INTRODUCTION

The use of digital media such as pictures, movies, and music has increased in recent years because of advances in computer technology. However, users can easily generate and redistribute illegal copies of this digital content. Digital watermarks are used to protect copyright material from such illegal acts (Bender, 1996). Digital watermarking embeds information such as copyright information or user information in the original content by changing some of its data. When an illegal copy of such content is found, the content owner can extract the embedded watermarks to expose the unauthorized use of that content. Digital watermarks can be embedded in various types of media, including still or moving pictures, animation, and sound. In this chapter, we treat and discuss the digital watermarking of still pictures.

Unauthorized users try to destroy embedded watermarks to prevent discovery of their unauthorized use. Therefore, it is necessary to...
properly evaluate the robustness of watermarking technologies to prevent the unauthorized use of digital content that uses digital watermarking. Benchmark tools such as Stirmark (1998) and JEWELS (2001) have been developed for this purpose. These tools can determine which attacks have the potential to damage embedded digital watermarks.

However, these conventional tools are difficult to use because they have command line interfaces and do not have image viewers. Therefore, users need to memorize attack commands and use another viewer to check the results. Furthermore, the implemented functions for evaluating robustness are inadequate because they only involve attacks based on a single image. Because of this limitation, most current digital watermarking technologies aim to be robust against single-image attacks. However, attacks that use multiple images are very powerful compared to those that use a single image, and they can be performed quite easily. In addition, these attacks do not degrade images. Therefore, the evaluation of robustness against such attacks is very important and has a practical use in benchmark tools for digital watermarking. We have developed a new benchmark tool that overcomes these limitations. Our tool has attacking functions involving both single and multiple images, and it can easily perform a combination of two or more attacks. In addition, the tool is easy to use because it has a Graphical User Interface (GUI).

In this chapter, we describe attacks on digital watermarking and existing benchmark tools, and we present the features of our new benchmark tool. We discuss its mounting interface and the functions that it implements, and we provide some benchmarking examples.

ATTACKS ON DIGITAL WATERMARKING

Attacks on digital watermarking involve image processing that transforms watermarked information and prevents it from being read. We classify these attacks into two groups.

Single-Image Attacks

A single-image attack is applied to a single image containing a digital watermark. Single-image attacks can employ image-processing operations such as noise addition, JPEG compression, trimming, and scaling. In general, because these operations are frequently performed on images, digital watermarking needs to be robust against these attacks. Some attacks are mounted in many existing image-editing tools, and these are considered to be innocent attacks.

However, malicious attacks intentionally change images to make it impossible to extract the watermark. For example, attacks that create small geometrical distortions in images are well known (Petitcolas, 1998). These attacks warp an image by multiple applications of minute, local rotations, and scaling. In addition, the possibility of Frequency Mode Laplacian Removal (FMLR) attacks has been discovered (Barnett, 1998). These attacks remove watermarks by using Laplacian convolution masks. In general, these single-image attacks degrade image quality.

Multiple-Image Attacks

A multiple-image attack involves two or more images. For example, consider the case where a content owner sends an image to two users. The content owner embeds different watermarks for users to identify. If the users collude and compare their images, the portion where the watermarks differ will be apparent and they can change the
Related Content

Web Accessibility for Users with Disabilities: A Multi-faceted Ethical Analysis
www.igi-global.com/chapter/web-accessibility-users-disabilities/23278?camid=4v1a

Analyzing Research Activity Duration and Uncertainty in Business Doctorate Degrees
www.igi-global.com/article/analyzing-research-activity-duration-uncertainty/65730?camid=4v1a

Assessing the Relationship between Awareness and Uptake of Insurance Products in Kenya
www.igi-global.com/article/assessing-the-relationship-between-awareness-and-uptake-of-insurance-products-in-kenya/152161?camid=4v1a

Reducing Risk through Segmentation, Permutations, Time and Space Exposure, Inverse States, and Separation
www.igi-global.com/article/reducing-risk-through-segmentation-permutations-time-and-space-exposure-inverse-states-and-separation/133544?camid=4v1a