Editor: Ron Vetter, North Dakota State University, IACC Bldg., Rm. 258, Fargo, ND 58105-5164; (701) 231-7084; rvetter@plains.nodak.edu

Protecting ownership rights through digital watermarking

Hal Berghel
University of Arkansas

Lawrence O'Gorman
Bell Laboratories

The Internet revolution is now in full swing, and commercial interests abound. As with other maturing media technologies, the focus is moving from technology to content, as commercial vendors and developers try to use network technology to deliver media products for profit. This shift inevitably raises questions about how to protect ownership rights.

Digital watermarking has been proposed as a way to identify the source, creator, owner, distributor, or authorized consumer of a document or image. Its objective is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute. In the event of illicit use, the watermark would facilitate the claim of ownership, the receipt of copyright revenues, or successful prosecution.

Watermarking has also been proposed for tracing images that have been illicitly redistributed. In the past, the infeasibility of large-scale photocopying and distribution often limited copyright infringement, but modern digital networks make large-scale dissemination simple and inexpensive. Digital watermarking allows each image to be uniquely marked for every buyer. If that buyer makes an illicit copy, the copy itself identifies the buyer as the source.

Digital watermarking allows each image to be uniquely marked for every buyer, so that illicit copies can be traced to their source.

Of course, digital watermarking is not the only technology intended to protect intellectual property in digital format. Digital documents are commonly encrypted to make them unviewable without the decryption key. This technique works well for transmission and storage, but once a document is decrypted for viewing or printing, subsequent retransmission or dissemination is not encrypted.

Visible versus invisible watermarks

A digital watermark is a digital signal or pattern inserted into a digital image. When visible, it is akin to its bond paper ancestors, in which the opacity of paper is altered with a stamp of an identifying pattern that signifies the paper type or manufacturer. The proposed applications of digital watermarking are far more diverse, and the watermark may not be visible to the casual viewer.

The watermarks in Figures 1 and 2 on the next page illustrate the technique. The high contrast between background and foreground makes the watermark in Figure 1 quite obtrusive—it has no place to hide. The color image in Figure 2 renders the watermark less obvious.

Visible and invisible watermarks both serve to deter theft but in very different ways. Visible watermarks are like a "Do Not Trespass" sign; invisible watermarks are like the dye banks use to indelibly mark the hands and clothes of bank robbers.

By conveying an immediate claim of ownership, visible watermarks diminish the commercial value of a document or image to a would-be thief without lessening its utility for legitimate purposes. This assumes, of course, that perpetrator and fence alike understand enough about the technology to be concerned. A familiar example of a visible watermark is the translucent logo placed at the bottom right of the screen image by CNN and other television networks.

Invisible watermarks, on the other hand, increase the likelihood of successful prosecution once a theft has occurred. To work effectively, an invisible watermark should nevertheless be detectable by those who know where and how to look—usually the original owners. If thieves could find it, they would try to remove it.

Though neither exhaustive nor definitive, Table 1 on the next page shows some anticipated primary and secondary benefits of visible and invisible watermarks.

Watermark requirements

To achieve maximum protection of intellectual property with watermarked documents, several objectives must be satisfied:

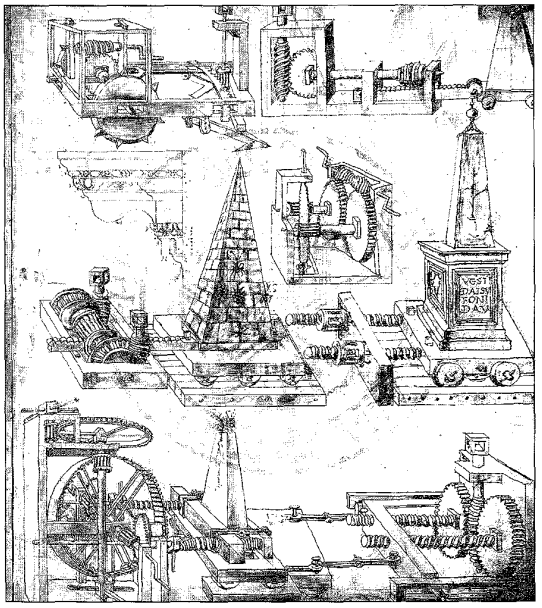

Figure 1. A digitally produced copy of a fifteenth-century drawing with a digital watermark superimposed.

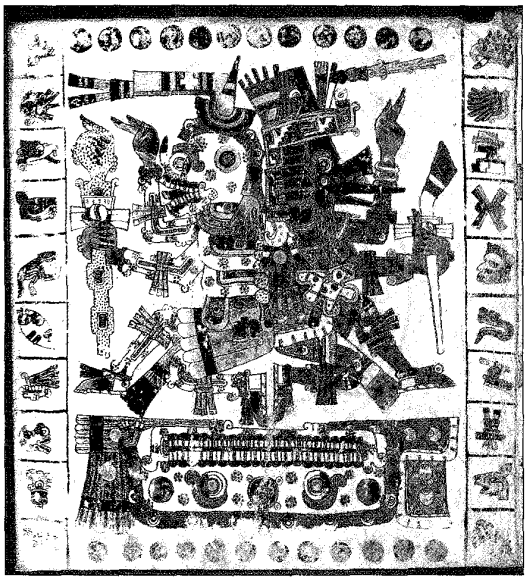

Figure 2. The digital watermark is subtle in this digitized artwork from a sixteenth-century Aztec manuscript. (Used with permission of IBM's Digital Library Project, http://www.ibm/features/library/.)

- The watermark must be difficult or impossible to remove, at least without visibly degrading the original image.
- The watermark must survive image modifications that are common to typical applications, such as scaling and color requantization, commonly performed by a picture editor, or lossy compression techniques like JPEG, used for transmission and storage.
- An invisible watermark should be imperceptible so as not to affect the experience of viewing the image.
- For some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decodability without requiring the original, unwatermarked image would be necessary for efficient recovery of property and subsequent prosecution.

Because these requirements compete with each other, researchers face significant challenges. A successful watermarking method would have to be accepted and used on a large, commercial scale, and it would have to stand up in court. None of the digital techniques developed so far meets all of these tests.

Watermarking techniques

The different approaches to digital watermarking tend to cluster into a few basic types within the text and graphics categories. Since we cannot describe all the methods here, we will look generally at families of techniques.

Techniques for images. Several different methods enable watermarking in the spatial domain. The simplest (*too* simple for many applications) is to just flip the lowest-order bit of chosen pixels in a gray-scale (8-bit) or color (24-bit) image. This works well only if the image will not be subject to any modification, such as color modification done by a photo editor.

Another technique embeds a more robust watermark in much the same way as a watermark is added to paper: You

Table 1. Some anticipated primary and secondary benefits of visible and invisible watermarks.

Purpose	Visible	Invisible
Validation of intended recipient	-	Primary
Nonrepudiable transmission	-	Primary
Theft deterrence	Primary	Primary
Diminishment of commercial value but not utility	Primary	-
Discouragement of unauthorized duplication	Primary	Secondary
Discouragement of analog duplication	Primary	-
Digital notarization and authentication	Secondary	Primary

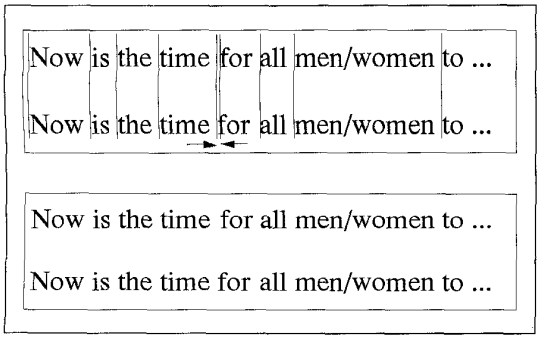

Figure 3. An illustration of textual watermarking. (Top): The word "for" is shifted subtly to the left, creating a watermark that is (bottom) imperceptible under normal reading conditions.

superimpose a watermark symbol over an area of the picture and add some fixed intensity value for the watermark to the varied pixel values of the picture. This approach lets you embed visible or invisible watermarks, depending on whether the intensity value is large or small, respectively.

One disadvantage of spatial domain watermarks—besides the trade-off between invisibility and decodability—is that a common picture-cropping operation can eliminate the watermark.

Using color separation characteristics, we can arrange for a spatial watermark to appear in only one of the color bands. Thus the watermark becomes more difficult to detect under regular viewing, but it appears immediately when the colors are separated for printing or xerography. The document is thus useless to the printer unless the watermark can be removed from the color band. This approach is used commercially to let editors inspect digital images from a stock-photo house before buying unwatermarked versions.

Watermarking can be applied in the frequency domain (and other transform domains) by first applying a transform like the fast Fourier transform. This method is similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture. Upon inverse transformation, watermarks applied to the frequency domain will be dispersed over the entire spatial image, so this method is not as susceptible to defeat by cropping as the spatial technique. However, the trade-off between invisibility and decodability is greater here, since in effect the watermark is applied indiscriminately across the spatial image.

Techniques for text. Three methods have been proposed for applying watermarking to text images: text-line coding, word-space coding, and character coding. For text-line coding, a document page's text lines are shifted imperceptibly up or down. For a 40-line text page, for instance, this yields 2^{40} possible code words. For word-space coding, the spacing between words in a line of justified text is altered, as shown in Figure 3. For character coding, a feature such as the end line at the top of a letter, say "b," is imperceptibly extended.

These methods have an advantage over those applied to picture images: Applying two or three methods to one document makes it impossible to extract the watermark by spatially registering two documents with different watermarks. Of course, the watermark can be defeated by retyping all the text in the document.

What's next for watermarking?

Although publishers have been clamoring for a way to protect their material on electronic networks, there has been no rush to embrace any of the current schemes. Perhaps the publishing community needs a period of inspection and appraisal. We believe that publishers and scientists don't fully understand the problem's practical aspects. Should the watermarks be visible or invisible? What constitutes invisible? How easily can watermarks be removed from images? What constitutes a reasonable level of photo editing? Of degradation? Can the original image be required for decoding? Is watermark transferal from the electronic medium to the printed medium important? How are the watermarks to be policed?

As scientists propose solutions and publishers experiment with them, debating the pros and cons of each, certain watermarking methods will prove themselves and gain wide use. When that happens, external agencies will emerge to monitor electronic copyright infringement (similar to agencies for music and print copyright management). In the meantime, the challenge for scientists is to develop ever more invisible, decodable, and permanent watermarking methods to meet known requirements and perhaps even some requirements not yet articulated.

For more information

O'Ruanaidh, J., F. Boland, and C. Dautzenberg, "Watermarking Digital Images for Copyright Protection," *Proc. IEE Conf. Image Processing and Its Applications*, Inst. Electrical Engineers, Stevenage, UK, 1995.

Brassil, J., et al., "Electronic Marking and Identification Techniques to Discourage Document Copying," *IEEE J. Selected Areas in Comm.*, Oct. 1995, pp. 1,495-1,504.

Zhao, J., "Copyright Protection, Digital Watermarking Technologies," Fraunhofer Inst. Computer Graphics, Darmstadt, Germany; Web page with links to a variety of watermarking methods, http://www.igd.fhg.de/~zhao/copyright.html.

Hal Berghel *is a professor of computer science at the University of Arkansas and a researcher and author on cyberspace. His columns and editorials appear regularly in various periodicals, including* Communications of the ACM, Computer, *and* PC AI. *His Web site is http://www.acm.org/~hlb/.*

Lawrence O'Gorman *received his PhD from Carnegie Mellon University and has been at Bell Laboratories since 1984, where he is currently a Distinguished Member of Technical Staff. His interests are in image and document processing.*