

A Comparative Analysis of Watermarking Techniques for Copy Protection of Digital Images

Dolley Shukla¹ and Manisha Sharma²

¹ ShriShankaracharya College of Engineering & Technology, Bhilai
dolleyshukla@yahoo.co.in

² Bhilai Institute of Technology, Durg
manishasharma1@rediffmail.com

Abstract. Digital watermarking is the process of embedding information into a digital signal, i.e. audio, pictures, video, etc. Embedded marks in the message are generally imperceptible but can be detected or extracted. By imperceptibly hiding information into the video content it is possible to provide copy protection. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. If the signal is copied, then the embedded information is also in the copy. So, Watermarking is an emerging technology that is claimed to have an important application in copy protection. A variety of watermarking techniques have been proposed by researchers for the copy-protection. This paper presents an extensive review of the prevailing literature in watermarking for copy protection.

Keywords: Broadcast monitoring, Copy protection, Digital image watermarking, Video.

1 Introduction

As the digital broadcasting is developing enormous digital multimedia contents are available easily. Digital media have an advantage that can be copied without loss in quality but it is also a disadvantage in the viewpoint of copyright management. Conventional cryptographic schemes permit only valid key holders to access the encrypted data, but once when such data is decrypted there is no way to trick its reproduction & redistribution. Therefore, conventional cryptographic schemes provide little protection against copy protection. A digital watermark is intended to complement cryptographic schemes for copy protection. There are several techniques presented for copy protection and copy right protection by the researchers[1– 3]. This paper concentrates on copy protection techniques.

The procedure of embedding watermark into a multimedia element like image, audio or video is referred to as watermarking [4]. It is possible to extract this embedded data at a later stage, or detected in the multimedia element for diverse purposes including copy protection, access control, and broadcast monitoring.

2 Watermark System Design Issues

An array of challenges related to the watermarking technology have arisen. There are a number of other issues, some technical and some non-technical, which have also come to play an important role. An image watermarking procedure needs to satisfy the following requirements [5].

- **Transparency**

The watermarked image should be indistinguishable from the original image even on the highest quality equipment.

- **Robustness**

The ideal watermark must be highly Robust & needs to be flexible to a range of possible attacks by pirates. These attacks may be robustness against compression such as JPEG, scaling and aspect ratio changes, rotation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks [6]. The watermark must survive the geometric distortions as well as more arbitrary scaling and cropping which a pirate may use to avoid watermark detection.

- **Economic Costs**

Adding a watermark detector require some degree of redesign. In order to minimize that cost, detector must be implemented in about 30 000 gates. 90 000 gates are often mentioned as a target for the complexity of the watermark detector.

- **False Positives Rate**

A true false positive occurs when a watermark is detected when no watermark has been embedded. An invalid positive occurs in case a watermark has been embedded but the wrong payload is retrieved. An invalid positive occurs in case a watermark has been embedded but the wrong payload is retrieved. False positive probability is 4.7×10^{-23} and is more than sufficient for all practical purposes.

3 Problem Statement

New platform that embeds hard disk drive in the DBR(Digital Broadcast Receiver) system is developed recently [7]. This system can cause a copyright infringement problem if there is no copy protection scheme. Once a scrambled program is descrambled, this stream can be copied several times after saving in the hard disk drive. So there is a need to add copy protection information to the stream. This information must be strongly embedded to the contents. It can only be removed when the contents suffers severe degradation. This is a reason why watermarking method should be used. For copy protection, watermark information must be embedded in the content and detected whether this content is copyrighted or not. Watermarked video data has two kinds of copy control information i.e., 'Copy never', or 'Copy freely'.

When the use users try to copy a stream to another media, after checking this copy control information, the copy process is done when the bit is ‘Copy freely’. In the case of ‘Copy never’, the content cannot be copied anymore.

4 Requirements of Copy Protection System

The main requirements of copy protection system are as follows:

- The copy-protection system may be implemented in four states: Copy-Free (CF), Copy-Never (CN), Copy-Once (CO), Copy-No-More (CM).
- Compliant devices (i.e. devices which obey the Content Scrambling System (CSS) rules) do not allow copying of Copy-Never (CN) and Copy-No-More (CM) content.
- A compliant device should allow copying Copy-Once (CO) content. A legal copy of Copy-Once(CO) content should have a Copy-No-More(CN) state.
- A compliant device should not play Copy-Never (CN) content off recordable media.
- The copy protection system should not affect the image quality.
- The copy protection system should not interfere with the content creation process.
- Detection of copy-protection state should be fast.
- The average consumer should not be able to circumvent the copy protection system.
- The false-positive rate should be extremely low.
- The copy protection system should be inexpensive to implement.

5 Comparative Analysis of Recent Researches

Watermarking digital media has received a great interest in the research community. In this section we have presented a comparative analysis of literatures provided by researchers in watermarking for copy protection. Most copy watermarking schemes focus on image and video watermarking.

A digital watermark is an imperceptible signal added to cover image, which can possibly be identified at a later stage for copy protection identification, ownership proof, and the like. Contemporary digital watermarking schemes mainly target image and video copy protection. The watermark comprises of information regarding the rules of usage and copying which the content owner desires to enforce. These will commonly be undemanding rules like “this content may not be copied”, or “this content may be copied, but no subsequent copies may be made of that copy”.

For copy protection several methods are proposed.

Cox et al [8] described the copy-protection system currently under consideration for DVD. This system broadly tries to prevent illicit copies from being made from either the analog or digital I/O channels of DVD recorders. An analog copy-protection

system is utilized to protect the NTSC/PAL output channel by preventing copies to Video Hollywood studio (VHS). The digital transmission of content is protected by a robust encryption protocol between two communicating devices. Watermarking is used to encode copy control information retrievable from both digital and analog signals. Hence, such embedded signals avoid the need for metadata to be carried in either the digital or analog domains.

F. G. Depovere, [9] discussed the various issues that play a role in designing a copy-protection system for digital versatile disk (DVD) video as perceived by Millennium, one of the two contenders in the DVD-video copy-protection standardization activity. It has presented the Millennium watermark system, the systems proposed for DVD video copy protection by Philips, Macro-vision and Digimarc. They also address some specific system aspects, such as watermark detector location and copy generation control. The DVD copy protection problem cannot be solved by encryption alone. Digital watermarking is needed to prevent copy-protection being circumvented by noncompliant devices. It describes the Millennium watermark system as proposed for DVD copy protection purposes, and it illustrates how the basic requirements for that application are met.

Ton Kalker [10] discussed that watermarking is an important enabling technology for copy protection or broadcast monitoring of video. A watermarking scheme that meets the requirements for these applications has been introduced. It discusses about the main requirement for watermarking solution for DVD copy protection.

Yeong Kyeong Seong et al [11] suggested a hard disk drive embedded digital satellite receiver with a scene change detector for video indexing. This paper discusses the implementation of a scene change detection algorithm in the compressed domain for low computing power systems. This receiver can store, retrieve and manage the broadcast data by implementing an interface between the conventional digital satellite receiver and digital storage media. In addition this receiver gives users an ability to search the scene change position by implementing a scene change detection algorithm. The detected temporal video segments are stored in the HDD and retrieved when users want. User can obtain more information for efficient video retrieval, using this proposed system.

Yeong et al [12] proposed another watermarking method based on scene segmentation for copy protection in the hard disk drive embedded digital broadcast receivers. In this, initially video sequence is segmented as scenes using the macroblock types of B-picture in the MPEG compressed domain. Second, for each scene, different embedding parameter is determined from the image complexity and motion vector amplitude. For copy protection, copy control watermark information is embedded in the DCT Domain content whether the content is copyrighted or not.

G. Boato et al [13] shows a major limitation of some recently proposed asymmetric watermarking techniques based on linear algebra lies in the strong dependence of the watermark on the original image.

Table 1. Comparative Analysis

S. No.	Author	Application Area	Remarks	Year
1.	L.J.Cox [8]	DVD	1.Improve the protection provided by encryption protocol. 2.Reduce the value of illegal unencrypted copies when they are made by making them unplayable on compliant devices. 3.This paper gives the main requirement for a watermarking solution for DVD copy protection	1999
2.	Ton Kalker [9]	Video or Broadcast Data	1.Differentiate of still Image and Video Watermarking 2. In video,due to the sheer volume of data & interlacing structure, the Quality of the content will reduce & the attack will not remove by consumer.	1999
3.	Ton kalker, Maurice Maes [10]	DVD	1.DVD copy protection problem can not be solved by encryption alone. 2.Correlation method for embedding & detection. 3.Watermark detector should be included in the playback drive. 4.System prevents the Local scrambling or bit inversion attack	2000
4.	Y. K. Seong, Y. H. Choi, J. A. Park, & T. S. Choi[11]	Broadcasting	1.Implemented a Scene change detection algorithm in compressed domain for low computing power system.	
5.	Yeong Seong, Yoon-Hee Choi, [12]	Digital Broadcast Receiver	1. Video is segmented into different scenes. 2. Encoded by using DCT. 3. Uses scene-change detection algorithm.	2004
6.	. Fontanari, F. G. B. De Natale, and G. Boato[13]	Video	1.Scheme is based on Linear Algebra, which is proven to be secure under protection attacks.	2006
7.	Alper Koz,Cigal [14]	Video or Broadcasting	1.Application is emerged as Free-view TV. 2.Image based rendering operation is performed. 3.Frame of multiple views are used. 4.Homography estimation method is proposed.	2010

6 Conclusion

Watermarking for copy protection is a new and emerging area of research. It mainly deals with adding hidden messages or copyright notices in digital video. This paper presents the comparative analysis of various copy protection schemes.

Even though copy protection has received ample attention in the standardization of digital video in the past five years, several issues have not yet been fully resolved. It may be unlikely that a bullet-proof solution will ever be found, but the discussions are converging on what technical mechanisms should be involved and against what these can protect.

References

1. Barni, M., Bartolini, F., Piva, A.: Managing copyright in open networks. *IEEE Transactions on Internet Computing* 6(3), 18–26 (2002)
2. Liao, M., Lu, C., Yuan, H.: Multipurpose watermarking for image authentication and Protection. *IEEE Transactions on Image Processing* 10(10), 1579–1592 (2001)

3. Akiyama, T., Motoyoshi, F., Nakanishi, S., Uchida, O.: Hybrid Digital Watermarking for Color Images Based on Wavelet Transform. In: International Conference on Applied Computing, pp. 150–154 (2006)
4. Ganic, A.E., Eskicioglu, A.M.: Robust DWTSVD domain image watermarking: embedding data in all frequencies. In: International Multimedia Conference, pp. 166–174 (2004)
5. Huang, J., Zeng, W., Kang, X.: Improving Robustness of Quantization- Based Image Watermarking via Adaptive Receiver. *IEEE Transactions on Multimedia* 10(6), 953–959 (2008)
6. Li, X., Xue, X.-Y., Li, W.: An Optimized Multi-bits Blind Watermarking Scheme. In: Qing, S., Gollmann, D., Zhou, J. (eds.) *ICICS 2003*. LNCS, vol. 2836, pp. 360–369. Springer, Heidelberg (2003)
7. Choi, T.S., Choi, Y.H., Seong, Y.K.: Design and implementation of hard disk drive embedded digital satellite receiver with file management. *IEEE Transactions on Consumer Electronics* 48(1), 125–130 (2002)
8. Boom, J.A., Cox, I.J., Kalker, T., Miller, M.L., Linnartz, J.-P.M.G., Traw, S., Brendan, C.: Copy protection for DVD video. In: *IEEE International Conference on Image Processing*, vol. 87(7), pp. 1267–1276 (1999)
9. Depovere, F.G., Haitzma, J., Kalker, T., Linnartz, J.-P.M.G., Maes, M., Talstra, J.: Digital watermarking for DVD video copy protection. *IEEE Signal Processing Magazine* 17(5), 47–57 (2000)
10. Kalker, T.: System issues in digital image and video watermarking for copy protection. In: *IEEE International Conference on Multimedia Computing and Systems*, vol. 1, pp. 562–567 (1999)
11. Choi, T.S., Choi, Y.H., Park, J.A., Seong, Y.K.: A hard disk drive embedded digital satellite receiver with scene change detector for video indexing. *IEEE Transactions on Consumer Electronics* 48(3), 776–782 (2002)
12. Choi, T.-S., Choi, Y.-H., Seong, Y.K.: Scene-Based Watermarking method for Copy-Protection using Image complexity and motion vector amplitude. In: *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 3, pp. 409–412 (2004)
13. Boato, G., Fontanari, C., De Natale, F.G.B.: An Improved Asymmetric Watermarking Scheme Suitable for Copy Protection. *IEEE Transactions on Signal Processing* 54(7), 2833–2834 (2006)
14. Aydın Alatan, A., Koz, A., Cigla, C.: Watermarking of Free-view Video. *IEEE Transactions on Image Processing* 19(7), 1779–1785 (2010)