RESEARCH PAPER | Engineering | Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X



A Survey on Digital Video Watermarking

KEYWORDS: Watermarking, Spatial Domain, Frequency Domain, Copy Right Protection.

Mr.Krunal R. Patel	Mr.Parimal A. Patel
ME (CSE Student), S. P. B. Patel Engineering College, Mehsana, Gujarat	CSE-IT Department, S. P. B. Patel Engineering College, Mehsana, Gujarat

ABSTRACT At the leading edge of the information world everything is in available in form of digital media. Digital watermarking was introduced to provide the copy right protection and owners' authentication. Digital video watermarking is the process to embedding a digital code into digital video sequences. Digital video watermarking nothing but a sequence of consecutive still images. In recent few years the applications based on video like, pay-per-view, video-on-demand, video broadcasting are becomes more and more popular, so the requirement of a secure video distribution increases. In this paper, the concept of digital video watermarking, its terminology, principle, properties, applications, and classification is introduced. Classification is based on the types of key used for embedding/detecting purpose, types of carriers and the working domains of watermark embedding are included.

General Terms

Digital Video Watermarking.Survey

1. INTRODUCTION

Today, digital media is available in a large scale, which can be easily copied and rapidly spread. People can acquire the copy of a digital media very easily; it may lead to large-scale unauthorized copies, which effect the development of the publishing industry. The owner of the content has to use some protection mechanism such as encryption or digital watermarking. Encryption is no longer sufficient for copy right protection and authentication, so digital watermarking is widely used. [1][2][3] It is an art of embedding information in invisible and robust manner. [1][3] Because the copy and temper of video is quite easy, in order to protecting copy right, digital video watermarking technology taken as an important and more urgent component. [4] Recently, video based applications such that video conferencing, wireless videos, video broadcasting, set-top box, video-on-demand, videophone and internet multimedia are becoming more and more popular and has increased the demand for a secure distribution of videos. [3][5]

In fact any image watermarking technique can be extended to watermarking videos, but in reality video watermarking techniques need to meet other challenges like video coding technologies, large volume of data, blind watermarking detection, the unbalance between motion and motionless region, some special attacks like frame averaging, frame swappingstatistical analysis and other real-time features than that in image watermarking scheme. [2][3][6].

2. VIDEO WATERMARKING

2.1 Digital Watermarking

Digital watermarking is nothing but a digital code embedded into digital cover content e.g. text, image, audio and in our case video sequence. [2][3][7] A watermark can be any random or serial number, ownership identifier, information about the creator, date etc.[2] It can carry any unlimited information, but as more information watermark carry, the original information will be more vulnerable. So the amount of watermark must be limited by the size of an original message, here video sequence. As watermark prefers to robustness, it carries tens to thousands bits per one video frame. [7]

2.2 Video Watermarking Terminology

Digital Video: Digital video is a sequence or collection of consecutive still images.

Payload: The amount of information that can be embedded into the video sequence.

Security: In watermarking the security is assured in the same way as in encryption. Though the algorithm of watermarking process is public, security depends on the choice of the key. [2]

2.3 The principle of video watermark

The complete process of digital video watermarking is described into four steps: Watermark insertion or embedding, Watermark transmission or distribution through a channel, Watermark extraction or detection and Watermark decision (Figure 2).

Watermark embedding algorithm embedded a watermark into original video using a Key, which may be either public or symmetric key. Then the watermarked video transmitted over the channel. At the receiver side, watermark detection/extraction algorithm used to detect a watermark. In last step, watermark decision, watermarking system analyzes the extracted data. [6]

2.4 Properties of Video Watermark

For digital video watermark some most important characteristics or properties of watermarking process are required. [2][3][6] Such as,

2.4.1 Robustness:

The watermark should be impossible to remove from watermarked video, without the sufficient knowledge of an embedding process. The robust one is specially designed to withstand a wide range of attacks. [8]

2.4.2 Imperceptibility:

The watermark embedded into the digital video sequence should be invisible to Human Vision System (HVS).

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

2.4.3 Unambiguous:
The extracted watermark should uniquely identify the original owner of the video.

2.4.4 Loyalty:
A watermark has a high reliability, if the degradation it causes is very difficult to perceive for the viewer.

2.4.5 Computational Cost:
Digital video watermark system includes, embedding and detecting process both should be fairly fast and should have low computational complexity.

2.4.6 Interoperability:
Watermark system must be interoperable for the compressed and decompressed operations.

2.4.7 CBR (Constant Bit Rate):
In the bit stream domain, watermarking should not increase the bit rate.

2.4.8 Random detection:
In video watermarking the detection of watermark can be done in any position of video.

2.4.9 Blind detection scheme:
Non-blind detection scheme require the original data, but for video sequence it is very inconvenient to use original data because of its huge content compare to image. While a blind detection scheme doesn't require a original data, so it is useful for video watermarking.

2.5 Applications of Video Watermarking
The major applications of digital video watermarking includes copyright protection, video authentication, broadcast monitoring, copy control, fingerprinting, taper resistance, video tagging, ownership identification and enhance video coding. [1][2][3][8][9] Some of them are explained below:

2.5.1 Copyright protection:
Copyright protection is the very first targeted application for digital watermarking. In digital multimedia, watermarking is used as copyright protection to identify the copyright owner.

2.5.2 Video authentication:
Authentication means storing the signature into the header section, but the header field still be prone to tempering. So we can directly embed this type of authentication information directly as a watermark.

2.5.3 Broadcast monitoring of video sequences:
In television network different products are distributed over the channel. A broadcast observation system must be built in order to check the entire broadcasted channel. Watermark is used for this type of broadcast monitoring system by putting a unique watermark for each video to broadcast.

2.5.4 Copy control:
Watermarking system has the available technologies in which the information is secured into the header and it prevents from copying of that data.

2.5.5 Fingerprinting (Distribution):
Pay-per-view and Video-on-demand are two real-time applications of video streaming, in which digital watermarking is used to enforce a fingerprinting policy. The customer ID is embedded into the video as a watermark to track back any user breaking his license agreement.

3. CLASSIFICATION OF DIGITAL VIDEO WATERMARKING

Digital video watermarking scheme can be classified into three different ways: according to their types of keys, types of carrier and working domain for watermark embedding.

3.1 According to the types of keys
As shown in Figure 2 the watermark insertion and detection process required a key. If both the process uses a same key, it is called symmetric watermarking, otherwise known as asymmetric or public key watermarking. [4]

The security of the watermarking is determined by the key. If we use any arithmetic on a single key, an attacker can make use of this and can temper the watermarked content. [10] It is advised to design the key is based on the features of the video frames; so on changing the content of the video key is automatically changed.

3.2 According to the types of carriers
According to the embedding strategy, video watermark algorithm can be divided into different three types (Figure 3): Original uncompressed based video watermarking (Embed 1); embedding watermark in the video encoder (Embed 2) and compression based video watermarking (Embed 3). [4][6][12]

3.2.1 Embed/Extract 1:
In this type of watermarking, watermark is directly embedded into the Original video sequences and after that watermark containing video sequence is encoded. [6] Advantage of this type is we can embed watermark easily but the disadvantage is that it will increase the bit rate of video data stream and also after compression watermark may be lost.

3.2.2 Embed/Extract 2:
In this type of watermarking, watermark embedding and detection are done at the encoder and decoder. [4][6] There are different video compression standard are available today: MPEG-1, MPEG-2, and MPEG-4. [4] Advantage of this type is that it does not increase the bit rate of video data stream and it is relatively simple method of watermark embedding in the transform domain.

3.2.3 Embed/Extract 3:
In this type of watermarking, watermark is embedded into the compressed domain. Advantage of this type is computational complexity is lower compare to other types, but the disadvantage is that the compressed bit rate constraints the size of the watermark data.

3.3 According to the working domain for watermark embedding
According to the working domains of watermark algorithms,video watermarking techniques are classified into different two domains: pixel domain or spatial domain and transform domain or frequency domain. [2][3][4][8] Although some hybrid approaches are also proposed by some researchers. [11]

3.3.1 Spatial domain watermarks:

In spatial domain the watermark is embedded in the original video by simply adding or replacing the bits of selected region. The different characteristics of this domain are:

- These domain techniques are very simple to understand.
- The time complexity is low which favors the real time implementations.

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

- Watermark is applied to the pixels, no transform are applied to the original content during watermark embedding.
- At the receiver side, watermark can be detected by correlating expected pattern with the received data.
- In this domain the watermark information is embedded in the redundant part of the carrier.

Several methods of watermarking in spatial domains are:

3.3.1.1 Correlation based techniques:
In correlation based technique, the watermark W(x,y) is added to the original content O(x,y) according to the equation(1).

$$Ow(x,y) = O(x,y) + kW(x,y) \qquad (1)$$

In equation (1), k is a gain factor and Ow is the watermarked content. As we increase the value of k, it will expense the quality of watermarked contents.

3.3.1.2 Least Significant Bit modification (LSB):
Least Significant Bit (LSB) method is the simplest technique of this domain. In this scheme the watermark is simply embedded into the least significant bits of the original video or flips the LSB. Due to its simplicity, it is the most popular scheme, but some limitations are also there like, poor quality of the produced video, inefficient in dealing with the various attacks, least robustness and lack of imperceptibility.

3.3.2 Frequency domain watermarks:
In frequency or transform domain the watermark information is embedded into the transform domain of the host signal for example DCT or wavelet domain.

The advantages of using this approach are:

- Watermark signal, embedding into the original content is not limited to some pixels but it is distributed to all the pixels in the domain.
- These domain methods can be compatible to the video compression standards.
- In this domain, some features of the human perceptual system can be integrated into the encoding process.

3.3.2.1 DCT:
Discrete Cosine Transform (DCT) is a classic and quite an important method for video watermarking. A lot of digital video watermarking algorithms embed the watermark into this domain. The usability of this transform is because that most of the video compression standards are based on DCT and some other related transforms. [12] In this domain some DCT coefficients of the video are selected and divided into groups, and then the watermark bits are embedded by doing adjustment in each group. [12][13]

3.3.2.2 DWT:
Discrete Wavelet Transform (DWT) is a transform based on frequency domain. [14]

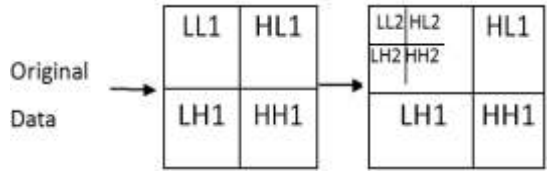


Figure 1: Frequency distribution after DWT
As shown in figure 1 the distributions of the frequency is transformed in each step of DWT, where L represents Low frequency, H represents High frequency and subscript behind them represents the number of layers of transforms. Sub graph LL represents the lower resolution approximation of the original video, while high-frequency and mid-frequency details sub graph LH, HL and HH represents vertical edge, horizontal edge and diagonal edge details. The process can be repeated to compute the multiple scale wavelet decomposition as shown in figure 1.

4. ACKNOWLEDGMENTS
I would like to thank my guide, Mahesh Goyani, for his professional leadership and valuable advice.

REFERENCE
[1] Gwena.el Do.err, Jean-Luc Dugelay, "A guide tour of video watermarking", Signal Processing: Image Communication 18 (2003) 263–282. | [2] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC". | [3] Vivek Kumar Agrawal, "Perceptual watermarking of digital video using the variable temporal length 3D-DCT", IIT, Kanpur, 2007. | [4] Luo Wei, "A Improved Video Watermarking Scheme Based on Spread-spectrum Technique", 2010 International Conference on Networking and Digital Society, 511-514. | [5] Myoung-Hoon Lee, Vincent So, and Jiying Zhao, "A Key-Code Watermarking Algorithm for Video Content Protection", 702-706. | [6] Xing Chang, Weilin Wang, Jianyu Zhao, Li Zhang,"A Survey of Digital Video Watermarking",2011 Seventh International Conference on Natural Computation,61-65. | [7] Martin Zlomek,"Master thesis on Video Watermarking" ,Prague, April 19, 2007. | [8] C. Navya Latha,K. Sumanth, "Digital Video Watermarking".