelet Filter, Daubechies Orthogonal Filters and Daubechies Bi-Orthogonal Filters. Each of these filters decomposes the image into several frequencies.

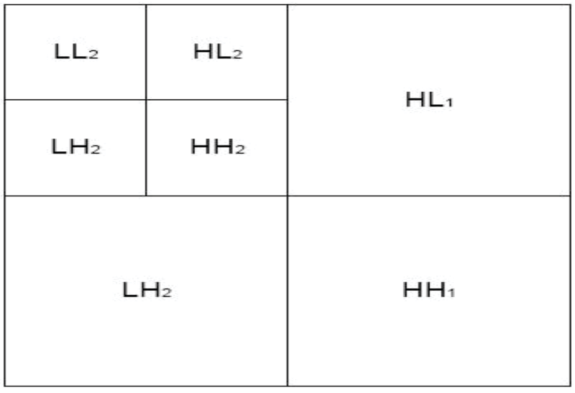

Figure: 2 Scale 2-Dimensional Discrete Wavelet Transform

Single level decomposition gives four frequency representations of the images. These four representations are called the LL, LH, HL, HH sub bands. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown in Figure 2. DWT algorithms can be classified based on their decoder requirements as Blind Detection or Non-blind Detection. Blind detection doesn't require the original image for detecting the watermarks; however, non-blind detection requires the original image.

5.2.4 DFT DOMAIN WATERMARKING

DFT domain has been explored by researches because it offers robustness against geometric attacks like rotation, scaling, cropping, translation etc [9].

CHARACTERISTICS OF DFT

- DFT of a real image is generally complex valued, which results in the phase and magnitude representation of an image. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transforms.
- Scaling of image results in amplification of extracted signal and can be detected by correlation coefficient. Translation of image has no result on extracted signal.

CO-EFFICIENT SELECTION CRITERIA

- Modification to the low frequency coefficients can cause visible artifacts in the spatial domain. Hence, low frequency coefficients should be avoided
- High frequency coefficients are not suitable because they are removed during JPEG compression.
- The best location to embed the watermark is the mid frequency.

Volume : 2 | Issue : 1 | Jan 2013 • ISSN No 2277 - 8179

REFERENCE

[1] Development of a robust blind digital video watermarking algorithm using discrete wavelet transform , Ahmed a. Bahaa al-deen, Master of science, University putra Malaysia, 2007 |[2] A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC ,Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, 2009 IEEE|[3] Multimedia Security: Watermarking Techniques , Edin Muharemagic and Borko Furht, Department of Computer Science and Engineering, Florida Atlantic University, U.S.A.,2004 |[4] F. Deguillaume, G. Csurka, J. Ruanaidh, and T. Pun, "Robust 3D DFT video watermarking," Proceedings Electronic Imaging' 99: Security and Watermarking of Multimedia Contents, Vol. 3657, San Jose, CA, Jan. 1999.|[5] M. Ejima and A. Miyazaki, "A wavelet-based watermarking for digital images and video," Proceedings International Conference on Image Processing (ICIP-2000), Vol. 3, pp. 678-681, Vancouver, Canada, 2001.|[6] S. Arena and M. Caramma, "Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking," Proceedings International Conference on Image Processing (ICIP-2000), Vol. 3, pp. 438-441, Vancouver, Canada, 2000|[7] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Proceedings Signal Processing, Vol. 66, pp. 283-301, 1998.}[8] Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery CHAN Pik-Wah, The Chinese University of Hong Kong, July 2004|[9] (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 5, August 2010, http://sites.google.com/site/ijcsis, ISSN 1947-5500