GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Overview of Digital Watermark—For Images and Files

By
Bryan Smith

"The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this (http://acm.org/~hlb/publications/dig_wtr/dig_watr.html)." Digital watermarking is a means to protecting ownership of files and images.

The idea behind digital watermarking is to create a unique identifier and imbed it on a file or image in order to be able to prove that the file or image is the property of the rightful owner.

> "Watermarking differs from authentication or digital signature that proves to a receiver that the message could only have come from one particular transmitter. Mostly, authentication messages in the form of conventional hash functions can easily be deleted by a pirate who wishes to use copyrighted material for illegal purposes. The goal is to give the copyright owner of a digital image (or other piece of information) the possibility to attest technically the origin of the image (http://diva.eecs.berkeley.edu/~linnartz/water.html)."

It is also important to make the distinction between a watermark and fingerprinting. A fingerprint is created by putting a "decoder" in a file or image or attached to a file or image. This "decoder" can be decoded to extract the message the creator made. It is important to note that a fingerprint can be imbedded in a file or image like a watermark (in this case a fingerprint will sometimes be referred to as a watermark) but it can also just be attached to the file or image, unlike a watermark.

There are two types of digital watermarking, visible and invisible. A visible watermark on a file or image is very similar to a corporation's logo on its letterhead. It is basically a semi-transparent identifier (i.e. logo) that is used to show the ownership of the file or image. An invisible watermark, is an identifier that is imbedded into a file or image but is completely invisible to the eye. "It hides in the naturally occurring variations throughout an image (http://www.webreference.com/content/watermarks/tracking.html)." This invisible watermark can then be digitally extracted in order to verify the proper owner (http://www.research.ibm.com/ image _apps/watermark.html).

Besides classifying watermarks as visible and invisible, "Another classification depends on whether the watermarks applied in the space domain or in a transform domain (http://ise.gmu.edu/~csis)." The difference between these two types of classifications is space domain is a method that places the image bits in the picture, of which remains unchanged, while transform domain adjusts the picture to contain the watermark. Techniques for space domain include least significant bit, while techniques for transform domain include cropping and compression.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Obviously, there are different protection ideas behind visible and invisible watermarks. A visible watermark simply shows who owns the product, and the creator feels that the visible identifier will ward off thieves. Thus, the idea here is the same as a company's letter head – i.e. the letterhead shows who the document belongs to and as such no one would try to falsely claim it as their own. "Invisible watermarks, on the other hand, are more of an aid in catching the thief than discouraging the theft in the first place (http://w.acm.org/~hlb /publications/dig wtr/dig watr.html)." The idea behind the invisible watermark is that we may not be able to stop a thief from taking our file or image, but if we have a digital watermark in place we can go back and claim that file or image when we find the thief.

The ideal digital watermark is one that is impossible to erase (although in the real world this is difficult due to advancing technology). Further, digital watermarks that are invisible should not cause much, if any, distortion to a given file or image. Also, "Another, somewhat more subtle requirement is that the correct owner should have in his possession a copy of the original image which should not have any other watermark except possibly his own (http://proxy3.nj.nec.com /ratakonda-digital.html)." With these requirements of what is needed to create a good digital watermark, the owner of the file or image will have to decide what type of software is necessary. For example, if a person wants to imbed an invisible digital watermark on an image, he/she will have to decide how strong of a watermark needs to be imbedded. The stronger the digital watermark, the more chance of image distortion. Further, the stronger and better the digital watermark, the more money the software will most likely cost. Thus, a cost/benefit relationship exists when deciding upon the desired level of effectiveness for digital watermarks.

"Attacks on watermarks may be accidental or intentional. Accidental attacks may be the result of standard image processing or compression procedures. Illicit attacks may include cryptanalysis, steganalysis, image processing techniques, other attempts to overwrite or remove existing watermarks or confuse the reader as to the authenticity of the watermark (http://ise.gmu .edu/~csis)." Of these different techniques, the most widely known are compression and image processing techniques. An attack using compression would be done by compressing the image or file and seeing if doing that destroys the digital watermark. On the other hand, image processing is done by trying to either overwrite the watermark, insert other watermarks over the original in order to make the original not retrievable, or try to distort the watermark so that its content can not be properly retrieved.

Though defense against attacks mainly depends on the skill of the attacker and the software involved (both the attacker's software and the creator's software), it is important to keep in mind that "Transform domain watermarking and masking techniques are more robust to attacks such as compression, cropping, and image processing techniques in which significant bits are changed watermark (http://ise.gmu .edu/~csis)." Also, keep in mind, "It is tempting to concentrate on the various attacks that malicious attackers might employ. However, this is pointless if the method is not properly resistant to image edits made by either the original owner or valid users of the image (http://paris.cs.berkley.edu/~perrig /projects/wmark-realworld/node6.html)."

If the watermark can withhold an attack or an edit, the watermark can be used to trace the attacker or editor. "In addition to tagging the image, the watermark can act as a beacon for sophisticated search programs, such as Digimarc's MarcSpider. MarcSpider constantly searches

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the web for watermarked images, noting their location and use. The information is stored and supplied to clients so that they know when their image has been posted or used, enabling them to contact the web site owner about licensing arrangements or potential copyright infringement (http://www.spie.org/web/oer/november/nov99/cover1.html)."

All in all, digital watermarking is taking an image and imbedding it into a file or image in order to defend the original copyright or other license. The watermark is created to be either visible or invisible and is done with either space domain or transform domain. In order for watermarking to be effective, it should be hard to erase and not be apparent in the file or image if that is the intended purpose. The main types of attacks include compression and image processing and can be done accidentally or intentionally. In order to defend against attacks, a cost/benefit relationship exists. Further, space domain is more susceptive to image attacks when compared to transform domain. Also, watermarks can help trace stolen files or images by allowing the image to be found using searches. Finally, due to the fact that watermarks are a good way to protect copyrights and can even help to find stolen files and images, watermarks have the potential to be a major player in file and image protection in the future.

References:

1. Berghel and O'Gorman. "Digital Watermarking." 2 January 1997. URL: http://acm.org/~hlb/publications/dig_wtr/dig_watr.html.

2. "Digital Watermarking and Tracking." 26 January 1998 URL: http://www.webreference.com/content/watermarks/tracking.html.

3. Duric, Johnson, and Jajodia. "Recovering Watermarks from Images." George Mason University. 15 April 1999. URL: http://ise.gmu.edu/~csis

4. Hardin, R. Winn. "Digital watermarking: perfecting the art of security." November 1999. URL: http://www.spie.org/web/oer/november/nov99/cover1.html.

5. Linnartz, Jean-Paul. "Fingerprinting and Watermarks." URL: http://diva.eecs.berkeley.edu/~linnartz/water.html.

6. Perrig, Adrian. "The Watermarking Process." 15 January 1998. URL: http://paris.cs.berkley.edu/~perrig/projects/wmark-realworld/node6.html.

7. Ratakonda, Dugad, and Ahuja. "Digital Image Watermarking: Issues in Resolving Rightful Ownership." Department of Electrical and Computer Engineering. URL: http://proxy3.nj.nec.com/ratakonda-digital.html.

© SANS Institute 2000 - 2002, Author retains full rights.

8. “Watermarks: Protecting the image.” URL: http://www.research.ibm.com/.

.

.

.

© SANS Institute 2000 - 2002, Author retains full rights.