Copyright Protection on the Web: A Hybrid Digital Video Watermarking Scheme

Pat P. W. Chan
Computer Science and
Engineering Department
The Chinese University of
Hong Kong

pwchan@cse.cuhk.edu.hk

Michael R. Lyu
Computer Science and
Engineering Department
The Chinese University of
Hong Kong

lyu@cse.cuhk.edu.hk

Roland T. Chin
Computer Science
Department
Hong Kong University of
Science and Technology

roland@cs.ust.hk

ABSTRACT

Video is one of the most popular data shared in the Web, and the protection of video copyright is of vast interest. In this paper, we present a comprehensive approach for protecting and managing video copyrights in the Internet with watermarking techniques. We propose a novel hybrid digital video watermarking scheme with scrambled watermarks and error correction codes. The effectiveness of this scheme is verified through a series of experiments, and the robustness of our approach is demonstrated using the criteria of the latest StirMark test.

Categories and Subject Descriptors

K.6.5 [**Computing Milieux**]: Security and Protection

General Terms

Security, Experimentation

Keywords

Digital watermarking, scene change, video, hybrid

1. INTRODUCTION

We have seen an explosive growth of the Internet and the extensive use of digital media. Consequently, digital data owners can quickly and massively exchange multimedia documents across the Internet and Peer-to-Peer networks. This leads to a wide concern in multimedia security and multimedia copyright protections [1]. In the World Wide Web, it is difficult to manage the copyright exclusively, thus a comprehensive and efficient approach is necessary for protecting the ownership. As a method of intellectual property protection, digital watermarks have recently stimulated significant interest and become a very active area of research. Video watermarking introduces a number of issues not present in image watermarking. Due to the large amount of data and inherent redundancies between frames, video signals are highly susceptible to piracy attacks, including frame averaging, frame dropping, frame swapping, statistical analysis, etc [2]. The currently proposed algorithms, on the other hand, do not solve these problems effectively. In the Web, the chance of a watermark being attacked is increased daily, hence, protecting the watermark and the copyright of multimedia contents posts formidable challenges to the Web community.

In this paper, we focus on engaging the digital watermarking techniques to protect digital multimedia intellectual copyright in the Web, and propose a new algorithm for video watermarking.

2. WATERMARKING SCHEME

We perform a complete survey on the current watermarking technologies and propose a hybrid watermarking scheme based on scene change analysis and error correction code [3]. Our video watermarking algorithm is robust against the attacks of frame dropping, averaging and statistical analysis, which were not solved effectively in the past. In our scheme, we apply scene change detections and scrambled watermarks in a video. The watermark is resized and scrambled into different parts. The same part of the watermark is embedded [4] into the frames of a scene; thus, the scheme is robust against frame dropping. For different scenes, different parts of the watermark are used, making the scheme robust against frame averaging and statistical analysis [3].

With a complete survey of the current watermarking technologies, it is noticed that none of the existing schemes is capable of resisting all attacks. Accordingly, we analyze the strengths of different watermarking schemes and apply a hybrid approach to form a super watermarking scheme that can resist most of the attacks. We propose several hybrid approaches. The first one is a visual-audio hybrid watermarking scheme. As videos consist of both video and audio channels, the robustness of our scheme can be enhanced by including an audio watermark. Consequently, we embed error correcting codes of a video watermark as a watermark embedding in audio channel and refine the retrieved watermark during the watermark detection. The second approach is anther hybrid with different watermarking schemes with two alternatives: independent watermarking schemes which embeds the watermarks into the frames with different watermarking schemes in different scenes, or dependent watermarking schemes which embeds the watermarks serially in a frame with different watermarking schemes. The overview of the proposed watermarking scheme is shown in Figure 1.

3. EXPERIMENTAL RESULTS

Distinguishable attacks are carried out to the watermarked videos to evaluate the performance and robustness of our scheme. These attacks, potentially launched in the Web, include frame dropping, frame averaging, statistical analysis, and StirMark 4.0 [5]. Another DWT-based watermarking scheme, which embeds an identical watermark in all frames, is implemented to compare with the proposed scheme. A video clip with 1526 frames of size 352×288 is used in our experiment. The video consists of 10 scene changes.
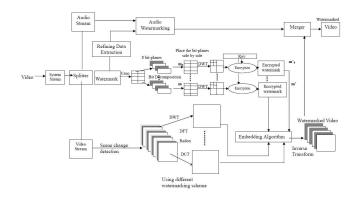
Figure 1: Overview of hybrid watermarking scheme

3.1 Frame dropping, averaging and statistical analysis

As a video contains a large amount of redundancies between frames, it may suffer attacks by frame dropping. The first experiment is aimed at examining the robustness of the scheme under the attack by frame dropping. Different percentages of frames are dropped and the obtained results are shown in Figure 2(a). The performance of the scheme is significantly improved by combining with an audio watermark, the visual-audio watermarking scheme, especially when the dropping rate of video frame is high. Due to the increased dropping rate, errors of the extracted watermark are increased, which significantly damages the watermark. The error correcting codes from the audio watermark provides information to correct the error and overcomes the corruption of the video watermark.
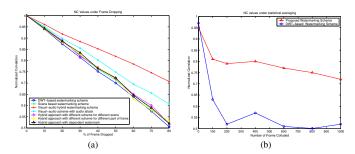

Figure 2: (a) NC values under frame dropping (b) NC values under statistical averaging

Further Experiments have been conducted to evaluate the proposed scheme under statistical analysis. After this attack is applied to the watermarked video with different numbers of video frame colluded, the results are obtained, as shown in Figure 2(b). It is found that the proposed scheme can resist statistical averaging quite well. Our scheme performs better because it crops a watermark into pieces and embeds them into different frames, making the watermark resistant to attacks by frame averaging for the watermark extraction. The identical watermark used within a scene can prevent attackers from taking the advantage of motionless regions in successive frames and removing the watermark by comparing and averaging the adjacent frames statistically. Different watermarks used for successive, yet different scenes can prevent attackers from colluding with frames from completely different scenes to extract the watermark.

Table 1: Comparison among different watermarking schemes

Attack Class	a	b	c	d	e	f
Lossy Compression	0.61	0.62	0.82	0.69	0.71	0.68
PSNR	0.72	0.76	0.86	0.80	0.82	0.81
Add Noise	0.63	0.60	0.76	0.67	0.70	0.64
Median Filter	0.54	0.54	0.74	0.60	0.55	0.52
Row / Column Removal	0.69	0.71	0.85	0.75	0.77	0.74
Cropping	0.68	0.66	0.78	0.70	0.72	0.69
Rescale	0.63	0.62	0.75	0.69	0.71	0.63
Rotation	0.60	0.61	0.73	0.67	0.69	0.64
Affine	0.55	0.55	0.78	0.70	0.73	0.63
Overall	0.62	0.63	0.78	0.69	0.71	0.66

3.2 Robustness Test with StirMark 4.0

StirMark 4.0 is a benchmark for testing robustness of a watermarking scheme. In this experiment, we use StirMark 4.0 to test the robustness of the proposed scheme when image processing is applied, and compare it with the current techniques that exist in the literature. Table 1 shows the result of the watermarked video under different attacks from StirMark with different watermarking schemes: (a) DWT-based scheme, (b) scene-based scheme, (c) visual-audio hybrid approach, (d) visual-audio hybrid approach with audio attack, (e) independent hybrid approach, and (f) dependent hybrid approach. The result shows that both visual-audio and independent hybrid approach improve the performance of the scheme. When there is an attack conducted on the video watermarked with the hybrid approach, different watermarking schemes employed in the hybrid approach are resistant against different attacks. Consequently, some parts of the watermark still survive after the attack. This approach enhances the chance of survival under several attacks.

4. CONCLUSIONS

This paper proposes an scene-based hybrid video watermarking scheme for protecting the video copyright in the Web. Our approach cultivates an innovative idea in embedding different parts of a watermark according to scene changes, in enclosing its error correcting codes as an audio watermark, and in applying a hybrid approach to the proposed scheme. This approach is never explored in the literature, and its advantages are clear and significant. Our scheme is verified to be resistant against the attacks targeted on the video characteristics and the attacks by image processing.

5. ACKNOWLEDGMENTS

6. REFERENCES

[1] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," *IEEE Transactions on Internet Computing*, Vol. 6, Issue. 3, pp. 18-26, May 2002.

[2] J. Lee and S. Jung, "A survey of watermarking techniques applied to multimedia," *Proceedings 2001 IEEE International Symposium on Industrial Electronics (ISIE2001)*, Vol. 1, pp. 272-277, 2001.

[3] P.W. Chan and M. R. Lyu, "A DWT-based Digital Video Watermarking Scheme with Error Correcting Code," *Proceedings Fifth International Conference on Information and Communications Security (ICICS2003)*, pp. 202-213, 10-13 Oct 2003.

[4] F.Y. Duan, I. King, L. Xu, and L.W. Chan, "Intra-block algorithm for digital watermarking", *Proceedings IEEE 14th International Conference on Pattern Recognition (ICPR'98)*, Vol. 2, pp. 1589-1591, 17-20 Aug 1998.

[5] http://www.petitcolas.net/fabien/watermarking/stirmark/