IF ONE WATERMARK IS GOOD, ARE MORE BETTER?

Fred Mintzer and Gordon W. Braudaway

IBM T.J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598, USA

ABSTRACT

Invisible watermarks are not all alike. Different techniques are used to embed different types of watermarks into digital media objects to accomplish different goals. Some watermarks are intended to robustly carry ownership information; some are intended to carry content-verification information; and some are intended to convey side information, or captions. In this talk, some opportunities to employ multiple watermarks to convey multiple sets of information, intended to satisfy differing or similar goals, are examined. Problems presented by the insertion of multiple watermarks are discussed. Progress towards developing techniques that embed multiple watermarks into an image will also be presented.

1. INTRODUCTION

Invisible watermarking involves imperceptibly embedding data, called a watermark, into an image or other digital media object to enhance or protect its value. Although watermarking is relatively new field, many applications have already been proposed. Recent work [1,2,3] has identified three clusters of applications. One uses watermarks **to convey ownership information**. A second uses watermarks **to verify that object content has not changed.** A third uses watermarks **to convey object-specific information, or captions**, to a community of willing recipients

The application clusters generally require application-specific watermarking techniques to best address them. In the remaining subsections of this **Introduction**, we briefly describe the application clusters and summarize their technical requirements.

1.1 Watermarks to convey ownership info

Applications that convey ownership information are often desired by organizations that own the copyrights to digital media objects and license them. These organizations include news agencies and photo banks, museums and libraries.

In a typical image application, the content owner provides an image that will be published by the recipient; in exchange, the owner will receive a royalty for the image's use. A concern of the owner is that the publisher will neglect to pay the royalty; this omission may be intentional or unintentional. To deter such misappropriation, the owner may wish to place a watermark, containing ownership information, in the image.

The ownership information may identity either the owner or the recipient. If the watermark identifies the owner, the owner might subsequently scan suspect published material to determine whether a printed image contained his watermark; the owner would consider its presence to be evidence of his ownership. If the watermark contained the recipient's identification, the owner might subsequently scan the published material to determine who received the material; if the image had been used without payment of royalties, the owner might wish to cease doing business with the recipient. Descriptions of three scenarios that use invisible watermarking to convey ownership information are given in [2]. Many techniques for applying an ownership watermark are described in [4].

For a watermark to be effective in ownership applications, it must remain in the media object and be reliably detectable from the published product. For the publishing example described above, it is important that the watermark be reliably detectable from the scan of a published image.

This is a considerable challenge. Before printing, an image is often cropped, re-sized, sharpened, contrast enhanced, color corrected, and JPEG compressed. Hence, a watermark for ownership applications must survive a variety of image processing tasks that are routinely used to prepare images for publishing. Furthermore, there is an economic incentive for publishers to remove watermarks. Those publishers that would seek to not pay royalties might attempt to remove the watermark, and many common image processing tools are available to accomplish this. Thus, for an ownership watermark to be effective it should robustly resist image-processing attacks, intentional and unintentional, that might remove it. For that reason, we describe watermarks for ownership applications as ***robust watermarks.***

One straightforward attack can be mounted whenever a malicious party has access to a watermark ***in the clear,*** where a watermark "in the clear" is one that can be extracted by anyone who has access to the extraction process. With this attack, the attacker alters the watermarked image and extracts the watermark. If the inserted watermark is identical to the extracted watermark, a different or additional alteration is attempted. The sequence of alterations continues until the extraction process reveals that the mark has been removed or altered; then, the evidence of ownership has been removed. To counter this ***iterative attack on watermarks in the clear***, most ownership marks are inserted with a ***watermark key.*** In this case, the watermark key is required to extract the watermark and that key is only supplied as needed. Without the watermark key, the attacker cannot extract the watermark with this attack. We note that the phase “in the clear” is now generally used to describe watermarks that are not protected by a watermark key.

Three recent papers [5,6,7] have discussed attacks to remove ownership watermarks. They provide a more detailed description of what watermark robustness entails.

Robust watermarks are often applied with great redundancy to achieve the robustness desired. Hence, ownership watermarks generally convey relatively small amounts of data, ranging from tens to hundreds of bits.

1.2 Watermarks to verify that object content

A second application cluster uses watermarks to determine whether a media object has been altered since some earlier time when it was watermarked. Some applications scenarios for this cluster are also given in [2]. Some example techniques are described in [9,10,11].

In a typical image application, an image is watermarked at the time it is loaded into a digital library. At some later time, the watermark is extracted. If the extracted watermark matches the inserted watermark, the object is judged to be unchanged; if it does not match the inserted watermark, the image is judged to have been altered. An inspection of the extracted watermark (and its difference from the inserted watermark) reveals where the alterations have occurred. For these applications, it is desired that the watermark will be altered if the image is altered; we call these watermarks ***fragile watermarks*** because they should be easily damaged if the object is altered.

If a fragile watermark is in the clear, one might alter the content of a false image, extract its watermark, and interate until the extracted watermark matched the watermark inserted in the true image. To prevent such a false insertion, a watermark key is also often used with fragile watermarks.

Fragile watermarks do not require redundancy. Consequently, they often convey very large amounts of data. The technique of [11], for example, embeds one bit of watermark data for each pixel in the marked image; this can be millions of bits.

1.3 Watermarks to convey captions

The third application cluster uses watermarks to convey object-specific information, called captions, to a community of willing recipients. With these applications, both the content owners and the recipients desire that the information be conveyed.

In a typical application, a digital photo agency uses a watermark to convey data that records the name of the owning agency and an image identification number. Then, when the image is published, the publisher knows whom to contact for permission. Furthermore, the owning agency knows how much to charge and what photographer to compensate (since it knows which image is being used). Other proposed collaborative watermarking applications are described in [1].

To enable proper conveyance, collaboration among the community of content owners and the community of recipients is needed. This is done so that the content owners may employ a single watermarking technique and the recipients can employ a single watermark extraction technique. Without such standards, it is difficult to imagine how this class of applications could be undertaken.

Although the recipients desire to extract the watermark information, some robustness is required, as captioning watermarks should survive unintended attacks to be most useful. However, captioning watermarks must often convey more information than ownership watermarks. Consequently they can employ less redundancy, and hence they are less robust.

2. Multiple Watermarks to Address Multiple Applications

To accomplish several goals, one might wish to embed several watermarks into the same image. For example, the owner might desire to:

- use one watermark to convey ownership information,
- use a second watermark to verify content integrity, and
- use a third watermark to convey a caption (that might describe the content of the image).

In attempting to accomplishment this, one should first look at the robustness of each technique. As noted earlier,

- ownership watermarks should be very robust,
- captioning watermarks should be robust, and
- verification watermarks should be quite fragile.

Embedding a fragile watermark followed by embedding a robust watermark is bound to damage the fragile watermark. Indeed, by design, a fragile watermark should be damaged by any operation that alters the image, and robust watermarking is such an operation.

In general, to apply multiple disparate watermarks,

- the most robust (ownership) watermark should be embedded first,
- the most fragile (verification) watermark should be embedded last, and
- moderately robust (captioning) watermarks should be inserted in between.

Embedding multiple watermarks will then be successful if the robust watermarks are sufficiently robust to withstand all subsequent watermark insertions

After the insertion of multiple watermarks, the watermarked image will posses texture resulting from each watermark. Embedding multiple watermarks, we note, also requires that each watermark add less texture than would be permissible if that watermark were employed alone.

Hence, embedding multiple disparate watermarks to an image can be successful if

- the robust watermarks are sufficiently robust, and
- each invisible watermark is sufficiently sub-visible that the suite of watermarking is still invisible.

3. Multiple Watermarks to Address one Application Multiple Times

One might also envision embedding multiple watermarks for similar applications.

3.1 Multiple ownership watermarks

For example, as noted earlier, ownership watermarks are sometimes used to identify the owner and sometimes used to identify the recipient. One can imagine employing two ownership watermarks to identify both the owner and the recipient.

Here, the question arises. How should the two watermarks best be embedded? Intuitively, we expect that embedding them simultaneously is desired. This is a topic of current research.

3.2 Multiple verification watermarks

One might envision employing multiple verification watermarks to an image to increase verification security. Then, if party one, possessing key one, forged a watermark on a false image, party two, using key two, would still be able to detect the alteration.

Since verification watermarks are intentionally fragile, one cannot apply a second fragile watermark after the first. Hence, to apply two verification watermarks, one must apply them simultaneously. How to accomplish this is another topic of current research.

3.3 Multiple watermarks for multiple captions

One might imagine the use of multiple captioning watermarks to apply multiple captions in the case where a recipient wants to add supplemental captioning to an object.

Here, the recipient might merely extract the original caption, append an additional caption, and embed a watermark that conveys the expanded caption.

However, if this were the case, the image would have been degraded by the application of two captioning watermarks. It might simply be more effective to contact the owner and ask that a watermark, conveying the expanded watermark, be applied to the original image. Hence, the need for multiple captioning watermarks is not readily apparent.

4. Remarks

Above, we have envisioned several situations in which it might be desired to embed multiple watermarks in an image.

When the multiple watermarks are intended to satisfy different applications, the order in which the watermarks are applied is vital. Increased robustness of the robust watermarks and decreased visibility of all watermarks are desired in this environment.

In the case where multiple watermarks of the same type are embedded, it may be advantageous to develop techniques that apply multiple watermarks simultaneously. This is especially true for verification watermarks; in this case, the multiple watermarks must be applied simultaneously.

5. Acknowledgements

Many of our ideas were formed in collaboration with our former IBM colleague, Minerva Yeung. We gladly acknowledge her contribution to this work.

6. References

[1] Fred Mintzer, Gordon W. Braudaway, and Alan E. Bell, "Opportunities for Watermark Standards," *Communications of the ACM*, vol. 41, July 1998, pages 57-64.

[2] Fred Mintzer, Gordon W. Braudaway, and Minerva M. Yeung, "Effective and Ineffective Image Watermarks," IEEE *1997 International Conference on Image Processing,* Oct 1997, vol. III, pages 9-12.

[3] Fred Mintzer, Jeffrey Lotspiech and Norishige Morimoto, "Safeguarding Digital Library Contents and Users: Digital Watermarking," *DLIB Magazine*, http://www.dlib.org/dlib/december97/ibm/12lotspiech.html, Dec.1997.

[4] Mitchell D. Swanson, Mei Kobayashi, and Ahmed Tewfik, "Multimedia Data Embedding and Watermarking Technologies," *Proceedings of the IEEE,* June 1998, pages 1064-1087.

[5] Scott Craver, Boon-Lock Yeo, and Minerva M. Yeung, "Technical Trials and Legal Tribulations," *Communications of the ACM*, vol. 41, July 1998, pages 45-54.

[6] S. Craver, N. Memon, B.L. Yeo, and M.M. Yeung, "Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," *IEEE JSAC,* May 1998, pages 573-586.

[7] C. Dwork, "Copyright? Protection?," *Mathematics of Information Coding,* edited by Cybenko, O'Leary, and Rissanen, Springer Verlag, New York, 1998.

[8] Gordon W. Braudaway, "Results of Attacks on a Claimed Robust Image Watermark, Proc. *IS&T/SPIE Symposium on Optical Security and Countefeit Deterrence Techniques II,* to appear, Feb 1998, pages 122-131.

[9] G.L. Friedman, "The Trustworthy Digital Camera," *IEEE Trans. Consumer Electron.,* Nov. 1993, pages 93-103.

[10] R. Wolfgang and E. Delp, "A Watermark for Digital Images," *1996 IEEE Internal Conference on Image Processing,* Sep 1996, proceedings pages 219-222.

[11] Minerva M. Yeung and Frederick C. Mintzer, "Invisible Watermarking for Image Verification, *Journal of Electronic Imaging*, March 1998, pages 578-591.