



Digital Watermarking for MPEG video

Author

Biswajit Biswas

Table of Contents

ABSTRACT.....	3
INTRODUCTION.....	4
REQUIREMENTS FOR WATERMARKING METHOD.....	4
VIDEO WATERMARKING PRINCIPLES.....	5
CHALLENGES FOR VIDEO WATER MARKING.....	5
UNCOMPRESSED DOMAIN WATERMARKING FOR VIDEO	6
COMPRESSED DOMAIN WATERMARKING FOR VIDEO	6
<i>Differential Energy Watermark</i>	7
<i>Spread Spectrum technique</i>	8
<i>JAWS</i>	9
CONCLUSION	9
REFERENCES.....	10

Abstract

Digital Watermarking is a data hiding technique where an information or message is hidden inside a signal transparent to the user. This method is used for copyright protection of digital media. Watermarking differs from encryption in a way that in the former case a general user is allowed to access, view and interpret the signal but cannot claim the ownership of the content, whereas in case of encryption the very access to the signal itself is denied. Watermarking is thus more popular than encryption where the content generator wants the general user to enjoy the content but shall not infringe upon the copyright. Digital representation of the signal has made the job of Watermarking easier and cost effective, and thus this technology is already developing very fast among the media industry. This paper describes the methods of Watermarking for MPEG based video content.

Digital Watermarking for MPEG video

Introduction

Since ancient times, there has been an effort to hide information within seemingly harmless information to avoid unwanted attention. The science of concealing information was later to be known as “steganography” and the current technology of “Digital Watermarking” has taken its root from it. The term “watermark” in terms of digital data was taken from the concept of watermarks used to prevent faking of currency notes.

“Watermarking” deals with embedding information like name of the creator, status, recipient, etc. into the host data in such a way that it remains transparent or undetectable. The watermark information should be embedded in such a way that this should not be detectable and removable even after many spurious or innocuous attempts. Watermarking can be done for any form of digital data – text, image, audio, or video where copyright needs to be protected.

Methods for embedding watermark information may vary between types of media, but the basis of these methods remain more or less same. In the following sections we will discuss the requirements for selecting a particular Watermarking method and discuss digital video Watermarking in detail.

Requirements for Watermarking method

A digital media in its journey, from the content creator’s studio to the end user, undergoes several phases of changes – analog, digital, transform based signal processing, coding, packetisation, fragmentation, decoding and so on. The selected Watermarking method for embedding information has to be very effective such that the hidden information is never detectable and removable under any condition during these several cycle of changes.

Requirements for Watermarking methods can be generally classified as below:

- a) Transparency
- b) Security
- c) Ease of embedding and retrieval
- d) Robustness
- e) Effect on bandwidth
- f) Interoperability

Transparency: The most fundamental requirement for any Watermarking method shall be such that it is transparent to the end user. The watermarked content should be consumable at the intended user device without giving annoyance to the user. Watermark only shows up at the watermark-detector device.

Security: Watermark information shall only be accessible to the authorized parties. Only authorized parties shall be able to alter the Watermark content. Encryption can be used to prevent unauthorized access of the watermarked data.

Ease of embedding and retrieval: Ideally, Watermarking on digital media should be possible to be performed “on the fly”. The computation need for the selected algorithm should be minimum.

Robustness: Watermarking must be robust enough to withstand all kinds for signal processing operations, “attacks” or unauthorized access. Any attempt, whether intentional or not, that has a potential to alter the data content is considered as an attack. Robustness against attack is a key requirement for Watermarking and the success of this technology for copyright protection depends on this.

Effect on bandwidth: Watermarking should be done in such a way that it doesn’t increase the bandwidth required for transmission. If Watermarking becomes a burden for the available bandwidth, the method will be rejected.

Interoperability: Digitally watermarked content shall still be interoperable so that it can be seamlessly accessed through heterogeneous networks and can be played on various playout devices that may be watermark aware or unaware.

Video Watermarking Principles

Video Watermarking is one of the most popular techniques among the various Watermarking techniques currently in use. This is because maximum occurrences of copyright infringement and abuse happen for video media content.

Challenges for video water marking

The challenges for video Watermarking are as follows:

- a) Video media is susceptible to increased attacks than any other media
- b) Video content is sensitive to subjective quality and Watermarking may degrade the quality
- c) Video compression algorithms are computationally intensive and hence there is less headroom for Watermarking computation
- d) Video is bandwidth hungry and that is why it is mostly carried in compressed domain. Therefore, Watermarking algorithm shall be adaptable for compress domain processing.
- e) For low-bitrate video, Watermarking poses additional challenges, as there is less room for watermark data.
- f) During video transmission, frame drops are very usual. If watermark data spreads over many frames, in case of frame drops, watermark data may become irretrievable. Watermarking should be robust enough against this phenomenon.

Watermarking for video can be performed for both compressed and uncompressed domains. A simple spread spectrum technique can be used for uncompressed video as shown by Hartung

and Girod [1], that meets all of the criteria required by Watermarking. Whereas, for compressed domain video many approaches are possible, including advanced tools like gain adjustment, drift adjustment and bit-rate control for containing data rate and artifacts [2]. For obvious reasons, compressed domain has more acceptance over uncompressed domain processing.

Uncompressed domain Watermarking for video

Spread spectrum scheme is used to embed the watermark data into the raw uncompressed video. Here, watermark data is considered as narrow band signal and video is considered as wide band signal. Narrow band signal is spread for increasing redundancy and then modulated with binary pseudo noise sequence. This modulated sequence is called spread spectrum watermark, which is added linearly to the video data. The reason for adding pseudo-noise is to prevent detection and attack of the watermark data. Figure 1 captures the method:

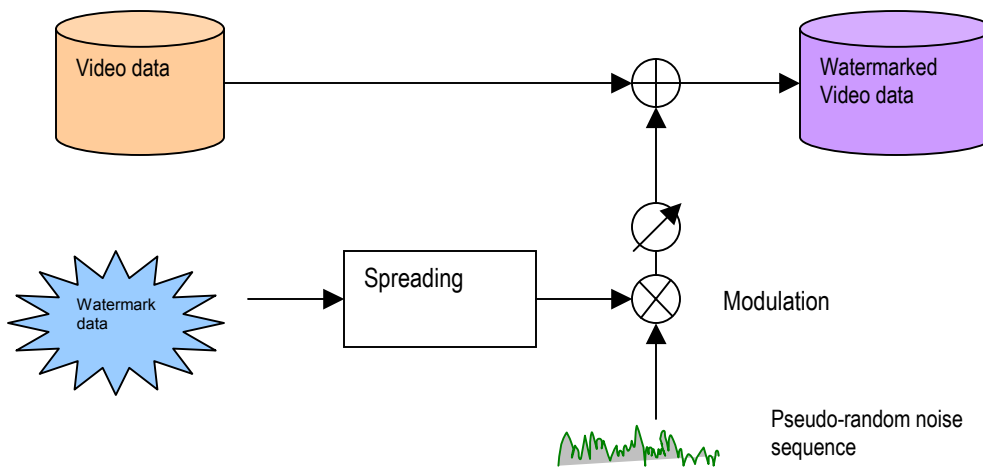


Figure 1: Spread spectrum watermark embedding in uncompress domain

Any authorized detector, which has the knowledge of the pseudo-random signal that was used for watermark embedding purpose, can recover the watermark. The steps are shown in figure 2 below.

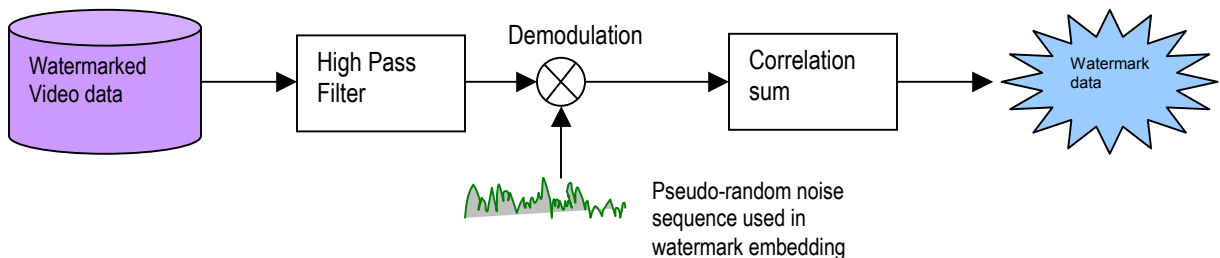


Figure 2: Spread spectrum watermark recovery in uncompress domain

Compressed domain Watermarking for video

Due to high bandwidth requirement, video is usually carried in compressed domain. Different encoding methods like H.261, H.263, MPEG-2, and MPEG-4 are used to compress video.

All of them use hybrid coding, which is motion compensated prediction-based algorithm. Encoding methods may vary from simple to complex depending on target bandwidth required.

As discussed in previous section, Watermarking for compressed video data in real time is very challenging because of computation requirements. The computation requirement is almost equal to (if not more) a decoder.

Watermarking algorithms usually tend to become more and more complex as bit rate for the output video decreases. For low-bit rate channels there is less headroom for watermark data and spreading cannot be done effectively. Hence, algorithm chosen should be robust enough to withstand different kinds of attack. Also, Watermarking scheme should vary for different application scenarios. Video bit-stream should be capable of carrying multiple watermarks as in the situation for Video-On-Demand. See Figure 3.

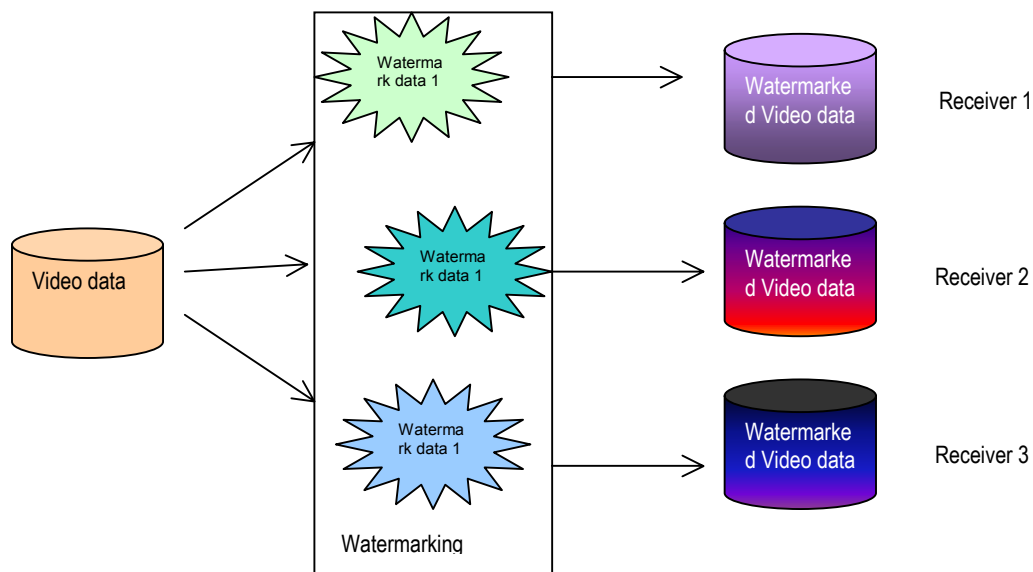


Figure 3: Watermarking for Video-On-Demand scenario

We are going to discuss a few watermark-embedding methods in compression domain.

Differential Energy Watermark

This method is employed for Intra coded frames. This is based on selectively discarding the high frequency DCT components from the data stream. [4] The method can be directly applied in compression domain after identifying Intra frames from the stream and then decoding the DCT coefficients. The following figure explains the method of embedding the watermark.

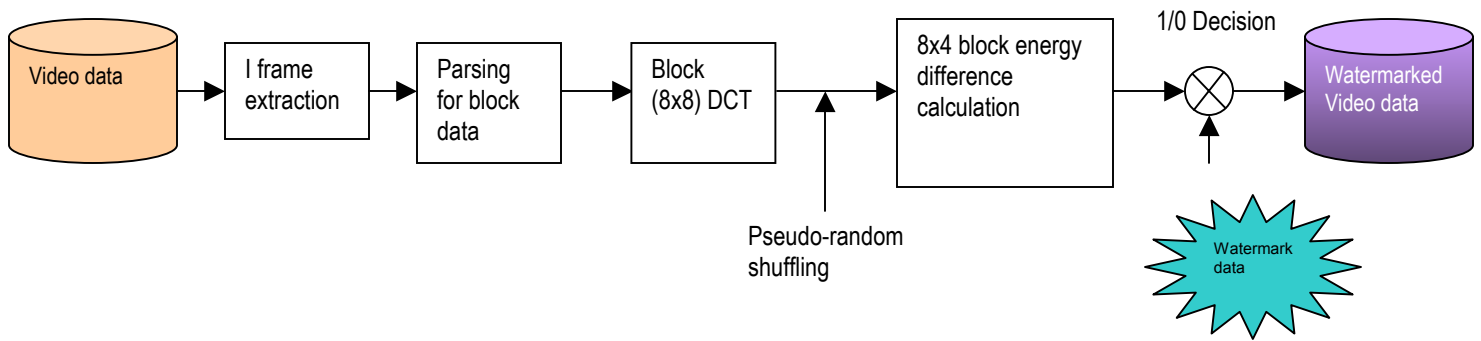


Figure 4: Differential energy watermark embedding

Bits for watermark data is embedded into each one of those blocks by introducing energy difference between top half and bottom half DCT coefficients of blocks. The value of the embedded bit is encoded as the sign off energy difference between two halves of the blocks. In the detector side the energy difference is calculated and embedded bit is determined according to the sign off difference.

Spread Spectrum technique

Spread spectrum technique, as described in [1], is a simple but very effective method for embedding digital watermark for compressed domain video. This method assumes incoming bit-stream in H.261/H.263 or MPEG format. In this method, video bit-stream is first parsed syntactically and data related to header information, motion, texture are separated out in separate buffers. Header information and motion data are kept unchanged and simply added to the output bit-stream without any alteration. DCT data is computed by performing Huffman decoding and inverse quantisation. Watermark data, which is to be embedded into the stream, is first suitably converted (encryption may be used) so that it is amenable for addition to the DCT data. Watermark data is then added to the obtained DCT coefficients carefully so that it does not result in increased bit-rate. Usually 10 to 20% of DCT coefficients are altered in this manner. Altered DCT coefficients are then re-quantized and Huffman coded and then added to the bit-streams. The diagram below shows the technique.

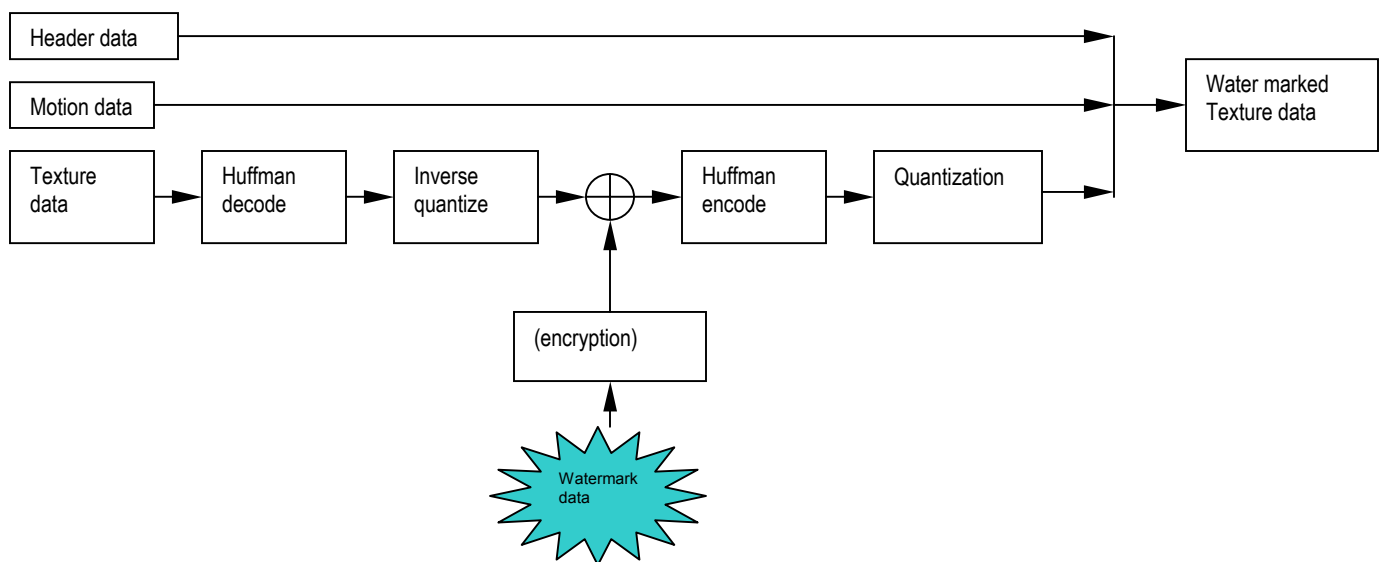


Figure 5: Watermarking method for compressed domain video

This method of Watermarking by spreading watermark information into DCT bits may result in degradation in the video signal over a period of time. To avoid this problem, a method known as "Drift Compensation" is applied. In this method, after a certain interval, the difference between watermark and un-watermarked signal is calculated and a drift compensation signal is generated. Propagation error that occurs due to Watermarking is subtracted from the drift compensation signal. This generic method can be modified by adding advanced tools like gain control, bit-rate controller, synchronization template for low-bit rate video.[2]

JAWS

Just Another Watermarking System or **JAWS** is designed by Philips Research and targeted for embedding watermark for broadcast system. This offers good real time performance and used for DVD applications [4]. In this method, a normally distributed reference pattern is generated with a secret key, which is then used to generate a reference watermark pattern as per following equation.

$$W_r = P_r - \text{shift}(P_r, \text{message})$$

Where W_r = generated watermark pattern

P_r = Normally distributed reference pattern

Message = Message to be embedded

This watermark is then perceptually shaped for each frame so that the watermark remains perceptually invisible. Perceptual shaping is done by taking activity measure of the frame (complex texture has high activity, flat area has low activity) and used for embedding information. An authorized detector can find out the watermark by computing FFT and IFFT to obtain peaks of the normally distributed reference pattern and watermark pattern. Peaks orientations provide sign information of the embedded bits.

Conclusion

Digital Watermarking is emerging as a favorite technique over traditional encryption for digital rights management (DRM). A lot of research is still going on and new methods are emerging. Current methods for video Watermarking are extension from image Watermarking and there is scope of more innovations. As more and more low-bit rate compression standards for video are emerging, and with the progress of wireless technology, a lot of challenges are now thrown to video Watermarking and simple extension of image Watermarking method would not be withstanding. A working group under MPEG committee is aggressively working on video Watermarking, and is investigating the possibility of motion information for watermark embedding. This technology has a great future in store and is going to significantly change the way digital media is managed.

References

- [1] Frank Hartung and Bernd Girod; University of Erlangen-Nuremberg (*Watermarking of compressed and uncompressed video*)
- [2] Adnan M. Alattar, Member IEEE (*Digital Watermarking of low bit-rate MPEG4 compressed video*)
- [3] Jonathan K. Su, Frank Hartung, Bernd Girod; University of Erlangen-Nuremberg (*Digital Watermarking of Text, Image and Video documents*)
- [4] Gwenaël Doërr and Jean-Luc Dugelay; Multimedia communication and image group (*Video Watermarking – overview and challenges*)