Hal Berghel

DIGITAL WATERMARKING FOR FUN AND PROFIT

Instead of worrying about our exposure to identity theft and financial fraud as we have in the past two columns, I thought it might be a nice change of pace to discuss something fun: digital watermarking. This brings back fond memories for I spent many years long ago doing R&D in the area. This will give me an opportunity to dust off some of my vintage software. (b.t.w., one of the smartest decisions Microsoft has made was to offer an XP virtual machine for Windows 7) one of the greatest benefits of which is the capability of running legacy and vintage software.

Let's start with an operative definition: digital watermarking is the act of imprinting a digital signal or pattern on a digital file. Since all digital files are – well – digital, one may watermark any of them regardless of format. There are two basic forms of digital watermarks: perceptible and imperceptible. The perceptible watermarks commonly associated with hardcopy have been with us for centuries, starting with elegant stationery and currency, then with proof sheets, galley proofs, photographic samples, and so forth. They're everywhere, so we'll emphasize them in this column. Contradistinguished from perceptible digital watermarks of the imperceptible variety that are present but not apparent in a document or image. Both types have their place, but serve different purposes with some overlap. The table below illustrates the differences.

Perceptible Watermarks

- identify ownership (obvious)
- non-repudiability (obvious)
- check of authenticity (obvious)
- discourages duplication (crude)
- deter theft (crude)

Imperceptible Watermarks

- identify ownership (subtle)
- non-repudiability (subtle)
- check of authenticity (subtle)
- discourages duplication (enlightened)
- deter theft (enlightened)

The subtlety and enlightened character of imperceptible watermarks is a product of the fact that the technique only works preventively if the criminal is knowledgeable enough to understand the capabilities and limitations of the digital technology behind it. For example, there are myriad ways to digitally sign a document to identify ownership. But the technique only works to prevent theft or unauthorized duplication if the potential crook knows that the document may be digitally signed and the theft traced back to him/her. Thus, the technique may be effective at preventing the theft of classified digital documents by IT professionals, but ineffective at preventing such theft by illiterati. Similarly, if a digital document is signed over to you biometrically (e.g., your fingerprint is embedded in the document) it would be challenging to say the least for a crook to argue in court that the document was signed over to him/her. Non-reputable denial is one of those legal buzzwords that mean "you can't plausibly deny it."

So perceptible and imperceptible watermarks serve to protect digital information, no matter whether images, movies, documents, audio files, etc., in different ways and toward different ends. This is where the art and science comes in knowing in which circumstances these techniques serve us best. Watermarks have been used to convey source or ownership information for copyright protection, as a self-referential authentication mechanism to determine whether the content has changed, and as a tool for covert back channeling to hide confidential or proprietary information, to name but a few applications. However, in order to be maximally effective watermarks should conform to a minimal set of guidelines:

- they must be difficult to remove without visibly degrading the original source,
- they must survive common image modifications (e.g., scaling, color re-quantization, cropping, compression, etc.),
- they must be recognizable as such in some manner - i.e., one must be able to separate the watermark from the thing watermarked even if it is not possible to recover the original source.

Of course, there are additional criteria that may be applied (e.g., the fragility, reversibility) but these will get us started. It should also be recognized that some applications are less demanding than others. One might have higher standards for determining the source of a leak of classified documents than determining the source of scanned digital postcards.

Watermarking is here to stay. Publishers are using it to protect online content. The motion picture industry is using it. Record producers are using it. Not surprisingly, the early adopters think of digital watermarking it terms of the protection of intellectual property. It has only recently been extended to classified and proprietary documents – and not very successfully at that.

SOME OF THE AUTHOR'S TOOLS OF THE TRADE

For brevity, I'll limit myself to digital imagery in the discussion to follow, although similar techniques apply to all other forms of digital media consistent with the character of the watermark.

Perhaps the easiest way to introduce the concept of a digital watermark is with a primitive form that all of us are used to: metadata in documents. You can easily look for metadata in Microsoft Word documents by clicking on "info" or selecting it from a pull-down menu. In recent versions of Word you can get a summary of the metadata with the Document Inspector (File>Info>Prepare for Sharing>Check for Issues>Inspect Document> **Note:** do not click "Remove All" unless you want to remove metadata permanently. If you're new at this, I recommend closing the window after you've viewed the summary!) Although Word metadata is pretty primitive, it does satisfy our definition of imprinting a digital signal pattern on a digital file – in this case the digital signal or pattern is simply hidden text. Word can create a perceptible watermark as well (Page Layout>Watermark>select watermark). There's an entire family of tools built into modern office productivity suites that may be thought of as variations on the watermarking theme (e.g., headers, footers, background images, track changes, and so forth). They all involve superimposing one digital element on another.

Now is the time for all men/women to ...

Now is the time for all men/women to ...

I'll illustrate another type of text-oriented watermarking below. See if you can detect the difference in the two lines of text in 0-a.

Now is the time for all men/women to ...

Now is the time for all men/women to ...

The two lines appear to be the same to the unaided eye. Now I'll superimpose some ruled lines over the text so we may check the spacing of the characters. See figure 0-b

The ruled lines clearly reveal that the position of the "f" in the lower line is several pixels to the left of the one above it. Let's assume that the horizontal bar of this "f" is 10 pixels long, 4 on each side of the vertical stroke. We could adopt a convention that the position of the left most pixel in the horizontal bar designates a number 0-4 according to its position relative to the preceding "e". We have thus created a primitive watermarking convention with 5 values. One may do that with every character in any printed line by spacing, kerning, modifying the size and shape of the serifs, modifying the length of the descenders, and so forth. One doesn't have to be an expert in calligraphy to see that one may bury a lot of information in such text-based watermarks.

Here's another example this time of spatial watermarking. I'll use an interactive watermarking tool that we built in my lab many years ago to demonstrate proof-of-concept. In this case, I'll superimpose some blocked text on an image background by altering the least significant bits of the color palette for each affected pixel in the image. From our experience, the least 4 bits of a 16-bit color palette are frequently not that important for the recognition of a typical image because the part of the image unaffected by watermarks is the equivalent of a 12-bit color palette. Watch the watermark immerge from the image in figures 1-3, as the hidden watermark is made gradually made visible.

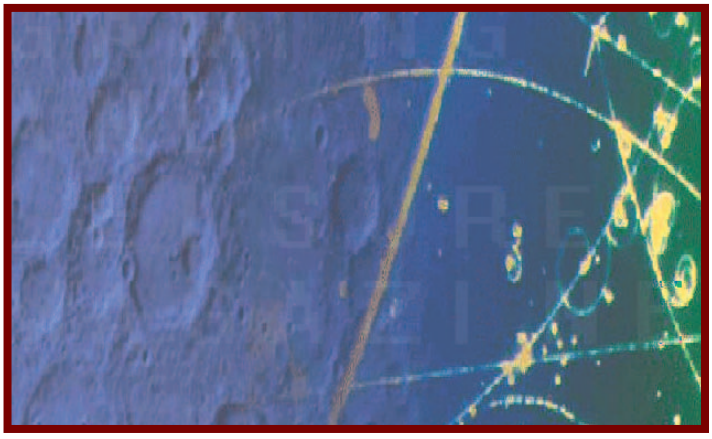

Figure 1: Text Barely Visible Against Background Image

Figure 2: Bringing Readable Text to Foreground

Figure 3: Text is as Visible as Background Image

There are a few thousand intervening stages of illumination of the text that are also possible. The point should be taken that using the least significant bits of the color palette to hide information is relatively straightforward and

Figure 4:

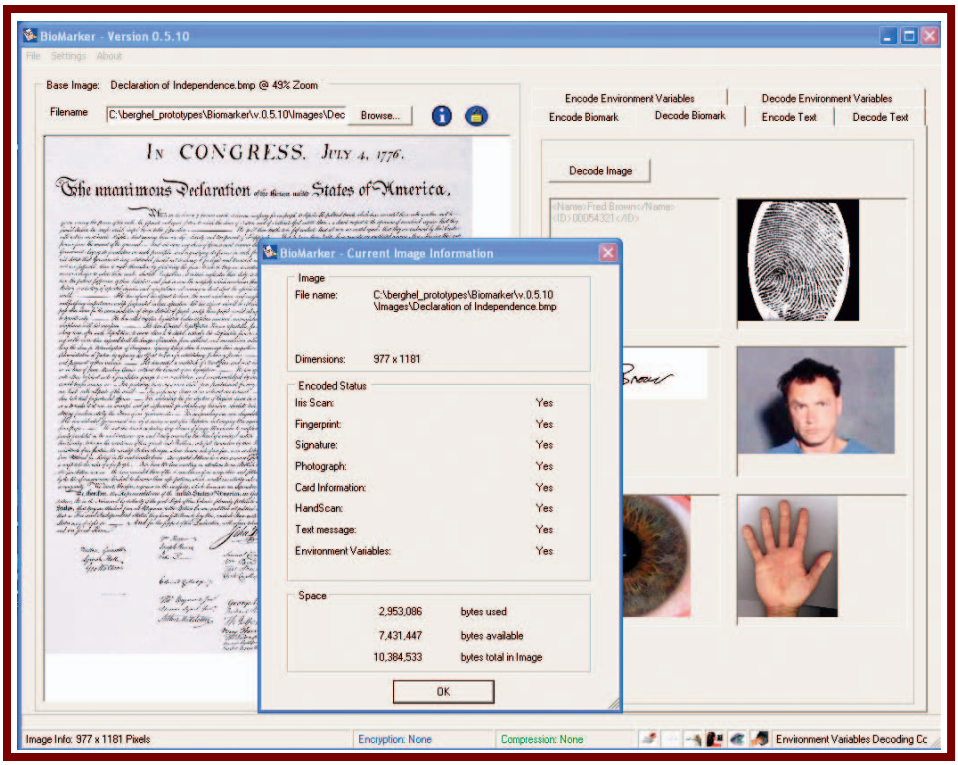

Figure 4: Biomarking at Work: Information summarized in right panel is actually embedded in the digital image (JPG) of the Declaration of Independence at left.

may have little effect on the overall quality of the image. This is an example of using the same algorithms for both perceptible and imperceptible watermarking applications. Variations on this theme of spatial watermarking abound.

To illustrate the capability of digital watermarking, I'll dust off another old program of my design – Biomarker. This was a tool that I designed about 10 years ago specifically to maximize the amount of information that could be hidden as an imperceptible watermark in another image. In this example, we take an arbitrary digital image in a standard format (jpg, bmp, gif, etc.) into which encrypted (3DES, AES, Blowfish) forms of the information below is embedded:

- name and ID number
- bitmap of scanned fingerprint
- signature from signature pad
- color photo
- iris scan
- hand scan or bone scan
- any or all of the computer and network environment variables
- and an earlier draft of this column

The result is depicted in Figure 4.

As the superimposed metadata window shows, all of these components have been successfully encrypted with AES256 and encoded into and then decoded from the 10MB digital copy of the Declaration of Independence. Approximately 29.5% of the image was used for this watermark. To put this in perspective, there are approximately 2,000 characters of text on a printed page. Using the same level of compression as our example, we could have used Biomarker to bury nearly 1,500 pages of AES 256-bit encrypted text in our image in the same amount of space. That's a reasonably sized book. I originally developed Biomarker for provenance purposes for the security and protection of classified or proprietary documents. Although I didn't bother with it, I could have added an owner's DNA profile for good measure.

BACK TO BASICS

Like most security technologies, digital watermarking isn't foolproof. For those of you who are technically minded, there is a counterfeiting scheme for a class of invertible, feature-based, frequency domain, imperceptible watermarking algorithms (how's that for a Google search term) that can subvert ownership claims for any such watermarked document. There are many other types of watermark hacks that can be used to obscure claims of provenance. And of course the most effective destruction of a digital watermark is the delete key. But what watermarking does for us is raise the bar so high as to be an effective deterrent to would be counterfeiters, fraudsters, hackers, and e_criminals of any stripe. Digital watermarking is not perfect, but it's close enough to be very useful. As I write this, the Government is prosecuting Pvt. Manning (of CableGate and Afghanistan War Diary fame) based on the correspondence of his computer's and network's logs and the logs of the Wikileak TOR sites, perhaps through some DNS leaks. As I understand the media reports, the Government claims that computer and network logs will provide the technological foundation for Manning's courts marshal. This sort of evidence seems pretty flimsy to me. However, had the documents been watermarked …

Watermarking is here to stay. Publishers are using it to protect online content. The motion picture industry is using it. Record producers are using it. Not surprisingly, the early adopters think of digital watermarking it terms of the protection of intellectual property. It has only recently been extended to classified and proprietary documents – and not very successfully at that. From a law enforcement perspective, it's a good thing that Anonymous admits its derring do or companies like Stratfor would never find the leaks. Eventually, digital watermarking will be extended to all forms of provenance of digital documents – in the widest sense. In fact, even camera manufacturers have adopted digital watermarking capability. It won't be long before it surfaces in cell phones. After Wikileaks, the light may even go on within Governments.

Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.