Digital Watermarking Technology with Practical Applications

Norishige Morimoto
IBM Japan, Ltd., Tokyo Research Laboratory
Noly@jp.ibm.com

Abstract

Digital watermarking technology has been actively studied and developed by a number of institutions and companies since mid '90s. This area draws more and more attention as one of the key technology elements for content management, copyright protection and copy control of digital contents. This article discusses several different types of digital watermark application, particularly the application of digital watermarks for DVD copy control. This would be the first digital watermark application requiring worldwide standardization.

Keywords: digital watermark, DataHiding*, copy control, DVD

(* DataHiding™ is a registered trade mark of IBM)

Introduction

Unlimited number of replicas of the original content can be made from unprotected digital content. This makes the content creators and content owners more anxious about the copyrights management of their digital contents. Concern for the protection of copyrighted digital intellectual properties, such as computer programs, have been high, since 1980s. Today, well-established cryptographic algorithms can resolve many of these issues. However, these solutions can only protect the digital contents if they never leave the digital domain, or remains in some well defined data formats. When multimedia content starts to be digitized, a new problem arises. Normally, the form of the data does not have significant impact on multimedia contents such as video or audio. The visible or audible information can be transferred into other formats or even passing through analog connections without significant change to the value of the contents. This situation calls for technological solutions to be used in addition to the cryptography technology.

Digital watermarking technology has been actively studied by several technical institutions since mid-1990s.[1,2,3] A few companies also started offering products and services for the purpose of copyrights protection and the tracking of unauthorized duplication of digital still images.[4, 5]. This group of technologies provides methods to "imprint" additional data or messages into multi-media contents such as still image, video and audio data. Generally, the imprinted data is invisible (or inaudible) to the ordinary users, and is difficult to be separated from the host media. The imprinted data can be extracted from the imprinted host media, as long as the degradation of the host media is within certain limitation.

This desirable characteristic makes digital watermark an ideal technology to carry the signature of its owner, identification code or copy control information that can travel with the content itself.

In Section 2, three practical applications of digital watermarking technologies are discussed. In Section 3, some details about the DVD copy control application for DVD are presented, including the standardization activity and the overview of a technology proposal to the DVD Copy Protection Technical Working Group (CPTWG).

Applications of Digital Watermarks

Digital watermarking technology for rights management

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from

the content owners to the receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user.

Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment.

The major technical requirements for this application are as follows;

- The watermark does not incur visible (or audible) artifacts to the ordinary users.
- The watermark is independent of the data format.
- The information carried by the watermark is robust to content manipulations, compression, and so on.
- The watermark can be detected without the unwatermarked original content.
- The watermark can be identified by some kind of "keys" that are used to identify large number of individual contents uniquely.

The contents may be changed to the other formats, edited or trimmed by the users or compressed for the storage and transmission, and it is desirable to be able to detect the watermark from those processed contents. Usually, the watermark signal embedded into the content does not disappear after the editing of the content, but becomes more and more difficult to detect while the content is distorted. In general, higher robustness can be achieved by increasing the strength of the watermark signal, thus improving the detection capability. In other words, the robustness of the watermark is a tradeoff between the amount of watermark signal that applies to the content and the overhead to the detection.

Currently, several commercial products and services using watermarking technology are available. They include applications for watermark embedding/detection and services to search the Internet for the contents with certain designated watermarks. These applications are mainly taking place between the large content owners (e.g. electronic publishers/distributors), and their customers (e.g. the content creators). Because the usage is limited within relatively smaller groups, each group tends to use their own proprietary watermark rather than a common one. Among these groups, the standardization is not an urgent issue until their markets shift to public domain consumers.

Digital watermarking technology for authentication and tamper proofing

Another application of digital watermark is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image.

Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/Printing/Exposing (DPE) compared to the traditional chemical photos. However, there are some critical issues for some particular applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos.

The way to realize this feature is to embed a layer of the authentication signature into the subject digital image using a digital watermark. This additional layer of watermark is used as a "sensor" to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. Through a joint study with a major Japanese insurance company, we confirmed the technical feasibility of the technology for the above-mentioned industrial applications.

The technical requirements for this application are as follows;

- Invisible to the ordinary users,
- Applicable to compressed image format (most digital cameras use JPEG compatible format), and
- Sensitive to content manipulations, compression, and so on.

Visible reversible watermarking for electronic distribution

Unlike other digital watermarking technologies described above, the visible reversible watermark is visible. It is available as a commercial product [8]. This unique form of watermarking technology by IBM allows the content owners to

embed a visible shape or logo mark such as company's logo on top of the image. The mark is removed (the watermark is reversed) only with the application of an appropriate "decryption" key and watermark remover software.

This mark is applied by modifying the Discrete Cosine Transformation (DCT) coefficients of the JPEG compressed image following certain pre-defined rule and visual effect analysis result to make it half transparent, but not totally destructive. The key, with the mark removal program, will be used to remove the mark from the image. The removal of the visible mark may be tied up with the embedding of another invisible mark for the tracking purpose.

With this visible watermark on the image, the content becomes self-protective, and content owners can distribute the entire image as a sample to various open media or to the Internet. When a user wants to use a clean copy of the image, all he/she needs to be is to request a "decryption" key and pay some fee for it. This will reduce the security risk and the amount of the data transmission per each buy/sell transaction.

Watermarking technology for DVD Playback and Record Control

In the previous section, several watermark applications that are currently in place or very close to being released were discussed. In most of the cases, those applications are targeting at a closed environment or exist between limited number of members, e.g., between image libraries and content creators, insurance companies and repair shops, and so on. In this section, I would like to focus on the watermark application that has much more public impact, namely DVD Copy Control.

Background

Since 1996, digital watermark has been considered one of the potential "safety nets" for copy protection and playback control of the DVD contents. A technical subgroup called Data-Hiding Subgroup (DHSG) was formed in June 1997 under the DVD CPTWG to evaluate the technical feasibility of a total of eleven watermark technology proposals. The interim report was released at the May 1998 meeting after a series of tests including visual quality test and survivability test. The result showed that the current watermark technology has potential technical feasibility to meet the technical requirements for the DVD copy control application, and the group decided to move on to the further evaluation with regard to practical implementation.

Technical Advantages

Watermarking technology can be viewed as a way to provide a secure data channel along with the contents without modifying the installed-base Consumer Electronics (CE) devices. The embedded watermark is transparently passing through the conventional data path, and will only be detected at the digital recorders. When the watermark detection is mandated in these recorders, this watermark can be used to trigger the copy protection mechanism implemented in it. The watermarking data embedded into the video is difficult to remove without damaging the quality of the content because it is carefully "woven" into the visible part of the video data. In this application, the data called Copy Control Information (CCI) is embedded into the video data to indicate that the status of the contents is "Never Copy", "One Copy Allowed" or "Copy Freely". Recording devices will be mandated to facilitate a "watermark detector" to detect the embedded CCI from the incoming and outgoing video data, and responding properly to the recording/playback rules that are defined.

The major advantage of the watermark technology is that CCI can be transmitted over the analog video channels. Even advanced digital encryption schemes cannot extend its protection over the analog video channel, but digital watermark could. The embedded CCI will survive even if the video content is transmit through the analog video channel, recorded to video cassette, and re-digitization. As far as the digital recorders are facilitated to detect the watermark from the video, the copy protection mechanism can be extended over all the devices.

From the implementation viewpoint, because the watermark is completely transparent to the existing system or devices, it does not require that any of the install-base devices to be modified or be made obsolete. The video contents with watermarks looks and works just the same as the contents without watermarks for the devices and channels that have nothing to do with the embedded CCI, thus can be treated transparently by current and future video transmission infrastructures and devices.

Although the primary focus of this system is DVD video, the same watermark can also be applied to other forms of video contents, such as videocassettes, laser discs or broadcasted contents.

The major functional requirements for this application are high robustness, high image quality, low false positive ratio, low detection cost and real-time embedding/detection capability. The embedded data needs to survive various kinds of video processing, and be detected on the fly with low-cost detection logic to be implemented in consumer electronics devices. The balance of the cost and the function thus is very critical. A list of thirteen essential technical requirements is shown below. The detail of each requirement is described in the Call for Proposals issued by the DHSG.[4]

1. Transparency
2. Low cost digital detection

3. Digital detection domain
4. Generational copy control for one copy
5. Low false positive detection
6. Reliable detection
7. Watermark will survive normal video processing in consumer use
8. Licensable under reasonable terms
9. Export/Import
10. Technical maturity
11. Data payload
12. Minimum impact on content preparation
13. Data rate

Status of the technology selection

The original nine proposals went through a series of evaluation conducted by DHSG and the result is summarized in the Interim report[5] generated by the co-chairs of DHSG. Currently, these proposals are merged into two proposals, one called Galaxy which is jointly proposed by IBM, NEC, Hitachi, SONY and Pioneer,[6] and the other is jointly proposed by Philips, Macrovision and Digimarc[7]. The final evaluation is planned by a sub-committee under CSS entity called the Watermark Review Panel (WaRP). The planned evaluation includes technology readiness, visual quality, detection reliability, statistical analysis of false positive ratio, gate-count analysis for hardware implementation and survivability against low-tech attacks. The review of licensing terms and conditions will also be included in this evaluation. The final decision is expected within three months.

Overview of Galaxy watermarking proposal for DVD copy control application

The Galaxy watermark proposal is one of the two proposals to be evaluated by the WaRP. IBM, NEC, Hitachi, SONY and Pioneer jointly propose it. The watermark technology is based on IBM DataHiding™ technology and NEC soft watermark technology, and was jointly improved by five companies with the expertise in both consumer electronics domain and information technology product domain. In this section, a brief overview of the Galaxy proposal is presented.

The Galaxy watermarking technology embeds 8 bits of data as a transparent digital watermark into baseband (uncompressed) digital master video at the motion picture studio environment. This watermark can be detected in both baseband and MPEG2 domains. We call it Primary Mark (PM). The first two bits of PM represents CCI, such as “No copy,” “One Copy” and “No More Copy”. The detector uses a uniquely designed Adaptive Frame Accumulation Detection (AFAD) algorithm to detect PM with pre-set false positive error ratio. The advantage of the AFAD algorithm is that the reliability of the detection is maintained uniformly while the detection period will be automatically adjusted depending on the level of the residual watermark signal by the detector.

Watermark compatibility between baseband video and MPEG2

Galaxy watermarking technology is compatible and interchangeable between the MPEG domain and baseband domain. This means the embedded watermark signal can be detected from either compressed MPEG2 stream or uncompressed baseband video. This is essential because the watermark detector may need to be implemented in the location where only one form of video is available. For instance, when the recording is made within the compressed digital domain, the only data available is compressed MPEG stream. On the other hand, if the watermark detector is implemented in the analog input/output of the recorder, the only data available to the decoder will be the baseband video. By having the compatibility between baseband video and MPEG2, the Galaxy system also offers device manufacturers a great deal of freedom to choose the implementation location of the watermark detector and the Copy Mark inserter.

Galaxy proposal for generational copy control

Galaxy proposes to have another transparent watermark inserted into the video at digital recorders to serve as an identifier of the copied material. This is called copy mark insertion (CMI). The CMI can take place in both baseband and MPEG2 domains and the detection of the same Copy Mark (CM) can be done in both domains. When the recording of the “One Copy” content is made, a CM will be inserted into the video to indicate the change of the status to “No more copy”. This is the generation copy control. Note that the CM can also be inserted and detected in both baseband and MPEG2 domains.

Future implementation

As described above, the implementation of the proposed watermark system requires enforcement to the device manufacturers to implement watermark detectors in their products. It may be done through a licensing entity or legislation, but details have not yet been discussed. However, the content owners may choose to start embedding watermark into their video contents, even before the full implementation in the consumer electronics devices is completed since the watermark does not affect to the current system, and can be used as a robust universal tag to identify the copyrighted contents.

Conclusion

The study of the watermark technology has become active since mid-1990s, and some technologies are already adopted in practical applications as a product or as a proprietary ser-

vices for enterprises. Although this is a relatively new technology area, it quickly becomes a practical and effective solution in some application areas, and has great potential for some other areas as well. The key to the successful implementation is to understand the advantages and the limitations of the watermark technology, and to use the watermark technology as a complimentary element to the existing security elements such as cryptographic algorithms.

References

[1] W. Bender, D. Gruhl and N. Morimoto, “Datahiding Techniques,” Proceedings, SPIE 2420 (1995).

[2] W. Bender, D Gruhl, N. Morimoto and A. Lu, “Techniques for Datahiding,” IBM System Journal, VOL.35, 3&4 (1996).

[3] I. Cox et al. “Secure spread spectrum watermarking for Multimedia,” Technical report 95-128, NEC Research Institute, Technical Report, (1995).

[4] DataHiding SubGroup Call for proposal Version 1.0 (1997).

[5] DHSG Interim Report (1998)

[6] Galaxy Watermark Proposal Version 1.0 (1999)

[7] Philips/Macrovision/Digimarc Watermark Proposal (1999)

[8] http://www.ibm.com/software/DataHiding