Wayne Pafko
Term Paper (Final Version)
SciC8011
Paul Morin
May 8, 2000

Digital Watermarks in Scientific Visualization

Introduction

Scientific visualization converts data into images. These images can have significant artistic value. For example, it is not uncommon to see people wearing t-shirts with fractal patterns or displaying posters that show the earth from orbit. Furthermore, significant time and effort is invested in generating, interpreting, and visualizing the data used in these images. It is therefore entirely appropriate that scientific images are eligible for copyright protection just like any other creative work.

Purpose

This paper examines three papers concerned with invisible digital watermarking, an emerging technology which offers great potential for the copyright protection of any image; including images created for scientific visualization. We will critically review each article, and then discuss possible implications of this technique as applied to scientific visualization. There are several advantages and disadvantages of inserting an invisible digital watermark into an image. There are also ethical issues that must be considered. But first, let us look at each article in detail…

Article 1: Protecting Digital-Image Copyrights

This article provides a conceptual framework for discussing the use of watermarks for copyright protection. An invisible digital watermark system is critically needed because images (both still and moving) are frequently transmitted across shared networks (the Internet). However, because a digital copy is identical to the original; legal ownership of an image can be called into question. An invisible digital watermark system provides a "realistic framework for protecting intellectual property rights in digital media."

But just how would such a system work? The article discusses a hypothetical system. First, each author "possesses a unique secret key." This key can generate a unique noninvertible watermark pattern (via chaotic systems, pseudo-random number generation, or some other algorithm). This watermark pattern should then be registered with a trusted authority. Second, this watermark pattern is applied to the original image to produce a watermarked image. The original image is stored by the author. Third, the author possesses an algorithm which can detect the presence of his or her watermark in a suspicious image using the secret key. "Positive detection of the [author's] watermark…is an indication of ownership that the [author] can use as substantiated evidence in a court of law." Furthermore, the author can monitor traffic on the shared network for the presence of his or her watermark via an automated system.

So, the proposed system provides a means to generate, embed, and detect the author's watermark in an image. The watermark is made "invisible" to prevent its mischievous removal. Noninvertibility is also important to prevent its removal. The proposed system also solves the problem of multiple ownership claims. Should someone subsequently imbed their own watermark in the image, only the original author can produce an image that contains only his or her watermark, thereby proving ownership of the image. Lastly, by monitoring the network traffic this system allows the author to determine if unauthorized use of the image is actually occurring.

The article concludes by discussing 8 important properties of any watermark scheme. A watermark process should:

1) *Preserve image quality*
2) *Provide for trustworthy detection*
3) *Be computationally efficient*
4) *Be robust to digital processing*
(cropping, color correction, compression…)
5) *Resist extraction*
6) *Minimize false positives*
7) *Prevent statistical extraction*
(by examining many images created with the same key)
8) *Enable multiple watermarking*
(may be required by resellers or distributors of the image)

This article provides an excellent overview of the technical requirements for any watermarking system. It also discusses why such a system is necessary, and how it might be used to settle conflicting copyright claims. It does not critically evaluate any specific watermarking algorithms, nor does it propose to do so. This therefore cannot be considered a failure of the article.

However, the article does fail to discuss any potential negative consequences of an invisible watermark system. With any new technology, one should ask: "Who does this technology potentially help, and who does it potentially harm?" This question seems especially appropriate as we convert our society's information into digital form. The article does warn us that future techniques might make a specific watermarking system obsolete or that loss of one's private key might enable others to remove the watermark, but these are not really criticisms of the watermarking methodology itself. Are there really no potential problems with such a system, or do the authors just neglect to share the negative consequences with us?

Article 2: Resolving Rightful Ownership with Invisible Watermarking

This article discusses various attacks which can be made against watermarked images, and how such attacks can be foiled. It also discusses failings of several watermark schemes proposed in the literature. It goes on to describe the importance of standardizing on a single (or small number of) watermark scheme(s). But the main finding of the article is that noninvertablity is not sufficient to ensure that a watermark cannot be removed from an image. Their "Twin Watermarked Images Counterfeit Original" (TWICO) attack allows the mischievous introduction of a counterfeit watermark which replaces the original watermark in the image. The authors call watermark systems which are not invertible, but are still susceptible to the TWICO attack, "quasi-invertible." This is important because it demonstrates a severe defect in many previously proposed watermark schemes. The article is very important for this reason.

The article also does a nice job of identifying several potential problems with adopting watermarking as a system of ownership identification. For example, they describe how currently unwatermarked images may be stolen by others who subsequently apply their own watermark and thereby claim ownership of those images. They go on to suggest that we should be more critical of proposed watermarking schemes. For example, they say, "In spite of the promises of digital watermarking, we have to think more carefully at the application end before we propose and adopt yet another watermarking scheme. In other words, the commonly asked questions, such as how to hide marks more invisibly and how to hide marks more robustly must be asked alongside questions like, 'for what purposes can this watermarking technique be used?' 'in what ways can this watermarking technique be attacked?' and 'for what reasons should this watermarking scheme be trusted to deliver on its promises?'"

However, the article does have several failings. First, at times it is poorly written and it suffers from several subtle, but annoying, errors. For example, the title reads "Resolving Rightful *OWNERSHIPS* with Invisible Watermarking Techniques…" (emphasis added). But *OWNERSHIPS* makes no sense in this context because we are trying to find the single legal owner of an image via watermarking. Therefore, the title should read "Resolving Rightful *OWNERSHIP* with Invisible Watermarking Techniques…" One starts to worry about the quality of the article as a whole when the title itself contains errors!

Furthermore, the article suffers from some leaps of logic. For example, the article concludes that "Current copyrighting mechanisms for photographs and images involve registration of the item being copyrighted with a centralized authority. All contests of ownership are then resolved by this central authority. It has been recognized for quite some time now that these laws are quite inadequate for dealing with digital data that can be so easily copied and manipulated." But this conclusion does not follow from the reasons. Why does ease of copying and manipulating make a central authority obsolete? This is the only location where the article discusses this topic, and their conclusion is not logically supported by their reasons. Granted, this argument is not central to the article, but annoying errors like these distract the reader from the rest of their argument.

Article 3: Watermarking Algorithm Based on a Human Visual Model

This article discusses "an additive watermarking technique for grey-scale pictures." This scheme uses a human visual model to help make the watermark "invisible." The article goes into great depth concerning the types of filters that are used to create the invisible watermark. It also discusses several characteristics of human vision, and how "image features at higher frequency are less visible and can be removed without altering the global picture quality." It goes on to discuss the theoretical problem of watermarking, and how that problem is similar to transmitting data across a very noisy medium (where the picture is interpreted as the "noise"). It compares the effectiveness of the proposed algorithm with several images and the robustness of the watermark to noise, lossy compression, and attempted forgery.

The article does do a good job at describing this particular watermarking method, and its strengths and weaknesses. The author finds that it is very robust and effective with most images. However, in certain types of images (the "boats" masts image) the quality can be significantly impacted. Overall, the author does a fine job describing the technical aspects of this invisible digital watermark method.

Yet, the author's opinions concerning the need for digital watermarking and importance of copyright protection is somewhat troubling. For example, he states that "…the replication of digital material is very easy and, more dangerous, is virtually perfect. The copy is identical to the original. The ease of transmission and multiple uses is worrying too…the plasticity of digital media is a great menace." But isn't the ease of replication, ease of transmission, and plasticity of digital medium actual a great benefit to society? Copyright is a LIMITED legal protection granted to encourage the creation of original works, but it does not always supersede the public's right to information. Provisions are made for "fair use" of the copyrighted material. This article takes too strong a position concerning the rights of the copyright owner. Is this an honest error, or does it hint at the intentions of many people who are generating watermarking schemes? Will watermarking further strengthen the power of the copyright holder, to the possible detriment of society in general? This is a question well worth asking before new watermarking methods are fully adopted.

Visualization Implications

Before we begin applying invisible digital watermarking to scientific visualization we should first consider the potential advantages, disadvantages, and ethical implications of this technology.

Advantages

- ***Content Verification***: Invisible digital watermarks allow the recipient to verify the author's identity. This might be very important with certain scientific visualizations, where a maliciously altered image could lead to costly mistakes. For example, an oil company might check for an invisible watermark in a map of oil deposits to ensure that the information is trustworthy. Watermarks provide a secure electronic signature.
- ***Determine rightful ownership***: Scientific visualizations are not just graphs of data; they are often artistic creations. It is therefore entirely appropriate to copyright these images. If an author is damaged by unauthorized use of such an image, the author is first obligated to prove rightful ownership. Invisible digital watermarking provides another method of proving ownership (in addition to posting a copyright notice and registering the image).
- ***Track "unlawful" use***: This technology might allow an author to track how his or her images are being used. Automated software would scan randomly selected images on the Internet (or any digital network) and flag those images which contain the author's watermark. This covert surveillance of network traffic would detect copyright violations thereby reducing piracy.
- ***Avoid malicious removal***: The "problem" with copyright notices is that they are easily removed by pirates. However, an invisible digital watermark is well hidden and therefore very difficult to remove. Hence, it could foil a pirate's attack.

Disadvantages

- ***Degrade image quality***: Even an invisible watermark will slightly alter the image during embedding. Therefore, they may not be appropriate for images which contain raw data from an experiment. For example, embedding an invisible watermark in a medical scan might alter the image enough to lead to false diagnosis.
- ***May lead to "unlawful" ownership claims for images not yet watermarked***: While invisible digital watermarks are intended to reduce piracy, their widespread acceptance as a means of legal proof of ownership may actually have the opposite effect. This is because a pirate could embed their watermark in older images not yet containing watermarks and make a malicious claim of ownership. Such claims might be difficult to challenge.
- ***No standard system in place***: While many watermarking techniques have been proposed, none of them have become the standard method. Furthermore, none of these schemes have yet been tested by a trial case in the courts. Therefore, they do not yet offer any real copyright protection.
- ***May become obsolete***: This technology only works if the watermarks cannot be extracted from an image. However, technological advances might allow future pirates to remove the watermarks of today. It is very difficult to ensure that a cryptographic method will remain secure for all time…

Ethical Considerations

Copyright notices allow an author to claim legal ownership of an image. So too does an invisible digital watermark. They are redundant unless confronted with someone who is trying to steal an image. Therefore, it only makes sense to embed an invisible watermark if you assume that people will try to steal your image. The watermark is only useful to "catch the thief."

However, invisible watermarks have the potential to turn a lot of innocent people into "thieves." For example, what if a lone pirate removed the copyright notice (or added his own) and then retransmitted the image across the Internet. It would then contain a false (or non-existent) copyright notice and the original embedded watermark. Honest individuals might subsequently use that image under a false impression of the owner's identity (maybe they think it is in the public domain because no copyright notice remains).

In effect, our assumption that the world is full of people with malicious intent is destined to be fulfilled; even if it is largely untrue. Just because you catch someone with an illegal copy does not mean that they are actually a thief. The person may have had no idea that the image is an illegal copy, especially in an environment like the Internet where most images are automatically assumed to be in the public domain if no copyright notice is presented.

So, the honest author is left with a dilemma. Is it worth the risk to use an image that appears to be in the public domain? The image may actually have an invisible digital watermark embedded—which will be detected by the author's automated detection software—which will result in some nasty e-mails from the copyright owner—which could lead to legal problems for our honest author. Therefore, it may not be worth the trouble to use the image, even if it appears to be in the public domain.

It is hard to fault the author for this reasoning, and yet it is a sad conclusion to draw. The public might be robbed of seeing their own images (public domain images) because of the very presence of an enforced invisible digital watermarking system. This would be especially sad for the scientific community, as scientific visualizations have such tremendous potential to educate and enlighten the public. We should be encouraging, not discouraging, the widespread use of scientific visualizations (that are in the public domain). However, invisible digital watermarking may greatly discourage their use.

Furthermore, the strict enforcement of copyright laws through watermarking techniques may give an author too much power at the public' expense. It could be used to inhibit the "fair use" of images already provided for in the copyright law which states: "…the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." (US Code, Title 17, Sec 107) Such a shift would be especially painful for scientific visualizations, which are often used for educational purposes.

So, where exactly do the rights of the copyright owner end, and society's right to use that information begin? Will invisible watermarking significantly shift the location of this boundary?

Who will win and who will loss should we adopt this technology? In short, will this shift benefit or harm our society? It may in-fact do more harm than good…

Conclusion

Invisible digital watermarking has rapidly advanced from theory to practice. The three articles reviewed in this paper show that the theoretical and practical components for invisible digital watermarking are already in place. Watermarking is not just a theory, it has already arrived!

However, watermarking has developed so quickly that we have not had time to adequately consider the advantages, disadvantages, and ethical implications of this technology. Do we really want this technology to become widespread? Who will benefit and who will be harmed by watermarking? Is this really in the public's best interest?

These questions are difficult to answer because so many people do not even know that this technology exists. The only voices currently in the literature are those of the people who are creating the software or running the companies who will benefit most from this technology. Other voices and opinions need to be heard because this technology could significantly alter the relationship between content owners and the public; something in which all of us are stakeholders. This shift in power may dramatically impact the Internet, something which until now, has been a haven for the free exchange of information. It is time all of us started paying more attention to this technology and its possible implications …

Works Cited

Craver, S., memon, B., Yeo, L., & Yeung, M. *Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications*. IEEE Journal on Selected Areas in Communications. Vol 16, No 4, May 1998, p 573-586.

Delaigle, J., De Vleeschouwer, C., & Macq, B. *Watermarking Algorithm Based on a Human Vision Model*. Signal Processing. Vol 66, No 3, May 1998, p 319-335.

Ioannis, P. & Voyatzis, G. *Protecting Digital-Image Copyrights: A Framework*. IEEE Computer Graphics and Applications. Vol 19, No 1, Jan/Feb 1999, p 18-24.