WATERMARKING SCHEMES FOR COPY PROTECTION : A SURVEY

Dolley Shukla[1] and Manisha Sharma[2]

[1]Shri Shankaracharya College of Engineering & Technology, Bhilai, India
dolleyshukla@yahoo.co.in
[2]Bhilai Institute of Technology, Durg, India
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. 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. BY IMPERCEPTIBLY HIDING INFORMATION INTO THE VIDEO CONTENT IT WILL BE POSSIBLE TO PREVENT COPYING OR PLAYBACK OF SUCH CONTENT. 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. There are several researches of copy protection in DVD (Digital Versatile Disk) recorder [1-3]. Digital watermarking is a technique that proffers a means to guard digital images from illegal copying and manipulation. The procedure of embedding data 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 . An image watermarking procedure needs to satisfy the following requirements [5].

• **Transparency:** The embedded watermark pattern does not visually destroy the original image fidelity and needs to be perceptually invisible.
• **Robustness:** The watermark pattern is hard to detect and remove in an illegal way. In order for a watermark to be beneficial it 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].

DOI : 10.5121/ijcses.2012.3106

1.1 Transparency

The *PSNR* is used for evaluating the transparency of watermarking technique for copy protection . Moreover, the peak signal-to-noise ratio (*PSNR*) was used to evaluate the quality of the watermarked image. The
PSNR is defined as :

$$PSNR = 10 \ \ log_{10}\frac{255^2}{MSE}(dB)$$

where mean-square error (*MSE*) is defined as :

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(h_{i,j} - h'_{i,j}\right)^2$$

where $h_{i,j}, h_{i,j}$ are the gray levels of pixels in the host and watermarked images, respectively. The image quality is increased with increasing *PSNR*.

1.2 Robustness of watermark

The Robustness is the most highly desired feature of a watermarking algorithm especially if the application demands copy protection.
The information carried by the watermark can be accessed using a detection algorithm provided the secret key is known. An important property of a watermark is its robustness with respect to image distortions. This means that the watermark should be readable from images that underwent common image processing operations, such as filtering, lossy compression, noise adding, histogram manipulation, and various geometrical transformations.
With the large number of watermarking techniques recently developed for copy protection, one becomes naturally wondering if it is possible to compare the performance of different techniques in a fair manner.

Robustness of watermarking technique can be compared by following method

1.2.1. Robustness depends on the information capacity of the watermark, the watermark strength / visibility, and the detection statistics (threshold).
1.2.2. Robustness is also influenced by the choice of images (size, content, color depth).
1.2.3. In some cases it is possible to trade robustness for security.
1.2.4. Techniques robust to a wider spectrum of image deformations may not have the best robustness for specific image deformations.

The robustness is directly influenced by the watermark extraction statistics. Majority of watermarking schemes for copy protection are based on thresholding a correlation between an extracted vector and a pseudo-random sequence. With decreasing threshold the probability of missed detections also decreases and the robustness increases. But at the same time, the rate of false detections will also increase.
The robustness is usually tested using typical image processing operations that can be divided into two groups: gray scale manipulations (filtering, noise adding, lossy compression, gamma correction, color quantization, color truncation to a finite palette, etc.) and geometric transformations (scaling, cropping, rotation, affine transforms, general rubber sheet deformations of StirMark-type[5]).

The guidelines for comparing watermarking techniques for copy protection are as follows:

1. Adjust watermark strength so that Girod's model indicates less than α % of pixels with visible changes (α=1).
2. Modify the scheme so that a one-bit watermark and a 60-bit watermark can be embedded.

3. Set decision thresholds so that the probability of false detections is less than 10^{-6}.
4. For each test image, run robustness tests for the following operations:

Table 1 Robustness test

S.No.	Operation	Parameter
1.	JPEG compression	Quality factor
2.	Blurring	Number of operations / kernel size
3.	Noise adding	Noise Amplitude (SNR)
4.	Gamma correction	Gamma exponent
5.	Permutation of pixels	Kernel size
6.	Mosaic filter	Kernel size
7.	Median filtering	Kernel size
8.	Histogram equalization	N /A

2. 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 evere 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.

3. 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-N0-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.

4. 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 unnoticeable signal added to digital data, known as cover work, which can possibly be identified at a later stage for copy protection identification, ownership proof, and the like. Contemporary digital watermarking schemes chiefly 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 copyprotection 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 acopy-protection system for digital versatile disk (DVD) video as perceived by Millennium, one of the two contenders in the DVD-video copyprotection standardization activity. It has presented the Millennium watermark system, the systems proposed for DVD video copy protection by Philips, Macrovision 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 illustrate 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 [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. Boatoet 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.	I.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. Authentication & session– Key generation mechanism is needed for all interfaces. 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.	2002
5.	Yeong Kyeong 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.	Video	1. Scheme is based on Linear Algebra, which is proven to be secure under protection attacks.	2006

	De Natale , and G. Boato[13]			
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. Camera position & homography estimation methods are proposed.	2010

5. CONCLUSIONS

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.

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 reviews various copy protection literatures for digital image and video watermarking.

REFERENCES

[1] Barni, M., Bartolini, & F., Piva,A., (2002) " Managing copyright in open networks", IEEE *Transactions on Internet Computing,* Vol. 6, No. 3,pp. 18–26.

[2] Liao, M., Lu, C. & Yuan, H.,(2001) " Multipurpose watermarking for image authentication and Protection" , IEEE *Transactions on Image Processing*, Vol. 10, No.10, pp. 1579–1592 .

[3] Akiyama, Tosihiro., Motoyoshi, Fumiaki., Nakanishi, Shohachiro. & Uchida, Osamu..:(2006) " Hybrid Digital Watermarking for Color Images Based on Wavelet Transform", International Conference on Applied Computing, pp. 150-154. (2006)

[4] Ganic, Authors Emir., Eskicioglu & Ahmet M. (2004) "Robust DWTSVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, pp. 166 – 174.

[5] Choi**,** T. S., Choi, Y. H & Seong, Y. K, (2002) ".Design and implementation of hard disk drive embedded digital satellite receiver with file management", IEEE *Transactions on Consumer Electronics*, Vol.48, No.1, pp125-130

[6] Li ,Wei., Li, Xiaoqiang., & Xue, Xiangyang., (2003) "An Optimized Multi-bits Blind Watermarking Scheme", Lecture Notes in ComputerScience, Vol. 2836, pp.360-369 .

[7] Huang, Jiwu., Zeng, Wenjun.,& Kang, Xiangui., (2008) " Improving Robustness of Quantization- Based Image Watermarking via Adaptive Receiver" , IEEE *Transactions on Multimedia*, Vol.10, No. 6, pp. 953-959. (2008)

[8] Boom, J. A., Cox, I. J., Kalker,T., Miller, M. L., Linnartz, J. -P. M. G. , & Traw, C. B. S.,(1999) Copy protection for DVD video, IEEE International Conference on Image Processing, Vol. 87, No. 7, pp. 1267-1276.

[9] Depovere, F. G., Haitsma, J., Kalker,T., Linnartz, J. -P. M. G., Maes, M., & Talstra,J, (2000) "Digital watermarking for DVD video copy protection" , IEEE *Signal Processing Magazine*, Vol. 17, No. 5, pp. 47-57.

[10] Kalker, T. (1999) " System issues in digital image and video watermarking for copy protection" IEEE *International Conference on Multimedia Computing and Systems*, Vol.1, pp.562-567.

[11] Choi, T.S., Choi, Y.H., Park,J.A., & Seong,Y.K , (2002) " A hard disk drive embedded digital satellite receiver with scene change detector for video indexing ", IEEE *Transactions on Consumer Electronics*, Vol. 48, No. 3, pp. 776-782 .

[12] Choi , Tae-Sun., Choi ,Yoon-Hee . & Seong, Yeong Kyeong., (2004) "Scene-Based Watermarking method for Copy-Protection using Image complexity and motion vector

Amplitude “, IEEE *International Conference on Acoustics, Speech and Signal Processing*, Vol.3, pp. 409-12 .

[13] Boato, G., Fontanari,C. & De Natale, F.G.B., (2006) “ An Improved Asymmetric Watermarking Scheme Suitable for Copy Protection,”, IEEE *Transactions on Signal Processing*, Vol. 54, No. 7,pp. 2833-2834 .

[14] Aydın Alatan,A., Koz, Alper. & Cigla, Cevahir. , (2010) “ Watermarking of Free-view Video”, IEEE *Transactions on Image Processing*, Vol.19, No. 7, pp. 1785-1779 .

Authors

Dolley Shukla was born in chhattisgarh, India in 1975.She received the B.E. degree from Pt. Ravishankar University, M.Tech. degree from M.A.N.I.T., Bhopal in Electronics & Telecommunication engineering in 1999 and in 2006 respectively. She currently pursuing the Ph.D. degree at the CSVTU, Bhilai , India.
Dolley Shukla is currently Associate Professor at SSCET, Bhilai, India.
Her research interests include Image Processing, Video Processing & Watermarking.

Dr. Manisha Sharma was born in 1970. She received the B.E. from Barkhattullah University, Bhopal in 1992 , M.E. from Government Engineering College, Jabalpur Rani Durgavati University, Jabalpur in 1995 and Ph.D. from C.S.V.T.U., Bhilai, India in 2010. Presently she is working as a professor & Head of the departm Institute of Technology , Durg, CHHATTISGARH, India. Her research Interest includ Processing , Image Segmentation , Video Processing , watermarking and Authenticati