Преглед НЦД 5 (2004), 59–62

Vesna Vučković
(Matematički fakultet, Beograd)

DIGITAL WATERMARK

Abstract. Digital watermark is a pattern of bits inserted into an image, audio or video file, which contains information related to this file. The purpose of digital watermark is to provide copyright protection for intellectual property that is in digital format.

Invisible digital watermark attracts greater attention than visible. It is not a simple task to make a good watermark. It must be imperceptible for the human observer; on the other hand, it must be robust against usual operations (change of brightness and contrast, cropping, rotation, lossy compression...) and against malicious attacks.

Keywords. digital watermark, robustness, fidelity, security, fragile watermark, copyright protection, steganography, digital signature

What is digital watermark?

Digital watermarking is the practice of hiding the message about the image, audio or video clip, or another digital work, in this work. **Digital watermark** is the bit pattern which contains this message. The message usually includes copyright data; the basic purpose of digital watermarking is **copyright protection**.

History

The term **digital watermark** originates from the watermark on paper. First watermarks appeared in Italy, at the end of 13th century. Term **watermark** is coined at 18th century, in the time it appeared on banknotes and important documents with the aim to protect them against forgery. Term digital watermark appeared at early 1990s.

Causes of appearance of digital watermark

The main causes of appearance of digital watermark are the invention of **digital copies** and fast development of **Internet**.

As long as the music and movies were kept on analog tapes, there was not too big danger for copyright. Analog copies were always of poor quality comparing with original. With appearance of digital copies, which are of the same quality as originals, piracy becomes really dangerous.

Internet, which is rapidly developing, becomes the excellent medium for trade. But, security against piracy is minimal. It becomes very important to make something to protect owners of digital works.

Encryption of data before sending

For security against the theft of digital works on Internet, one solution is encryption of files before sending. The customer gets from salesman the decryption key. The data travel encrypted. After arriving of the data, the customer decrypts them. This solution has the drawback: there aren't any guaranties what the customer will do with the work after decryption - if he will, for example, resale it.

Where to write in the copyright data

It's important that copyright information is stored permanently somewhere in the work. One solution is to store it in file's header. This solution is not good - saving this work in the other format, copyright information will be lost.

For permanently saving copyright information, it must be written together with file's data. For example, we can write information about the owner of the image, inside the very image, changing some pixels. That is **watermarking**.

Visible and invisible digital watermark

Embedding of watermark (changing the pixels of image) may be:

- (intentionally) noticeable - **visible** watermark
- imperceptible - **invisible** watermark

The invisible watermark is much bigger challenge for scientists than visible.

Requests for good watermark

The good watermark must fulfill several fairly opposite requests:

- **Fidelity**: Changes of image (or other digital work) must be imperceptible for casual observer
- **Robustness**: Watermark must withstand habitual operations (if the work is image: changing of brightness and contrast, rotation, scaling, cropping, lossy compression; in the case of audio or video: changing of sound magnitude, changing of number of frames per second...)
- **Security**: The watermark must withstand hostile attacks; it may be removed from the work only if distortions are so strong that the work is out of commercial interest.

Embedding and detection techniques

There exist many different embedding and detection techniques. Basic classification is on informed and blind techniques.

Embedding is **blind** if it doesn't take into account work's characteristics.

Informed embedding previously analyses work; results of such embedding are better.

Detection is **informed** if detector with watermarked work also uses original work (without watermark). In this case the watermark is given by subtraction original from watermarked work. That is usually neither good, nor possible choice.
Blind detector doesn't use original work in watermark detection.

Embedding of other contents

In digital work, besides the data about it, may be embedded the other content. Steganography investigates techniques of secret messages hiding. Although watermarking and steganography share same ideas (putting one content into another), there is a great difference in realization. In transmission of secret messages, the secrecy is the most important requirement. Adversary may not be aware of pure existence of the message in the work. Here, it is the most important that fidelity stays untouched. Sometimes, the robustness is even undesirable characteristic. Instead of being robust, usually secret messages are fragile, and disappear at the least changes of file. That is the reason why the techniques of the embedding are very different. In steganography, common technique is embedding in the least significant bits. In watermarking, in order to improve robustness, embedding technique is considerable different; for example, often the watermark is embedded in frequency domain.

There exists also **steganographic watermarking** - embedding of secret messages about the contents of the work. For example, it is very simple to change the content of photography in Photoshop: removing somebody from the photo, changing license plate on the car... Therefore, there exists real danger of changes in very important photography which should be used as a proof in the court.
If we wish to prevent the forgery, we may embed in photo the digital signature, which will not be correct if the adversary changes some detail on the photo. Digital signature is often embedded in the least significant bits, on the basis of contents of most significant bits.

Some watermarking applications

Today, there exist a lot of applications of the digital watermarking:

- **Broadcast monitoring:** Watermark may be embedded in the advertising spot, or in the movie; it is easier to monitor one pattern, than the whole movie. In that way, advertisers know if it is broadcasted the whole time of advertisement that is paid. The movie's copyright owners know if a pirate TV station broadcasts their movie.
- **Copy control**: U.S. legislation allows that TV spectators record TV broadcast for later viewing. However, copy of that copy is not allowed. In the broadcast it may be embedded fragile watermark that means "copy allowed"; video recorder would erase that watermark, and the copy will not contain that watermark.
- **Informing conscientious users about copyrights**: Digimarc embedded his watermark detector in Adobe Photoshop. In this way, everyone may inform himself who is the owner of the work (provided that the owner was embedding the Digimarc's watermark in the work).
- **Content authentication:** The possibility of the digital works authentication is very important. This is true for all kinds of digital works, for photographs and

video clips of surveillance camera, as well as for important scanned documents. It is not very difficult to forge the digital document, for example, to remove somebody from photo or to change a part of text or the date in scanned text document. With embedding of digital signature, it would be easy to obtain the proof of authenticity of digital works. The digital signature is actually encrypted resume of the work. If someone attempts to make any change in the work, digital signature will not match with the work hence the change of the work will be detected.

- **Watermark as a proof of ownership in the court:** This is one of the most attractive applications of digital watermarking. Digital watermarking possesses the possibility of uniquely denoting each person of the world, just as well as fingerprints, blood samples or iris recognition can. However, there still exists the possibility of forgery, where someone embeds another watermark in the presence of the original. If such forgery happens, the court would not be able to recognize which watermark is the original, and which is the fake. The solution for that problem may be that we embed besides the watermark, digital signature of that work.

Bibliography

[1] Ingemar Cox, Matthew Miller, Jeffrey Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2001

[2] *Digital Watermarking World*, http://www.watermarkingworld.org/

[3] Stefan Katzenbeisser, Fabien A. P. Petitcolas (Editors): *Information hiding techniques for steganography and digital watermarking*; Artech House Books, 1999

[4] *Webopedia*, http://webopedia.com/