Chapter 8
Using Watermarking Techniques to Prove Rightful Ownership of Web Images

Abdallah Al-Tahan Al-Nu'aimi
Isra University, Jordan

ABSTRACT

This article introduces intelligent watermarking scheme to protect Web images from attackers who try to counterfeit the copyright to damage the rightful ownership. Using secret signs and logos that are embedded within the digital images, the technique can investigate technically the ownership claim. Also, the nature of each individual image is taken into consideration which gives more reliable results. The colour channel used was chosen depending on the value of its standard deviation to compromise between robustness and invisibility of the watermarks. Several types of test images, logos, attacks and evaluation metrics were used to examine the performance of the techniques used. Subjective and objective tests were used to check visually and mathematically the solidity and weakness of the used scheme.

INTRODUCTION

Digital technologies changed all the perceptual video and audio transmission systems and the world became digital. With the incredible progress in digital transmission systems and the huge amount of information includes data, images, audio and video throughout the world, the need for protection of this multimedia efforts becomes very important (Hartung & Girod, 1997; Lu & Liao, 2001). Among all others types of digital signals, images play an important role in this digital world. The images have a greater impact on human beings than words and sound. So, there is more concentration on protecting images from illegal copying, manipulation and distribution in the last years.

The World Wide Web contains millions of different kinds of digital images. Some of them are freely downloadable and the others are not. Taken into consideration the rightful ownership to access some of them, the others are not. In contrast to analogue images, digital images can be easily copied, manipulated, stored and distributed which lead to a big challenge regarding the protection of copyrights.

DOI: 10.4018/978-1-4666-2157-2.ch008

Many papers tackled the problem of proving the real owner of digital images (Gulstad & Bruvold, 2003; Chen, Horng, & Wang, 2003). Among other technologies, watermarking comes into view as a powerful technology that share in solving this big challenge. Different watermarking algorithms were submitted to literature some of them can be seen in Hyvarinen (1999) and Cox, Kilian, Leighton, and Shamoon (1997).

Watermarking is an intelligent digital technology for embedding certain secret information in multimedia products to preserve the copyright and authentication, and to overcome the problem of theft and tampering (Fu & Au, 2002; Anderson & Petitcolas, 1998). For images, watermarking depends on embedding certain stream of bits or small images within the pixels of the original images to prove who the real owner is (Mohammad, Alhaj, & Shaltaf, 2008). On the contrary to cryptography, which restricts access to the information from the beginning to prevent illegal usage, watermarking gives the evidence of illegal attacking after it has happened. So, the real owner has the ability to prove technically that he is the real owner for that work. The watermarking approach of verifying the identity of the real owner is similar to the crimes investigation approach that is done by law enforcement authorities after the occurrence of unlawful events. The understanding of indictment evidence and conviction serves as a deterrent of the future crimes. Thus, watermarking technology depends on how these cases are prosecuted in copyright protection authorities, besides its dependence on technological factors.

The main idea of watermarking for digital images is putting some secret information that is related to the real owner in his image so he can extract this information later to prove his ownership. This may be done via using the direct spatial domain or the indirect transform domain. Putting the secret information in the spatial domain of certain image means that the numerical values of the image pixels will be directly changed corresponding to the amount and nature of the added secret information. In the other hand, using certain transform domain to change the image to a new case and host the secret information in the resulted coefficients of the new version of the image may give some additional benefits. There are several types of different transforms that are used in literature for such uses. Some of them are Discrete Fourier Transform (Solachidis & Pitas, 2001, 2004), Discrete Cosine Transform (Huang & Guan, 2004) and Discrete Wavelet Transform (Feng & Yang, 2005; Kunder & Hatzinakos, 2004).

From point of view of the human visual perceptual, the digital image watermark may be divided into: visible and invisible. Visible watermarks have a low number of applications, while invisible watermarks have more applications and represent the desired case. The visible watermark can be seen by the human visual system (Chen, Horng, & Wang, 2003), and the human eye sees the watermark within the background of the image like what is found in the backgrounds of television broadcasting stations and what is used in some applied programs like Microsoft Word at the background of its pages to prove originality and authenticity. The most obvious disadvantage of visible watermarks is that they can be filtered, changed and removed. So, the visible watermarks are categorized within fragile watermarks that cannot withstand against the attacks. Invisible watermarks are embedded in the host image and the human eye cannot see them. Thus, the existence of it cannot be determined unless some advanced operations are carried out using professional algorithms (Joseph, Ruanaidh, & Pun, 1998; Lu, Liao, & Kutter, 2002). On the other hand, visible watermarks can be categorized into: fragile which may filtered, changed and removed easily; robust which can withstands against intentional and unintentional attacks (Ganic & Eskicioglu, 2005); and semi fragile which represent intermediate case. Every type of these techniques of different robustness is used in several types of applications. These applications contain, but are not limited to, the following applications: