Digital Watermarks

Authentication of Digital Data

H R Madhusudan

This article explores the concept and utility of digital watermarks. It takes a look at the techniques used to embed and detect a watermark on digital data.

Consider the following hypothetical situations. You go to a shop, buy some goods and at the counter you are given a currency note you have never come across before. How do you verify that it is not counterfeit? Or say you go to a stationery shop and ask for a ream of bond paper. How do you verify that you have actually been given what you asked for? How does a philatelist verify the authenticity of a stamp? In all these cases, the watermark is used to authenticate. Watermarks have been in existence almost from the time paper has been in use. The impression created by the mesh moulds on the slurry of fibre and water remains on the paper. It serves to identify the manufacturer and thus authenticate the product without actually degrading the aesthetics and utility of the stock. (*Box 1*) It also makes forgery significantly tougher. Even today, important government and legal documents are watermarked. But what is watermarking when it comes to digital data? Information is no longer present on a physical material but is represented as a series of zeros and ones. Duplication of information is achieved easily by just reproducing that combination of zeros and ones. How then can one protect ownership rights and authenticate data? The digital watermarks come to our rescue. The concept and utility of digital watermarks is the same as that of conventional watermarks. They are characterizing patterns, of varying visibility, added to the presentation media as a guarantee of authenticity, quality, ownership, and source. A commonly encountered digital watermark is the logo most television channels add along the periphery of the television screen. Not only does it advertise the channel but also provides the legal benefit of having a source signature persist during video

The author is an undergraduate student at the Indian Institute of Technology, Kharagpur. This article was written during his summer training under V Rajaraman, SERC, IISc, Bangalore.

Box 1. Origin of Watermarks

Watermarking was first 'formalized' by the Italians in the 13th century. Their designs were simple twists of wire sewn into the screens of the mold. Watermarking in color was invented by Sir William George in 1818 and in 1845, William Henry Smith devised the light and shade watermarks.

recording. The same is required for digital data. A digital watermark may be added before distribution of digital data to authenticate data and enable detection of the source even after the data has been altered or modified.

Having understood what a watermark is, let us delve a little deeper. What are the parameters to be considered in choosing a watermark? A digital watermark is primarily added to prove the ownership. Hence it should be impossible to remove or separate the watermark from the source. But the watermark should not degrade the utility of the stock. In addition, the watermark should be resistant to tampering i.e. any sort of signal processing and even deliberate addition of noise. There also exists the possibility of data changing hands and being watermarked repeatedly. In such cases, it should be possible to retrieve each of the watermarks. But should a watermark be visible or not? That depends on the type of security required. Visible watermarks are like a ' DO NOT TRESPASS ' sign. They discourage theft and unauthorized use by diminishing the commercial value and establishing the ownership beyond doubt (*Figure 1*). Invisible watermarks only have this effect if the digital thief is aware of such technology and there is a high probability of the data being watermarked. Invisible watermarks are however tougher to detect and identify. A comparison of the effects of visible and invisible watermarks is given in *Table 1*.Other requirements are that the watermarks must be easy to generate and detect. They should not make unreasonable demands on the computing resources of

Table 1. Comparison of visible and invisible watermarks.

S No.	Purpose	Invisible Watermark	Visible Watermark
1	Validation of intended recipient	Primary	—
2	Non repudiable transmission	Primary	—
3	Theft Deterrence	Primary	Primary
4	Reducing commercial value but not utility	Primary	Secondary
5	Discouragement of unauthorized duplication	Primary	Secondary
6	Digital notarization and authentication	Secondary	Primary
7	Discouragement of analog duplication	Primary	—
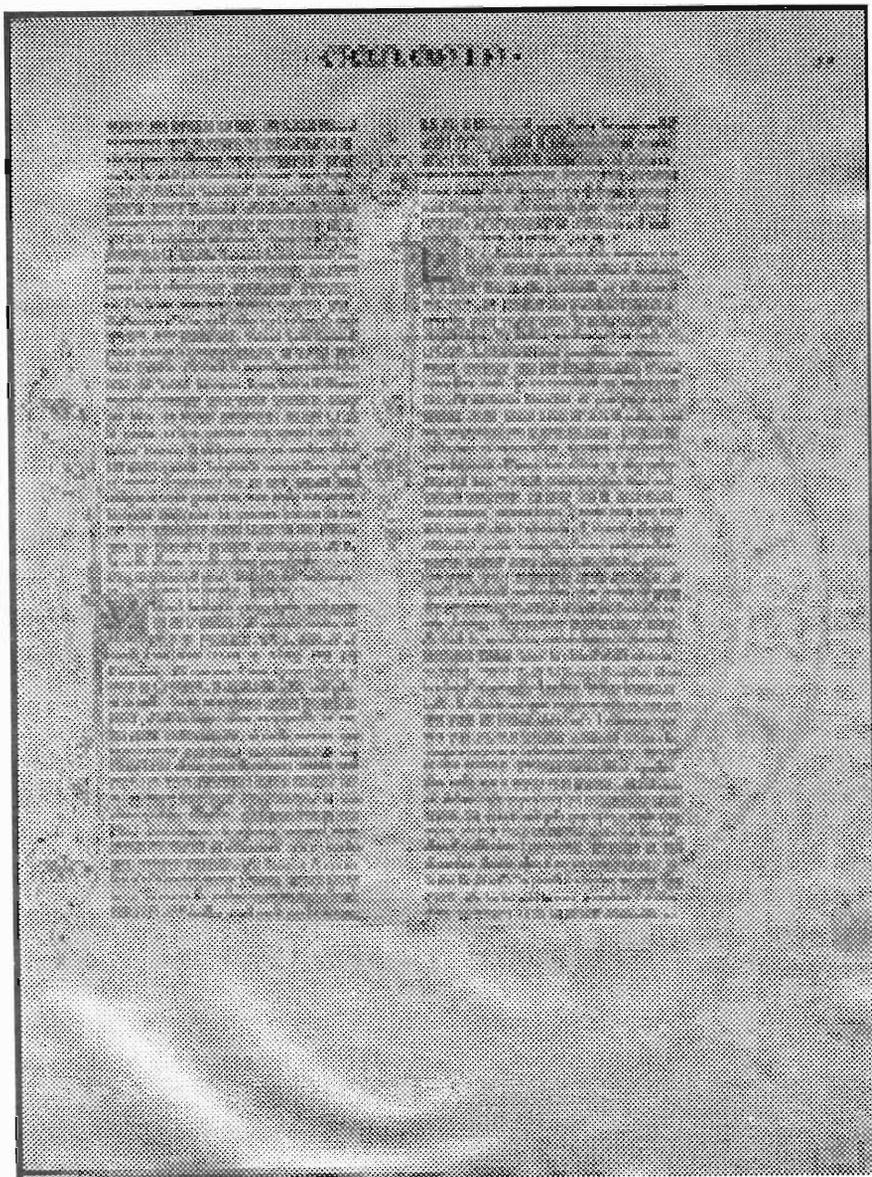
Figure 1. A visible watermark. (courtesy IBM)
(www.almaden.ibm.com/journal/rd/mintz/mintz6.gif).
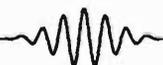
either the watermarker or the verifier. It is an advantage if a large number of watermarks can be generated as this opens up the possibility of watermarking each data separately.

Watermarking Techniques

Numerous methods for watermarking exist and they can be classified based on various parameters like the embedding algorithms and the detection algorithms used. We shall study them based on the data they watermark.

Watermarking for text: Three methods have been proposed for watermarking text, namely –

Word space coding : In this method, the spacing between words is varied by horizontally shifting the locations of the words within text lines, thus watermarking the document uniquely. This however is applicable only to documents in which variable spacing between adjacent words is possible. Also because inter-word spacing is often varied to format the document, the original document is necessary to verify the watermark. An example of word space coding is given below in *Figure 2a*.

Line shift coding: The same concept of word space coding is used, only it is applied in the vertical domain. Text lines are shifted vertically to watermark the image uniquely. If the original image has uniform line spacing, then verification of the watermark can be accomplished without the original. An example of line shift coding is shown if *Figure 2b*.

Feature coding: This method alters the specifications of particular characters by either lengthening or shortening them.
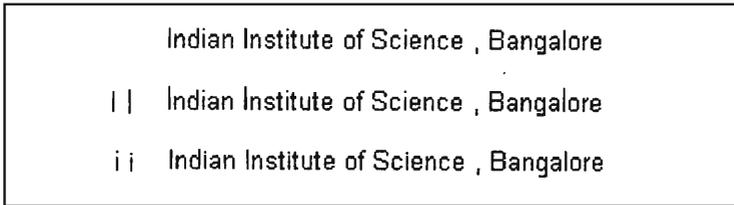
Figure 2a (left). This figure illustrates word shift encoding. Note the additional space of one pixel between 'n' of 'Indian' and 'I' of 'Institute'. Such minor variations are not perceptible to the human eye. They are recognized only on close comparison. Figure 2b (right). This illustrates the technique of line shift encoding (see lines 2 and 3). Notice that line shift encoding is more evident than word shift encoding because of the length of the lines.

	Supercomputer Education and Research Centre , IISc
	Supercomputer Education and Research Centre , IISc
Indian Institute of Science , Bangalore	Supercomputer Education and Research Centre , IISc
Indian Institute of Science , Bangalore	Supercomputer Education and Research Centre , IISc
	Supercomputer Education and Research Centre , IISc

Indian Institute of Science , Bangalore

I I   Indian Institute of Science , Bangalore

i i   Indian Institute of Science , Bangalore

It provides numerous possibilities of watermarking. However, for decoding, the original image is necessary, or rather, the original characteristics of the characters are required. An example is shown in *Figure 2c*.

The above three techniques each have their own advantages and disadvantages. Line shift coding is easily discernible but decoding it is easier. Word space coding will be less discernible as word space is often varied to support text justification. Feature coding is also largely indiscernible and has the advantage of being directly applicable to image files.

None of the above techniques is foolproof. A technically sophisticated attacker can easily detect and defeat the watermarking. Line shift coding can easily be identified by measuring the pixels between baselines and can be defeated by re-spacing the lines. A careful analysis might even lead to the method of watermarking which might be used to impersonate. Feature encoding can also be detected by measurement of character features and comparing it with the ones in the original. Making uniform, or adjusting the features to a maximum or minimum can defeat it. Word space coding is the toughest to detect as text is often justified. Only a pixel-by-pixel comparison with the original document can yield the watermark. It is also impossible to defeat the watermark by random spacing as that will produce a bizarre presentation. A combination of the above three will certainly produce a 'tough to beat' watermark. However watermarking techniques for text images are far from satisfactory. None of them are truly robust and they cannot withstand a serious attack made possible by powerful word processors. The easiest way to beat text watermarking is to retype the text again.

ii) *Watermarking for images:* Image data is binary in nature i.e.

Figure 2c. This figure illustrates the technique of feature encoding. In the second line the length of the letter 'I' has been imperceptibly increased; it is evident only on close comparison. In the third line the distance between the dot and the line in the character 'i' has been reduced. Such features are not noticeable until and unless specifically looked for.

The easiest way to beat text watermarking is to retype the text again.

One specific spatial watermarking technique uses color separation. On display devices a color image is made up of the basic additive colors R, G and B while in printing C, M, Y and K are the basic subtractive colors. The watermark is embedded in only one of the colors making it virtually impossible to detect while viewing. However on printing the watermark immediately appears, rendering the image useless.

all image files are a combination of zeros and ones. Thus they are easily manipulated, processed, and tampered with. Hence, robust and standard watermarks for image files are a challenge. Images, being digital in nature, can be visualized in two forms – either they can be thought of as a two-dimensional array of zeros and ones or they can be considered to be the digital representation of an analog signal. Watermarking techniques for images are based on these methods of representation.

Spatial Domain Watermarking: The image is considered to be a two-dimensional array and manipulating certain pixels based on their spatial locations in the array embeds the watermark. Techniques may be as simple as flipping the least significant bit (LSB) or may be a complex superposition of watermarking symbols over an area of the image. In the latter technique, a lot of flexibility exists in terms of placement, size, and intensity of the watermark (*Box 2*).

Frequency Domain Watermarking: The image is considered to be a sampled-digitized data of an analog signal. The analog signal can be obtained by various transforms like the DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform), FFT (Fast Fourier Transform) etc. and hence represented as a series of signals of increasing frequencies. The watermark can now be embedded in the coefficients of the various frequency components. The watermark is not embedded in the high frequency components, as they are usually lost on compression or scaling. Frequency domain watermarking disperses the watermark over the whole image thus rendering it less visible (or detectable) than spatial domain watermarking. However, it is more difficult to decode a watermark applied in the frequency domain.

Another novel method is to embed the watermark in the phase component of the DFT. It has been demonstrated quite conclusively that the phase is more important than the magnitude of the DFT values, so a watermark embedded in the phase will be robust to tampering as any noise deliberately introduced will
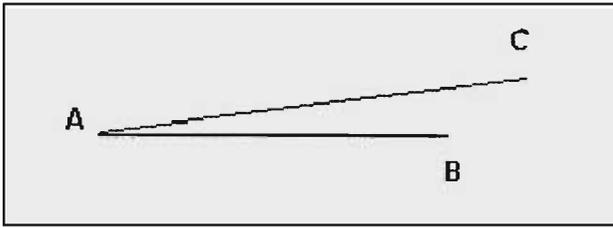
Figure 3. |AB| is the original vector. |AC| is the final vector after the addition of noise. Notice that the phase variation is quite small compared to the amplitude variation.

have to be sufficiently large to destroy the watermark thus damaging the image. It has also been shown that angle modulation possesses superior noise immunity when compared to amplitude modulation. Also, a phase-based watermark is robust to changes in image contrast. *Figure 3* illustrates the robustness of phase watermarking.

iii) Watermarking Audio Data: It is relatively tough to watermark audio data as the human ear can detect even the slightest change in tone or delay. Watermarks for audio data, in addition to the existing conditions, must not tend to accumulate in particular time intervals. If the signal energy is concentrated in a time interval, then it may happen that the watermark is not watermarked in that time interval. One method that has been proposed is to generate sequences with filters approximating the human auditory system's frequency masking characteristics. To prevent audible distortion, the watermark is weighed or attenuated in the time domain with the relative energies of the signal.

It has also been observed that the human auditory system is insensitive to phase distortion. Hence a variety of phase based watermarks can be explored. However, as of now watermarks for audio data are far away.

iv) Watermarking Video Data: Video clips on the computer are displayed at the rate of thirty frames per second. A movie of one and half-hours will thus have about sixteen lakh frames. The very magnitude rules out watermarking each frame. A constant standard watermark is preferred. In publicly broadcast video the watermark is the corporate logo whose constant presence acts as a watermark and advertises the channel. In private screenings, the same is possible. Invisible watermarks for video

It is relatively tough to watermark audio data as the human ear can detect even the slightest change in tone or delay.

Suggested Reading

[1] Jian Zhao. Look, it's not there. *Byte.* 22, No 1, Jan, 7–12,1997

[2] Hal BergheL Watermarking Cyberspace. *Communications of the ACM.* 40/11, Nov 1997

[3] The DICE company homepage (HYPERLINK http://www.digital-watermark.com www.digital-watermark.com)

[4] Digital Intellectual Property Protecting Everyone's Interests. Henry M. Gladney IBM Almaden Research Center.
(HYPERLINK http://www.software.ibm.com/is/dig-lib/fdlrpm.htm, http://www.software.ibm.com/is/dig-lib/fdlrpm.htm)

[5] Alessandro Piva's watermarking pages. (HYPERLINK http://cosimo.die.unifi.it/~piva/watermarking/watermark.hml http://cosimo.die.unifi.it/~piva/watermarking/watermark.hml)

[6] *The IEEE International Conference on Image Processing.* 3, 211-250,1996

data face the same problems as for audio data and tend to be more complex and demanding. Considering the fact that the volume of data dealt with is enormous and that the data is usually compressed, watermarking video data is a daunting task.

We have examined various watermarking techniques for a wide range of data. Watermarking ASCII (American Standard Code for Information Interchange) representations of text is nearly impossible, as modifying even the LSB will alter the meaning or the basic utility of the data. Text needs to be represented either as a bitmap or as a formatted document in order to be able to watermark it.

Detection of Watermarks

It needs to be emphasized that a watermark can be defeated in two ways – one, by removing the watermark from the original data and two, by proving it to be unreliable i.e. identifying a watermark when there is none. If the latter can be achieved then the watermark cannot be proved in a legal battle. Hence detection of watermarks needs to be even more reliable than their embedding. Detection algorithms are dependent on or are derived from embedding algorithms. Hence, a rigorous and detailed classification is ruled out. A broad generalization follows.

Detection algorithms can be divided into two broad categories – those which need the original unwatermarked data, and those which do not. The former generally makes a byte-by-byte comparison and arrives at a decision after allowing for a reasonable amount of error. Say, for example, the image has been watermarked by increasing the intensity of certain pixels in the original unwatermarked image by a known factor K, the average intensity of these pixels in the original image and the test image are compared. If they differ by more than 0.7K, the image is watermarked while if they differ by less than 0.3K, the image is not watermarked. The inbetween range of 0.3K to 0.7K is a gray area and needs a more detailed analysis of the conditions

---

Box 3. Cryptography

Cryptography involves modifying the data such that any third party that intercepts the data cannot use it. Cryptographical techniques can be either symmetric (where the encrypting and decrypting keys are the same) or asymmetric (where the keys are different).

---

undergone by the image. It should be said that the figures of 0.3K and 0.7K are an offhand estimate. They need to be arrived at after mathematical estimations.

The second category of algorithms inherently checks the image for a particular characteristic – say an embedded pattern or that the coefficients of its DCT confirm to a predetermined pattern. Most detection algorithms have their root in statistics. This is because of the large volume of data dealt with. A lot is deman-

---

Box 4. Digital Signatures

A Digital Signature is a string of bits produced by a hashing function acting on the data. It is appended to the data and serves to verify the authenticity of the data. The algorithms used to hash trace their roots to the asymmetric key systems of cryptography. An example of a digital signature is given in the figure.

```
--------BEGIN SIGNATURE------
IQB1AwUBMVSiA5QYCuMfgHYjAQFAKgL/ZkDfbeHEsbthba4Blrcnjaqbc KgHv+a5kr8
RCd+RHm75yYh5xxA1ojELwHhhb7cItrp2V7LlOnAelws4S87UX80cLBtBcH6AACf11qymC2hRb2j5SU+rmXWru+=QFMx
------END SIGNATURE------
```

---

ded from these algorithms. Apart from their accuracy, they should also be able to deal with simple spatial transformations like rotation, mirroring or scaling. It must be emphasized that watermarking is not a stand-alone technique. It can be used with other data security and authentication techniques like cryptography (*Box 3*) and digital signatures (*Box 4*) to provide a secure delivery system. Each method has its own advantages and disadvantages. Together however they form a formidable security system.

To summarize, digital watermarking enables authentication of data by embedding a pattern robust to signal processing and normal utility of the data. Watermarks have to be designed based on the data they will be applied to.

Address for Correspondence
H R Madhusudan
'Parijatha', Plot No 25/2,
Saraswathi Nagar, Lothkunta
Secunderabad –500 015