Information Hiding, Digital Watermarking and Steganography

Kuanchin Chen
Western Michigan University, USA

INTRODUCTION

Digital representation of data is becoming popular as technology improves our ways of information dissemination, sharing and presentation. Without careful planning, digitized resources could easily be misused, especially those distributed broadly over the Internet. Examples of such misuse include use without owner's permission and modification of a digitized resource to fake ownership. One way to prevent such behaviors is to employ some form of authentication mechanism, such as digital watermarks.

Digital watermarks refer to data embedded into a digital source (e.g., images, text, audio or video recording). They are similar to watermarks in printed materials, as a message inserted in the source typically becomes an integral part of the source. Apart from traditional watermarks in printed forms, digital watermarks may be: invisible, in forms other than graphics and digitally removed.

INFORMATION HIDING, STEGANOGRAPHY AND WATERMARKING

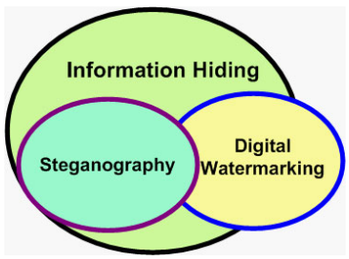
To many people, information hiding, steganography and watermarking refer to the same set of techniques to hide some form of data. This is true in part, because these terms are closely related and sometimes used interchangeably.

Information hiding is a general term that involves message embedding in some host media (Cox, Miller & Bloom, 2002). The purpose of information hiding is to make the information imperceptible or to keep the existence of the information secret. Steganography means "covered writing," a term derived from the Greek literature. Its purpose is to conceal the very existence of a message. Digital watermarking, however, embeds information into the host documents, but the embedded information may be visible (e.g., a company logo) or invisible (in which case, it is similar to steganography.)

Steganography and digital watermarking differ in several ways. First, the watermarked messages are related to the host documents (Cox et al., 2002). An example is the ownership information inserted into an image. Second, watermarks do not always have to be hidden. See Taylor, Foster and Pelly (2003) for applications of visible watermarks. However, visible watermarks are typically not considered steganography by definition (Johnson & Jajodia, 1998). Third, watermarking requires additional "robustness" in its algorithms. Robustness refers to the ability of a watermarking algorithm to resist removal or manipulation attempts (Craver, Perrig & Petitcolas, 2000; Acken, 1998). This characteristic deters attackers by forcing them to spend an unreasonable amount of computation time and/or by inflicting an unreasonable amount of damage to the watermarked documents in the attempts of watermark extraction. Figure 1 shows that there are considerable overlaps in the meaning and even the application of the three terms. Many of the algorithms in use today are in fact shared among information hiding, steganography and digital watermarking. The difference relies largely on "the intent of use" (Johnson & Jajodia, 1998). Therefore, discussions in the rest of the paper on watermarking also apply to steganography and information hiding, unless specifically mentioned otherwise.

To be consistent with the existing literature, a few terms are used in the rest of this article. *Cover work* refers to the host document (text, image, multimedia or other media content) that will be used to embed another document. This other document to be embedded is not limited to only text messages. It can be another image or other media content. *Watermark* refers to this latter document that will be

Figure 1. Information hiding, steganography and digital watermarking



embedded in the cover work. The result of this embedding is called a *stego-object*.

CHARACTERISTICS OF EFFECTIVE WATERMARKING ALGORITHMS

Watermarking algorithms are not created equal. Some will not survive simple image processing operations, while others are robust enough to deter attackers from some forms of modifications. Effective and robust image watermarking algorithms should meet the following requirements:

- Modification tolerance. They must survive common document modifications and transformations (Berghel, 1997).
- Ease of authorized removal. They must be detectable and removable easily by authorized users (Berghel, 1997).
- Difficult unauthorized modifications. They also must be difficult enough to discourage unauthorized modifications.

In addition to the above requirements for image watermarking algorithms, Mintzer, Braudaway and Bell (1998) suggest the following for watermarking digital motion pictures:

- **Invisibility.** The presence of the watermark should not degrade the quality of motion pictures.
- **Unchanged compressibility.** The watermark should not affect the compressibility of the media content.
- **Low cost.** Watermark algorithms may be implemented in the hardware that only adds insignificant cost and complexity to the hardware manufacturers.

The main focus of these requirements concerns the capabilities of watermarking algorithms to survive various attacks or full/partial changes to the stego-object. However, the fundamental requirement for most algorithms is unobtrusiveness. Unless the goal of using an algorithm is to render the host medium unusable or partially unavailable, many algorithms will not produce something perceptibly different from the cover work. However, theoretically speaking, stego-objects are hardly the same as the cover work when something is embedded into the cover work.

When it comes to watermarking text documents, most of the above requirements apply. A text watermarking algorithm should not produce something that is easily detectable or render the resulting stego-object illegible. Different from many image or multimedia watermarking techniques, which produce imperceptible watermarks, text watermarking techniques typically render a visible difference if the cover work and stego-object are compared side by side.

DIGITAL WATERMARKS IN USE

Authentication of the host document is one important use of digital watermarks. In this scenario, a watermark is inserted into the cover work, resulting in a stego-object. Stripping off the watermark should yield the original cover work. Common uses of authentication watermarks include verification of object content (Mintzer, Braudaway & Bell, 1998) and copyright protection (Acken, 1998). The general concept of watermarking works in the following way.

$\boldsymbol{W} + \boldsymbol{M} = \boldsymbol{S}$, where $\boldsymbol{W}$ is the cover work, $\boldsymbol{M}$ is the watermark and $\boldsymbol{S}$ is the stego-object. The + operator embeds the watermark $\boldsymbol{M}$ into the cover work $\boldsymbol{W}$. (1.1)

The properties of watermarks used for authentication imply the following: