A report on *Watermarking*

Submitted to

Dr. Pranab Kumar Dhar

Asst. Professor, CSE, CUET

Submitted by

Emtiaj Hasan

ID – 1004050

L – 4, T - 2

Under the course of

Project & Thesis

CSE - 400

Watermarking

To hide a message or to limit the access there are mainly three process to do it.

1) Cryptography
2) Steganography
3) Watermarking

Watermarking is the process of hiding a message (related to signal) within the signal itself. The signal can be image, audio or may be video. The same thing can be done using steganography. But the main thing that differs them is that, in steganography, there is no relation with signal and message and it is used as cover to hide the existence. Whereas watermarking tries to hide the actual content of digital signal.

And cryptography is other thing that is different from others. The most important thing is that, watermarking can protect data even after it is decrypted.

To do watermarking, a watermark is inserted into signal. And a watermark is actually a pattern of bits (low energy signal).

Necessity of watermarking

The necessity of it, is lied into its definition. The other things is discussed below (The application area of watermarking)

Application area of watermarking

Copyright protection

When a person needs to protect his data from illigal use, then watermark should be imposed. Suppose Person A creates an image and watermarks to it. He sends it to Person B. If personn B tries to sell it to others, then person A extracts his watermark and proves his copyright.

Source tracking

Different recipients get differently watermarked content, so that no one can distribute to other. For example, watermark is embedded into each movie's DVD. If the movie is then leaked to the Internet, the movie producers could identify which recipient of the movie was the source of the leak.

Broadcast monitoring

Advertising agencies want to ensure that their commercials are properly aired. As they want this commercials to be displayed at exact time they wanted to. In this thing, watermark is applied. Information

that can identify individual video, embedded to video using watermarking, making broadcasting easier.

Indexing

Comments and markers or key information related to the data is inserted as watermark. This watermark information is used by a search engine for retrieving the required data quickly and without any ambiguity.

Metadata Tagging

Watermarks convey object specific information to user of the object. For example, it is used to attach patient identification data to medical images.

Life cycle phase of Digital Watermarking

1) Embedding
2) Attack
3) Detection

Inserting of watermark into signal is embedding. Then it is stored or passed to other person. If it is modified by other, then it is called attack. The detection is the extraction of watermark from message.

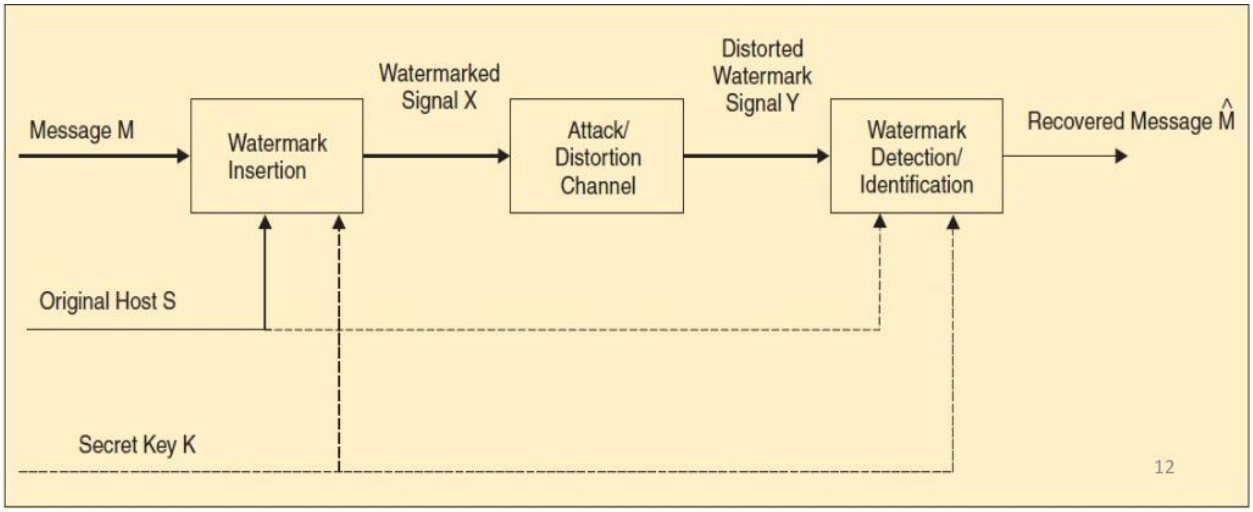

Figure: The steps of watermarking

Embedding watermark

The signal where the watermark is to be embedded is called the host signal. In embedding, an algorithm accepts the host and the data to be embedded and produces watermarked signal.

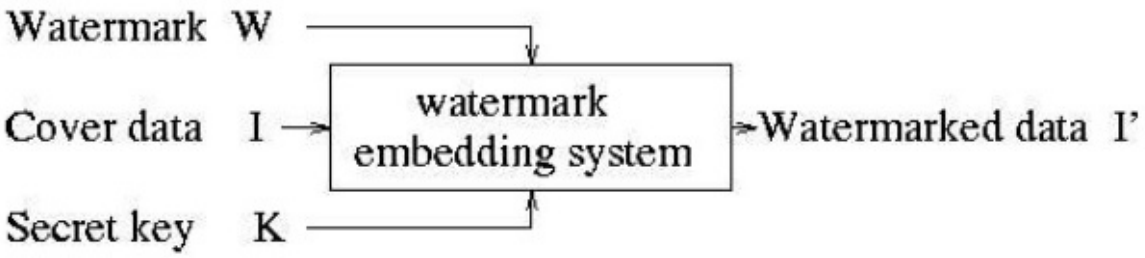

Figure: Embedding of watermark step

Inputs are watermark, cover data and secret key. The secret key is for security purpose. And output is watermarked data.

Detection of watermark

Detection is an algorithm that is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified, then the watermark still is present and it may be extract.

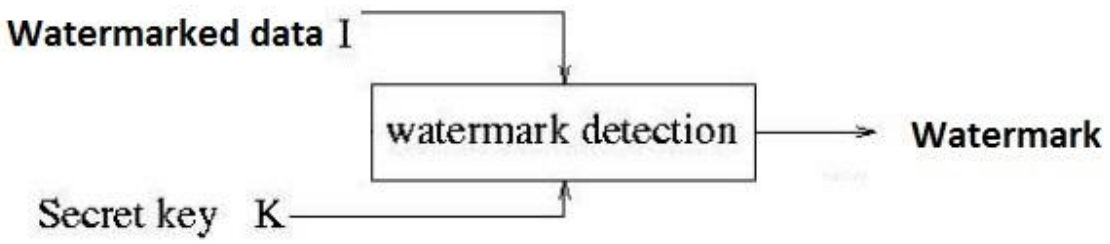

Figure: Detection of watermark

Inputs are watermarked data and secret key. And the output is recovered watermarked data.

Digital watermarking techniques may be **classified** in several ways, like

- Imperceptiblity
- Robustness
- Security
- Capacity

Imperceptibility

A digital watermark is called **imperceptible** if the original cover signal and the marked signal are perceptually indistinguishable. It is invisible to human eye. It remains hidden in content and can be detected only by authorized agencies.

And a digital watermark is called **perceptible** if its presence in the marked signal is noticeable. For example, watermark in video, DVD.

Robustness

A watermark is called **fragile** if detection falis with even minor modification. It is useful in tempering detection.

A watermark is called **robust** if detection is accurate under any modification. It is used in copyright control application.

Security

If the key that is used during watermarking is lost or the key is public, the watermark can be read and can be removed.

Capacity

The length of the embedded message determines two different main classes of digital watermarking schemes:

The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as **zero-bit** or presence watermarking schemes. Sometimes, this type of watermarking scheme is called **1-bit** watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

The message is an n-bit-long stream and is modulated in the watermark. These kinds of schemes usually are referred to as **multiple-bit** watermarking or non-zero-bit watermarking schemes.