Digital watermarking: Tool for Image Authenticity

*Yashu Pradhan

Introduction

Image watermarking is the process of embedding an image with a secondary parameter intended for authenticity of ownership, without loss in quality of the image and to make legal assertion based on parameter, which can be detected or extracted later. This parameter is termed as watermark. Retrieval of the watermark unambiguously identifies the owner. Furthermore, the accuracy of owner identification degrades piracy gracefully in the face of attack.

In general, any watermarking scheme consists of the following three parts: The watermark signal,

(1) Watermark embedder, that embeds the watermark into the media

(2) Watermark detector that verifies the presence of watermark

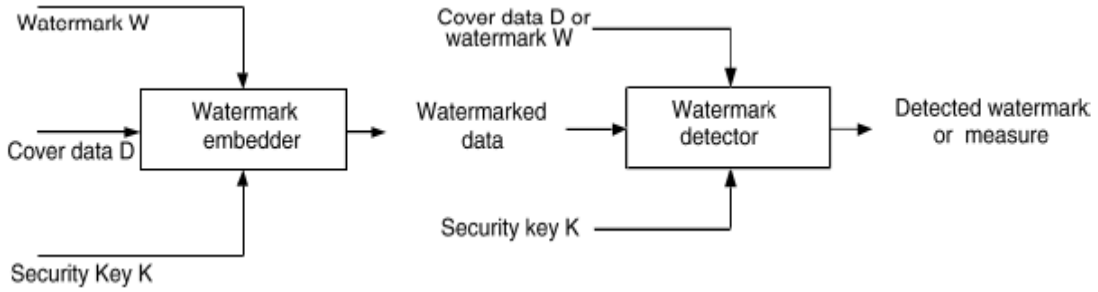
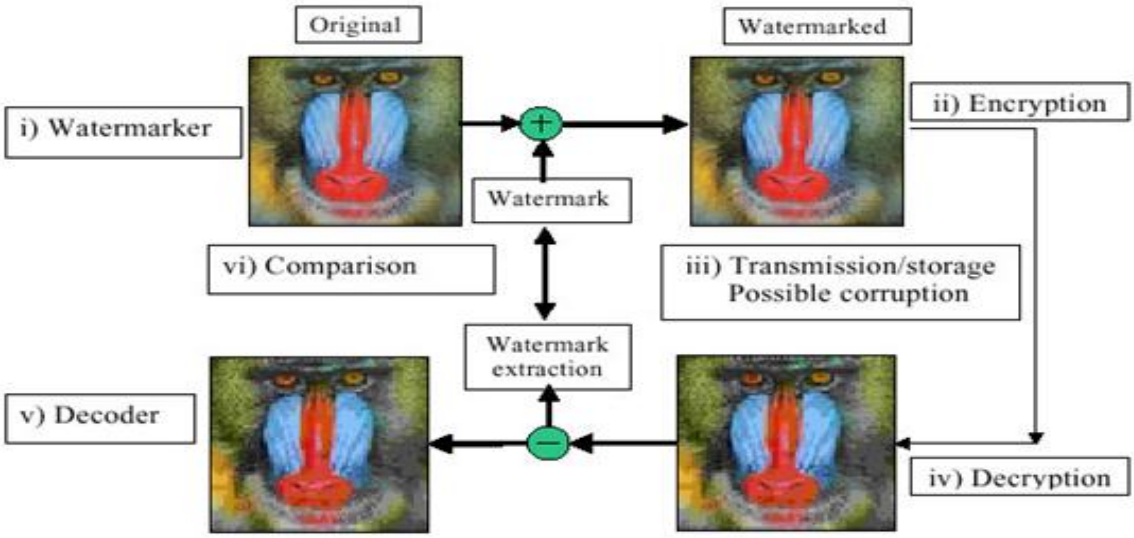


Figure (a): A typical watermarking system

Above Figure (a) is a conventional watermarking system consists of watermark embedder and watermark detector. The inputs to the watermark embedder are the watermark, the cover media data and the embedding security key. The 'key' is used to enhance the security of the whole system. The watermark can be a

number sequence, a binary bit sequence or may be an image. The output of the watermark embedder is the watermarked data.

An example is illustrated below



Robustness of Digital Watermarking

In order to be robust the watermark should be resistant to any alteration in its property during either normal use (unintentional attack), or a desired attempt to deform or remove the watermark present (intentional, or malicious attack). During normal use e.g. cropping, contrast enhancement, resizing…etc the watermark must be resistant enough to withstand the change.

A digital image watermark is a complete package of robustness, security, imperceptibility, complexity, and verification. "Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, color correction, or geometric modifications". It means the embedded watermark cannot be removed beyond reliable detection by targeted attacks. Imperceptibility means the watermark cannot be sensed by the human

visual system. Complexity is described as the effort and time required for watermark embedding and retrieval.

Threats on watermark

In this field threats may come in many forms and it may impair detection of the watermark or the information conveyed by the watermark. In most watermarking applications, the marked data is likely to be processed in some way before it reaches the watermark receiver. The processing could be lossy compression, lossyless compression, signal enhancement etc. However these threats may result due to various attacks which can be broadly classified as Intentional Attacks and Non-Intentional Attacks.

Existing watermarking attacks

The wide class of existing attacks contains four classes of Attacks:

- Removal Attacks
- Geometric Attacks
- Cryptographic Attacks
- Protocol Attacks.
- Estimation based Attacks.

Watermark Removal Attacks

The main objective of this type is complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm (e.g., without the key used for watermark embedding). The data lost due to this type cannot be recovered. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly.

Geometric Attacks

Geometric attacks do not actually remove the embedded watermark, but try to disturb the watermark detector synchronization with the embedded

information. However, if desired, the detector could recover the embedded watermark information when perfect synchronization is regained but the process might be too great to be practical. With the use of special synchronization techniques watermark could survive these attacks. However, an attacker with proper knowledge of the synchronization scheme can design dedicated attacks that can be vulnerable for the embedded watermark.

Cryptographic Attacks

This kind attacks the watermark by finding a way to remove the embedded watermark information by cracking the security methods in watermarking schemes. For accessing the embedded secret information brute force attack is quite perfect. Another attack is the so-called Oracle attack, which creates a non-watermarked signal in case a watermark detector device is found available. However their application is overpowered due to high complexity involved in their computation.

Protocol Attacks

It threats the watermark by attacking the entire concept of the watermarking application. It is based on the concept of invertible watermarks by which the attacker claims to be the owner of the watermarked data. This directly affects the true ownership of the data and i.e. watermarks need to be noninvertible for copyright protection applications. Also the scope of extracting a watermark from a non-watermarked document aids protocol attack. However it can be solved by making the watermarks signal-dependent with one-way functions. Another technique is the copy attack which does not destroy the watermark rather copies it to target data. This attack is applicable only when a valid watermark can be copied without using watermarking algorithmic.

Estimation-Based Attacks

The concept of estimation-based attacks lies in the estimation of the embedded watermark, used with some prior knowledge of the signals' statistics. The estimation is free from any knowledge of the watermark key or embedding rule. However with it the attack will be more effective and for the completion of attack, the attacker must concentrates on different ways to exploit the obtained estimates to impair the embedded watermark. Depending on estimation, this type can classify estimation-based attacks as removal, protocol, or de-synchronization attacks.

Methods used to test Digital Watermark Robustness

Some methods that can be used to test whether a watermark can survive different changes to the image it is embedded in.

- Horizontal Flipping: The watermark should withstand horizontal flipping without losing quality otherwise watermark cannot be considered as a robust one.
- Rotation & Cropping: Rotation with cropping doesn't reduce image quality, but can make watermarks undetectable as rotation realigns horizontal features of an image, used to check for the presence of a watermark.

- JPEG Compression/Re-compression: JPEG is a widely used compression algorithms for images and any watermarking system should be resilient to some degree to compression or change of compression level e.g. from 71% to 70% in quality like the example at left.

ONLINE ISSN 2278-5264
Volume-I, Issue-II, October-2012

- Scaling: Uniform scaling increases/decreases an image by the same percentage rate in the horizontal and vertical directions. Non-uniform scaling like the example at left increases/decreases the image horizontally and vertically at different percentage rates. Digital watermarking methods are often resilient only to uniform scaling.

- Dithering: Dithering approximates colours not in the current palette by alternating two available similar colors from pixel to pixel. If done correctly this method can completely obliterate a watermark, however it can make an image appear to be "patchy" when the image is over-dithered (as in the elbow area of the image at left).

Prioritizing Attack Resistance

For making a watermark resistant to a large number of image transformation is a difficult task, it is very important to prioritize these transforms. A watermark should be most resistant to the most common attacks. However complete watermark security is an unachievable goal. Therefore it is more rational to work out for a high probability of recovery.

ONLINE ISSN 2278-5264
Volume-I, Issue-II, October-2012

References:

[1] Zheng, D., Liu, Y., Zhao, J., and El Saddik, A. "A survey of RST invariant image watermarking algorithms", ACM Computing Surveys, Volume 39, No. 2, Article 5, June 2007.

[2] Mohanty, Saraju P., "Watermarking of Digital Images", MSc Thesis, Indian Institue of Science, January 1999.

[3] Mohanty , Saraju P., "Digital Watermarking : A Tutorial Review", Dept of Comp Sc and Eng. Unversity of South Florida, Tampa, FL 33620, http://www.csee.usf.edu

[4] Cox, I., Millar, M., and Bloom, J. 2002. "Digital watermarking", Morgan-Kaufmann, San Francisco, CA, ISBN: 1-55860-714-5.

[5] Meerwald, Peter, "Digital Image Watermarking in the Wavelet Transform Domain", MSc thesis in University of Salzburg, 2001.

[6] Neil F. Johnson, Zoran Duric, Sushil Jajodia "A Role for Digital Watermarking in Electronic Commerce".

[7] Chaelynne M. Wolak, "Digital Watermarking".

[8] Cristian V.Serdean, Martian Tomlinson, Graham J.Wade and Adrian M. Ambroze, "Protecting intellectual rights: Digital watermarking in the wavelet domain"

*Research Scholar, CMJ University, Shillong, Email: yashupradhan@gmail.com