Video Watermarking Scheme Based on MPEG-2 for Copyright Protection

Ming Jiang\textsuperscript{a,b},*, Zhao-feng Ma\textsuperscript{a,b}, Xin-xin Niu\textsuperscript{a}, Yi-xian Yang\textsuperscript{a}

\textsuperscript{a} Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
\textsuperscript{b} Beijing National Security Science and Technology Co., Ltd., Beijing, 100086, China

Abstract

An innovative practical video watermarking scheme based on MPEG-2 is proposed in this paper. By operating the compressed video data-stream directly, we embed watermarking information in DC coefficients of block image which is in the IDR picture, in DPCM process of MPEG-2 coder. Watermark can be extracted blindly without original images and complete decoding is unnecessary. The algorithm designs one kind of synchronization code in order to resolve the synchronization problem. Watermark information is embedded periodically for random testing. The experimental results show the proposed scheme can achieve good excellent robustness to common video processing methods such as low bit rate MPEG-2 compression and synchronization attacks.

Key words: MPEG-2 compression; video watermarking; DPCM; synchronization

1. Introduction

Television broadcast is an important way to spread news and entertainments information. The main digital television technology is still based on MPEG-2 video compression and transmission technology. MPEG-2 standard is also being used in Digital Audio Video Interactive (DAVI) and DVD technology. Along with the popularization of Internet and the progress of computer technology, the restoration, distribution, and copy of multimedia audio/video products become much easier. At the same time, the copyright protection problems for digital works grow much more important.

Video watermarking [1-3] is an effective digital copyrights management technology for video. According to different stages of watermark embedding process, video watermarking can be classified into three kinds: embedding watermark in original video datas or uncompressed video sequence, in video encoding process and in video streaming.

The watermark is embedded in the video bit stream domain directly [4], which can achieve good real-time performance, but the complexity of which is very high. In [5], methods for embedding additive

* * Corresponding author. Tel.: +86 15210896946 E-mail address: jiangandming@yahoo.com.cn.

© 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license. Selection and/or peer-review under responsibility of Conference ESIAT2011 Organization Committee.

Key words: MPEG-2 compression; video watermarking; DPCM; synchronization
digital watermarks into uncompressed and compressed video were presented. The basic principle of the paper borrows from spread spectrum communications. The disadvantage is that embedding capacity is very limited and the robustness of this method is low against frame averaging and deleting attack processing. In [6], the differential energy watermarking (DEW) algorithm for MPEG streams was proposed. The DEW algorithm embeds label bits by selectively discarding high frequency DCT coefficients in certain regions. The advantage is that complete decoding is unnecessary and high watermark capacity, while the algorithm is not very robust against video transcoding process and structured handling. In order to improve the DEW algorithm, Sun[7] et al. presented a novel differential energy video watermarking based on Watson visual model and achieves good performance.

In this paper we propose a video watermarking scheme based on MPEG-2 for copyright protection. The algorithm operates the watermark embedding directly on DPCM(Differential Pulse Code Modulation) process of DCT DC coefficients in the encoding process. In watermark extraction, only entropy decoding is needed. This scheme is good for resisting temporal synchronization attacks[8] and is easily to use in the broadcast monitoring scene.

2. Watermarking scheme based on MPEG-2

2.1 MPEG-2 video compression

MPEG-2 standard supports four source formats, including lower resolution video(VCR) to high definition television(HDTV), and uses hierarchical codes including video sequence, group of pictures, pictures, slice, macroblock and block.

In the picture layer, three kinds of frame types are used, namely I-frame, P-frame and B-frame. In MPEG-2 coding, the organization of frames with different types is very flexible. The typical order of picture group is displayed: IBBPBBPBBPBB. The first frame of any picture group is I-frame, namely IDR frame, which is a random access point of video signals. In order to guarantee the random access of video signals, about 0.5 second will appear one IDR fame, which means there are about two groups of picture(GOP) in one second video.

In the MPEG-2 coding process, video images frame is processed in units of a macroblock (corresponding to 16x16 pixels in the original image). Each macroblock is encoded in intra or inter mode. Some key technologies are used in the coding process, like DCT, quantization, entropy coding, motion compensation and so on. In the decoding process, the decoder receives a compressed bit stream. The data elements are entropy decoded and reordered to produce a set of quantized coefficients. These are rescaled and inverse transformed to get video pictures decoded.

A practical video watermarking scheme should guarantee that this scheme can resist video transcoding and AD conversion processing. Meanwhile, the scheme should has satisfactory ability in resisting the temporal synchronization attacks of frame deleting and frame inserting. So in this paper, we operates the watermark embedding directly on DPCM(Differential Pulse Code Modulation) process of DCT DC coefficients in the encoding process. In watermark extraction, only entropy decoding is needed.

2.2 MPEG-2 video watermarking algorithm

2.2.1 Watermark preprocessing

We select the $M \times N$ binary image as watermark $W$. $W = \{W(i, j) | 0 \leq i < M, 0 \leq j < N\}$, and $W(i, j) \in \{0, 1\}$. For security, we scramble the watermark and then scan the image into one dimensional signal, namely $W = \{w_i\}, i = 1, 2, \ldots, C; C = M \times N, w_i = 0 \ or \ 1$. 

2.2.2 Video watermark embedding and extraction

In view of P-frame and B-frame are inter prediction coding types with high compression ratio and less code data, we select the luminance of IDR frame to embed watermarks. In MPEG-2, the I-frame picture with one luminance and two chroma signals is divided into 16×16 macroblocks. MPEG divides the luminance of each macroblocks into 8×8 blocks.

For the adjacent pixels sequence of natural video images has the correlation, the changes of DC coefficients in neighbor region is a even and random process. MPEG-2 encodes DC coefficients in using difference pulse code modulation (DPCM) forecast coding.

1) watermarking embedding algorithm

If the first \( w_0 \) is 1, change the first DPCM coefficient to the nearest odd, otherwise change to even. The other watermarks embedding rule is: if \( w_i \) is the same with the \( w_{i+1} \), change corresponding difference value into one even, otherwise one odd, with the basic principle that the absolute of the difference changed is to not to be bigger. The flow is shown in Fig. 1.

![Watermark embedding algorithm flow](image)

For example, DC coefficients are 83, 85, 84, 86. The DPCM results are 83, +2, -1, +2. The watermark is 1001. The DC coefficients embedded are 83, 84, 84, 87 in the method of [9]. In the method of this paper, the results are 83, 84, 84, 85. The results makes clear that the correlation of DC coefficients is better in the neighboring region.

2) watermarking extracting algorithm

In the MPEG-2 decoding, decode the DPCM data to DC coefficients. If the DC coefficient is odd, the watermark information is 1, otherwise the watermark information is 0. After extracting the information, anti-scramble the information to get the watermark extracted.

2.2.3 Analysis of video watermark synchronicity[10]

For a practical video watermark system, watermark should be extracted in any duration of the time period. In order to realize the random detecting of video watermarks, we embed the watermark periodically. Short period means it is to the benefit of the random detecting but influencing the video quality, while long period signifies it is not to the benefit of the random detecting but reducing the influence of video stream. Generally speaking, the duration of a meaningful video clip is about up to 8
seconds, which contains about 16 IDR frames. In this scheme, we embed the watermark every 8 seconds. We select the 4-bit code $C = [c_0, c_1, c_2, c_3]$, $c_i = 0$ or $1$, $i = 0, 1, 2, 3$, as a synchronicity code, which remarks the number from 0 to 15 corresponding to the synchronicity order number of the IDR frame marked. The synchronicity code is embedded repeatedly before embedding every watermark.

2.2.4 Watermark detecting

We select the $NC$ coefficient as a similarity method to evaluate the watermark method proposed. The $NC$ formula is as follow:

$$NC = \frac{\sum_i \sum_j w(i, j)' \cdot w(i, j)}{\sum_i \sum_j w(i, j)'}$$

where $w(i, j)'$ is the watermark extracted while $w(i, j)$ is the original watermark information. If $NC > \tau$, we judge that the watermark is existed in the JPEG image, otherwise not. The value of $\tau$ determines the false alarm rate and missing alarm rate. Here, $\tau$ is 0.5.

3. Experimental results

3.1 MPEG-2 video watermarking algorithm

Static video sequence News and Dynamic video sequence Foreman in 352×288 and YUV420 format are used in the test of watermarking embedding. According the requirement of experiments, the bit rate of MPEG-2 compression is 320kbits/s, and the frame rate is 25fps. The length of video sequence is 300 frames. The group is displayed: IBBPBBPB, the length of which is 12. Period of watermarking embedding is 8 seconds. Binary sequence in 198×128 format is selected as watermark. 4-bit code $C = [c_0, c_1, c_2, c_3]$, $c_i = 0$ or $1$, $i = 0, 1, 2, 3$ is chosen as a synchronicity code. The average PSNR of the picture marked in two sequence is 48.3917dB and 44.5043dB.

![Original video](a) original video ![Video after watermarking](b) video after watermarking

![Original watermark](c) original watermark ![Watermark extracted](d) watermark extracted

Fig. 2. Video watermarking testing results

![Relation between PSNR and compression bit rate](e) Relation between PSNR and compression bit rate

In Fig. 3., the impact on PSNR in different compression bit rate is shown.
### 3.2 Watermarking attack testing

In order to verify the robustness of the proposed method, different kinds of attacks are tested, such as chaos, filter, scale, frame crop, frame average and so on. Test results are as follow:

Static video sequence *News* and Dynamic video sequence *Foreman* in 352×288 and YUV420 format are used in the test of watermarking embedding. According the requirement of experiments, the bit rate of MPEG-2 compression is 320kbits/s, and the frame rate is 25fps. The length of video sequence is 300 frames. The group is displayed: IBBPBBPBBPBB, the length of which is 12. Period of watermarking embedding is 8 seconds. Binary sequence in 176×144 format is selected as watermark. 4_bit code $C_i = [c_0, c_1, c_2, c_3]$, $c_i = 0$ or 1, $i = 0, 1, 2, 3$ is chosen as a synchronicity code. The average PSNR of the picture marked in two sequence is 48.3917dB and 44.5043dB. Testing results are shown in Fig. 4. and Table 1.

![Testing results](image)

**Fig. 4.** Testing results

**Table 1.** NC and BER of testing results

<table>
<thead>
<tr>
<th>attack</th>
<th>News</th>
<th>Foreman</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NC</td>
<td>BER</td>
</tr>
<tr>
<td>0.01 pepper and salt</td>
<td>97.23%</td>
<td>4.76%</td>
</tr>
<tr>
<td>Median filter [3x3]</td>
<td>87.70%</td>
<td>20.17%</td>
</tr>
<tr>
<td>Gaussian low pass [5x5]</td>
<td>81.95%</td>
<td>28.78%</td>
</tr>
<tr>
<td>scale in 2 times</td>
<td>92.99%</td>
<td>11.79%</td>
</tr>
<tr>
<td>scale out 2 times</td>
<td>84.20%</td>
<td>25.47%</td>
</tr>
<tr>
<td>MPEG2(200Kbits/s)</td>
<td>99.97%</td>
<td>0.05%</td>
</tr>
<tr>
<td>MPEG2(120Kbits/s)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Frame crop(30%)</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Frame crop(40%)</td>
<td>98.16%</td>
<td>3.16%</td>
</tr>
<tr>
<td>Frame average</td>
<td>93.21%</td>
<td>11.43%</td>
</tr>
</tbody>
</table>

According to the experiment results, we obtain the conclusion as follow:

(1) In static and dynamic video sequence, the former is much superior to as a carrier to hidden the watermarks in resisting against spatiotemporal de-synchronization attacks.

(2) In this scheme, we embed the watermark on the DC coefficient of block images, so the algorithm has a certain robustness and the embedding of watermark does not affect the bit rate of video stream.

(3) For resisting the video watermark synchronous attack, we select the 4_bit synchronicity code to ensure the synchronism of watermark, the repetition of synchronicity code embedding enhance the robustness.

### 4. Summaries

In this paper, an innovative practical watermarking scheme for the copyright protection of MPEG-2 video is proposed. In this scheme, we embed the watermark in the DPCM encoding process and get excellent performance. In general we have the following contributions:
(1) In the method, we scramble the watermark improve the imperceptible and security of watermark.
(2) We embed the watermark in the DPCM encoding process and get excellent performance. Watermark can be extracted blindly without original images and complete decoding is unnecessary.
(3) One 4_bit code is selected as a synchronicity code, which remarks the number from 0 to 15 corresponding to the synchronicity order number of the IDR frame marked. The repeatly embedding ensure the robustness of synchronicity code.
(4) The watermark is embedded periodcally to ensure the random detecting of video watermarks.
The scheme is convenient, feasible and practical for providing copyright protection. Experimental results show that the proposed scheme can achieve excellent robustness to common video processing methods and some common attacks.

Acknowledgements

This work has been Supported by the National Basic Research Program of China (No: 2007CB311203), the National Natural Science Foundation of China under Grant No. 60803157, 60821001, the Standardization Public Industry Special Foundation of China under Grant No. 10-126, and the National Standard development planning under Grant No.20080200-T-339.

References