A New Video Watermarking Protocol

by Edward J. Delp and Eugene T. Lin

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

A NEW VIDEO WATERMARKING PROTOCOL

Edward Delp and Eugene Lin

Video and Image Processing Laboratory
Purdue University
School of Electrical and Computer Engineering
West Lafayette, Indiana
USA

ABSTRACT

This paper overviews the problems with temporal synchronization in video watermarking and describes a new approach for efficient synchronization and resynchronization. A complete version of the new method is presented in [1].

1. INTRODUCTION

Many blind watermark detection techniques (including the correlation-based detectors often used in spread-spectrum watermarks [2, 3]) require the detector to be synchronized with the watermarked signal before reliable watermark detection can occur. Synchronization is the process of identifying the correspondence between the spatial and temporal coordinates of the watermarked signal and that of an embedded watermark. Ideally, the watermark detector will be given a watermarked signal such that the coordinates of the embedded watermark have not been changed since the embedding process. In this case, synchronization is trivial and the detector can proceed in the manner prescribed by the watermark detection technique [4]. However, if the coordinates of the embedded watermark have been changed (such as when the watermarked signal is re-scaled, rotated, translated, and cropped as shown on Figure 1) the detector must identify the coordinates of the watermark prior ‹to detection. Synchronization is crucial to successful watermark detection and if the detector cannot synchronize with its input signal, an embedded watermark may not be detectable even though it is present in the signal. Many of the techniques that are used to attack watermarked signals do not "remove" the watermark, as widely believed, but desynchronize the detector [5, 6].

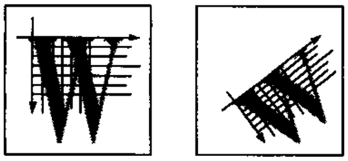

Figure 1. A synchronization attack

Synchronization is a problem that cannot be ignored in most video watermarking applications, even in the absence of a malicious attacker. In applications such as secure digital television and broadcast monitoring, the watermark detector may be expected to detect the watermark starting from any arbitrary temporal location within the video signal (as opposed to starting detection from the "beginning" of the video signal), which is known as initial synchronization. In other applications, the video signal arriving at the watermark detector may have been damaged to the extent that the detector loses synchronization and must resynchronize before watermark detection can resume. One such application is streaming video [7, 8, 9], where parts of the video signal can be damaged or lost as it is transmitted over a network. The video signal may also be interrupted for an indeterminate time for reasons beyond the control of the user, such as network congestion. (We note that in video streaming, the network is not under any constraint to preserve the perceptual quality of the video.) In these applications, it is essential that the watermark detector can resynchronize to the video, even after many frames of the video have been lost. Obviously, robust watermarking techniques should be robust against synchronization attacks by a hostile attacker.

In the worst case, establishing synchronization would involve an exhaustive search over the space of all possible geometric and temporal transformations to find the watermark. This is not practical for video watermarking applications that require real-time watermark detection. Methods for spatial synchronization in still images (see [10] for an overview) have been examined and typically involve efficient search techniques to deduce the geometric transformation or the use of embedding domains that are invariant to geometric transformations. However, some still-image watermark synchronization techniques are too computationally expensive for real-time video applications, and those still-image techniques that are suitably efficient for real-time implementation do not consider temporal synchronization.

One oft-mentioned synchronization technique is the embedding of a pattern, known as a template, which a detector can examine to determine the orientation and scale of the watermark. (Templates have been suggested for video watermark synchronization [2, 11].) There are several disadvantages to template embedding. First, a template is designed to be easily detected; hence the template itself

This work was supported by a grant from Digimarc.
Address all correspondence to E. J. Delp, ace@ecn.purdue.edu

0-7803-7523-8/02/$17.00 ©2002 IEEE

can be vulnerable to removal [12]. Second, the template must be robustly embedded into the video signal that could introduce additional distortion in the watermarked video.

In this presentation, we consider the problem of temporal synchronization in video watermarking and temporal attacks. (These issues can also apply for time-varying signals other than video, such as audio.) Spatial synchronization issues, such as synchronization after rotation, scaling, translation, and cropping attacks, is not considered here. A method for synchronization in the presence of spatial shifts is described in [13]. The inclusion of the temporal coordinate dramatically increases the potential search space necessary for synchronization in video as compared to still images. More significantly, however, the temporal redundancy that is present in most video sequences can be exploited in attacks against watermarked video that are not possible for still images, such as frame cropping, insertion, transposition, and frame averaging (temporal collusion.)

We will present a method (or protocol) in the design of video watermarks that allows efficient temporal synchronization by introducing redundancy in the structure of the embedded watermark. Our work exploits the use of frame dependent watermarks [14, 15]. The detection mechanism takes advantage of the redundancy to reduce the search required for synchronization. The method does not involve the embedding of templates and generates a watermark that is dependent on the content of the video.

It is important to note that our new method is independent of the actual watermarking technique (embedder and detector). In fact our method could be retrofitted into most existing video watermarking techniques. A complete description of our method is available in [1].

2. REFERENCES

[1] E. T. Lin and E. J. Delp, "Temporal Synchronization in Video Watermarking," *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents IV*, Vol. 4675, January 20 - 25, 2002, San Jose, CA.

[2] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing*, vol. 66, no. 3, pp. 283-301, May 1998.

[3] I. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, December 1997.

[4] R. Wolfgang, C. Podilchuk, and E. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108-1126, July 1999.

[5] F. Petitcolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking systems," *Proceedings of the Second International Workshop in Information Hiding*, pp. 218-238, Portland, April 14-17, 1998.

[6] G. Braudaway and F. Mintzer, "Automatic recovery of invisible image watermarks from geometrically distorted images," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents II*, vol. 3971, pp. 74-81, San Jose, January 24-26, 2000.

[7] E. Lin, C. Podilchuk, T. Kalker, and E. Delp, "Streaming video and rate scalable compression: What are the challenges for watermarking?", *Proceedings of the SPIE Security and Watermarking of Multimedia Contents III*, vol. 4314, pp. 116-127, San Jose, January 22-25, 2001.

[8] E. Lin, G. Cook, P. Salama, and E. Delp, "An overview of security issues in streaming video," *Proceedings of the International Conference on Information Technology: Coding and Computing*, pp. 345-348, Las Vegas, 2001.

[9] A. Eskicioglu and E. Delp, "An Overview of Multimedia Content Protection in Consumer Electronics Devices," *Signal Processing: Image Communication*, vol. 16, pp. 681-699, 2000.

[10] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*, San Francisco: Morgan Kauffman Publishing, 2002.

[11] F. Deguillamue, G. Csurka, J. Ruanaidh, and T. Pun, "Robust 3D DFT video watermarking," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 113-124, San Jose, January 25-27, 1999.

[12] A. Herrigel, S. Voloshynovskiy, and Y. Rytsar, "The watermark template attack," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents III*, vol. 4314, pp. 394-405, San Jose, January 22-25, 2001.

[13] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, "A video watermarking system for broadcast monitoring," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 103-112, San Jose, January 25-27, 1999.

[14] M. Holliman, W. Macy, and M. Yeung, "Robust frame-dependent video watermarking," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents*, vol. 3971, pp. 186-197, San Jose, January 24-26, 2000.

[15] B. Mobasseri and A. Evans, "Content-dependent video authentication by self-watermarking in color space," *Proceedings of the SPIE Security and Watermarking of Multimedia Contents III*, vol. 4314, pp. 35-44, San Jose, January 22-25, 2001.