Digital Watermarking as Content Protection Scheme

Petrus Santoso
Faculty of Technology Industry, Department of Electrical Engineering, Petra Christian University
e-mail: petrus@petra.ac.id

Abstract

Nowadays, as the Internet grows rapidly, the copyright laws are not effective anymore, since a lot of copyrighted products (picture, audio, video, document, etc.) are available as digital data. Any unauthorized parties able to produce identical copies of digital data without degrading the original contents and to distribute the copies over the network. This condition has led to a strong demand for reliable and secure distribution of digital data over networks. Such a technique developed to overcome this problem is digital watermarking. Digital watermarking is a process in digital domain, which embeds a watermark into a copyrighted digital data, to protect its value, so that it cannot be used by unauthorized parties.

This paper is intended to give an overview on digital watermarking. First, three application fields of watermarking are described and illustrated with some scenarios, namely watermarking for copyright protection, watermarking for copy protection, and watermarking for image authentication. Then watermarking techniques are discussed, starting from the basic watermarking procedure, followed by review of some watermarking techniques. And later, some attacks and obstacles to watermarking are highlighted.

In conclusion, digital watermarking technology plays important role in content protection issues. Attacks and obstacles are also had to be faced by this technology. The main obstacle is that there is no standard available for watermarking techniques. Without any specific standard, it is difficult to determine how robust a watermarking technique should be.

Keywords: Digital Watermarking, Content Protection, Watermarking Techniques.

1. Introduction

For many years, intellectual property rights have been protected by copyright laws with some restrictions on the distribution of the products and modification of the copyrighted contents. Nowadays, as the Internet grows rapidly, the copyright laws are not effective anymore, since a lot of copyrighted products (picture, audio, video, document, etc.) are available as digital data. The Internet and computer technology give chances for any unauthorized parties to produce identical copies of digital data without degrading the original contents and to distribute the copies over the network.

The condition described above has led to a strong demand for reliable and secure distribution of digital data over networks. This need has motivated significant research to find ways to protect the digital data against the illegal actions by attaching hidden copyright messages into the data. Some techniques have been developed for this purpose, one of them is digital watermarking.

Mintzer, Braudaway, and Bell [4] state that digital watermarking involves embedding data, often imperceptibly, into a media or multimedia object to enhance or protect its value. While Cox, Kilian, Leighton, and Shamoon [6] defines a digital watermark as a preferably invisible, identification code (information) that is permanently embedded in the data (multimedia data) and remains present within the data after any digital or analog process applied to the data unless the data has become useless. Digital watermarks are not always hidden; as some systems use visible watermarks.

According to some perspectives, watermarks can be classified into some types. From the visibility point of view, watermarks can be clustered into two types, namely: visible watermarks and invisible watermarks.

Visible watermarks are visual patterns like logos which are inserted into or overlaid on images (or video), very similar to visible paper watermarks [1]. An example of visible watermark is the watermark in the banknotes. Figure 1 shows part of a banknote with visible watermark.

Note: Discussion is expected before June, 1st 2004. The proper discussion will be published in “Jurnal Teknik Elektro” volume 4, number 2, September 2004.

Figure 1. Part of a Banknote With Visible Watermark

Invisible watermarks are designed to be beyond normal human's observation. Normal human's observation cannot distinguish between the original data and the watermarked data. It is designed to be imperceptible, to be undetectable by any unauthorized parties but detectable by the owner, helping the owner to claim if a copyright infringement happens.

Figure 2 and Figure 3 gives example of a picture before and after an invisible watermark is attached to it.

Figure 2 "Bavarian Couple" courtesy of Corel Stock Photo Library [6]

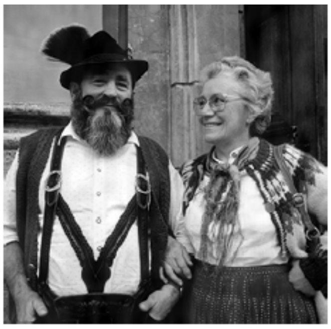

Figure 3 Watermarked version of "Bavarian Couple" [6]

Furthermore, invisible watermarks can be further clustered into three types, from its robustness point of view [2] [3]:

1. **Fragile watermarks:** Fragile watermarks are designed to be very sensitive, as they can be destroyed easily, even by the slightest modification to the data. But this watermark should survive unintentional attacks, i.e. modifications that are normally performed to prepare data before publication. This characteristic is meant to indicate whether any intentional modifications have been made to the data or not, or to identify the area of modification.
2. **Robust watermarks:** Robust watermarks are designed to be resilient to any attacks that can destroy or remove the watermarks. After the attacks, the watermarks will still exist as before.
3. **Semi-fragile watermarks:** Semi-fragile watermarks combine the characteristics of fragile and robust watermarks. This type of watermarks is resilient against attacks just like the robust watermarks, while it is also able to identify the altered area just like fragile watermarking. This type of watermarks is able to distinguish between any altered and unaltered area.

2. Fields of Application

This section introduces three fields of watermarking application, which are proposed by Kutter and Hartung [1], namely watermarking for copyright protection, watermarking for copy protection, and watermarking for image authorization. While Mintzer, Braudaway, and Yeung [5] proposes eight scenarios of watermarking application. Below we cluster the scenarios from [5] as examples of the application fields proposed in [1].

2.1 Watermarking For Copyright Protection

Most of the watermarking applications are for copyright protection, which is the main goal of watermarking. The purpose of this application is to attach information about the ownership of the data in order to prevent other people to misuse the data or to claim the copyright of the data. Besides, this kind of application can also be used to track the distribution of the data.

The users of this application can be organizations that own the copyrights to digital data (picture, audio, video, document, etc.), such as advertising company, recording company, libraries, news agency, etc. In order to achieve the objective for copyright protection, both visible and invisible watermarks can be used.

This type of application requires a very high level of robustness [1]. The watermark must remain and be detectable in the data. Some scenarios from [5] that can be clustered into this application field are:

- **Visible watermarking for enhanced copyright protection:** A visible watermark is attached to the data, which will be provided available on the Internet. By the help of the visible watermark, the owner of the data can force copyright from the commercial use, as the visible watermark obviously announces the ownership of the data.
- **Visible watermarking used to indicate ownership of originals:** Similar to the previous scenario, a visible watermark is attached to the data, which is provided available on the Internet. As the visible watermark obviously announces the ownership of the data, it may encourage some observers to patronize the owner of the data.
- **Invisible watermarking to detect misappropriated images:** An invisible watermark is attached to the data, which is an image in this scenario, before the image is distributed. The owner of the image is aware that someone may distribute the image for free. Then the owner might subsequently scan the Internet, to find out whether the watermarked image is available on the Internet.
- **Invisible watermarking as evidence of ownership:** An invisible watermark is attached to the data before sold. Then the owner of the data suspects that the data has been modified and published without giving any rewards to the owner. In this scenario, the invisible watermark can be used as a proof about the ownership.
- **Invisible watermarking to determine the identity of a misappropriator:** This scenario is similar with the previous one, an invisible watermark is used to investigate when the data has been modified and published without giving any rewards to the owner. But in this case, the watermark indicates the purchaser of the data, so that the owner of the data can identify which one of the purchasers has misused the data.

2.2 Watermarking For Copy Protection

Other application of watermarking is to prevent illegal copying of the digital media. The watermark is used to indicate the copy information of the data. One of the scenarios from [5] can be clustered into this application field, which is:

- **Invisible watermarking for a digital VCR:** An invisible watermark is attached to an MPEG-compressed video. Then the player looks for a “special watermark” to determine whether the video may be copied, or only played. Sometimes the video carries “no copy watermark”, which means that the video can only be played, and sometimes it carries a “copy once watermark”, which means that the video may be copied, but no further consecutive copies are allowed to be made from the copy.

2.3 Watermarking For Image Authentication

Another alternative of watermarking application is to determine whether an image has been modified or altered since some earlier time or not. This purpose can be achieved by using invisible watermarks of types fragile and semi-fragile watermarks (See Section 1).
This kind of application is useful for law, commerce, defense, and journalism. Two of the scenarios from [5] can be clustered into this application field, namely:

- **Invisible watermarking for a trustworthy camera:** This scenario can be used for journalism, to ensure the authenticity of a published scene. The scene is captured with a digital camera which automatically attaches an invisible watermark to the picture at the capture time. This way, the watermark indicates that the scene is not fake.
- **Invisible watermarking to detect alteration of images stored in a digital library:** An invisible watermark is attached to every image stored in a digital library. Later on, the watermark will be extracted and compared with the original attached watermark. If the extracted watermark matches the original one, then it is assumed that the image has not been altered, otherwise it is assumed that the image has been altered. This scenario is particularly useful for a digital library that is connected to the Internet.

3. Watermarking Techniques

3.1 Basic Watermarking Procedure

Generally, watermarking procedure can be divided into two processes: the watermark embedding process and the watermark recovery process.

1. **Watermark embedding process**

   This process embeds a watermark to the digital data. The watermark can be any number, text, or an image. Before being processed, the digital data may be involved in an initial process, such as compression.

   Figure 4 depicts the process scheme in embedding a watermark to a digital data. The inputs to this process are watermark, digital data, and key (optional); while the output is the watermarked version of the data. This process may involve a secret/public key mechanism. The purpose of using secret / public key mechanism is to raise the security level, i.e. to avoid the possibility that the watermark W may be replaced or manipulated by unauthorized parties.

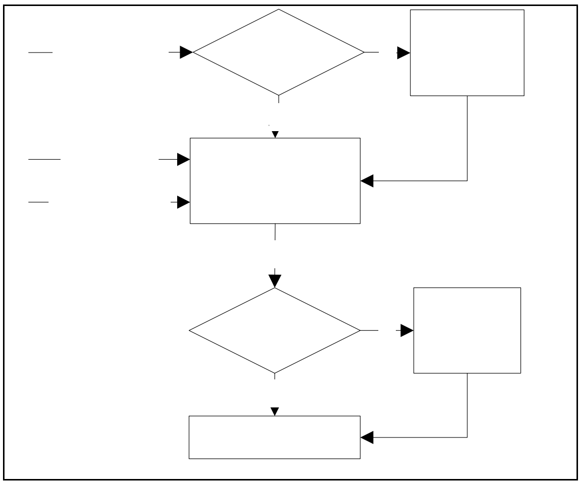

Figure 4 Generic watermark embedding process

   After the embedding process, before the watermarked digital data is distributed, it may be involved in additional process, such as encryption or compression.

2. **Watermark recovery process**

   This process detects and recovers (extracts) watermark from the data. Before being processed, the watermarked data may be involved in an initial process, such as decryption (if the watermarked data is encrypted).

   There are two ways to detect the watermark: coherent detection and blind detection. The coherent detection needs the original data in order to detect the watermark while the blind detection can detect the watermark without the original data.

   Figure 5 depicts the recovery process scheme of the watermark from watermarked data. The inputs to this process are (possibly altered) watermarked data, and key (optional, depends on the mechanism used in the watermark embedding process); while the output is the watermark and the original data, or a confidence measure whether the watermark is similar with the original watermark or not.

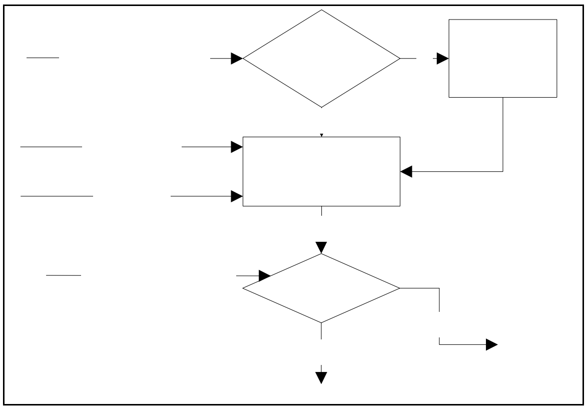

Figure 5 Generic watermark recovery process

3.2 Watermarking Techniques

There are many techniques developed to be involved in the watermarking procedure, in order to fulfill various requirements.

The most popular cluster of watermarking techniques is transform domain techniques. Transform domain techniques embed the watermark in a transform domain of the signal, e.g. in the frequency domain. This technique is believed to be the most robust way Johnson, N.F. and Katzenbeisser, S.C. [1] states that embedding information in the frequency domain of a signal can be much more robust than embedding rules in the time domain.

Another technique that is also widely applied is spread spectrum, which adopts ideas from spread spectrum scheme in the communication. This technique is strongly related to watermarking in frequency domain.

3.2.1 Discrete Cosine Transform (DCT)

At present, DCT is the most widely used technique in image compression and watermarking areas. In image compression, DCT is the core of the JPEG compression technology. In watermarking, this technique is used for copyright protection and image authentication.

3.2.1.1 DCT Technique's Characteristics

Applied to images, the DCT helps to separate the image into parts of differing significance, with respect to the image's visual quality.

$$S(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{x=0}^{N-1} s(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

Formula 1- Forward DCT Equation (FDCT) [1]

Formula 1 gives the Forward Discrete Cosine Transform (FDCT) equation, used in digital image processing, with an input image *s*, resulting the coefficients for the output image *S*.

The input image is N pixels wide by N pixels high; *s(x,y)* is the intensity of the pixel in row *x* and column *y*; *S(u, v)* is the DCT coefficient in row *u* and column *v* of the DCT matrix.

The input to the FDCT equation is an 8 by 8 array of integers. The value at each field of the array represents each pixel's grayscale level; 8 bit pixels have levels from 0 to 255. The output from the FDCT equation is also an 8 by 8 array of integers, which values can range from -1024 to 1023.

$$s(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)S(u,v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

Formula 2- Inverse DCT Equation (IDCT) [1]

Formula 2 gives the Inverse Discrete Cosine Transform equation. The input and output images are the inverse of the input and output images of the FDCT equation.

3.2.1.2 DCT in JPEG Compression

JPEG uses the DCT technique for compression. The JPEG standard divides the image data into 8x8 pixel blocks and transforms each block with DCT.

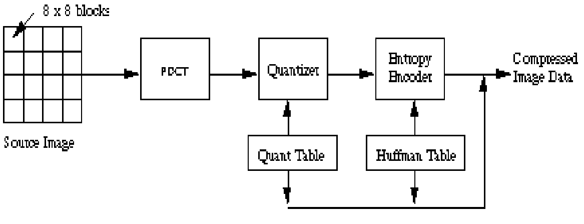

Figure 6 JPEG Encoder Block Diagram [12]

Figure 6 represents the JPEG encoder block diagram. The input to the process encoding process of JPEG is a source image, divided to 8 x 8 pixel blocks, and the output of this process is a compressed image data. From Figure 6, it can be seen that the encoding process of JPEG works as follows:

1. First, each of the 64 pixel blocks of source image data is transformed with FDCT.
2. Then, each DCT coefficient is quantized, divided by values from a user defined quantization table, and all the results are rounded to the closest integer.
3. The resulting values from the quantization step are then compressed using an entropy coder (e.g. Huffman coding).

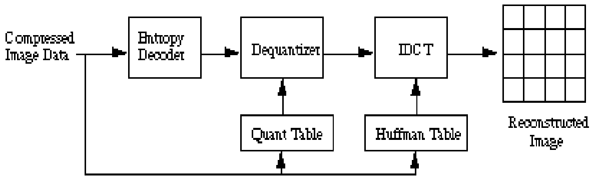

Figure 7 JPEG Decoder Block Diagram [12]

Figure 7 represents the JPEG decoder block diagram. The decoding process of JPEG is the inverse of the encoding process; the input to the process is the compressed image data and the output is a reconstructed image.

In the decoding process' dequantization step, each DCT coefficient is dequantized by multiplying the DCT coefficient with the corresponding value from the table used in the encoding process. Then the data is reconstructed by using inverse DCT.

3.2.1.3 Watermark Embedding with DCT

In the embedding process, a watermark should be placed in the perceptually significant area of the image. As most digital images experience lossy compression such as JPEG, which compresses an image by disregarding high frequency signal in the image, here we consider that the perceptually significant area of an image can be the low band or middle band in the DCT matrix.

Generally, in images, much of the signal energy lies at low frequencies, which appear on the upper left corner of the DCT matrix. The upper left corner area is called low band. The lower right corner of the DCT matrix values represents higher frequencies, which are often disregarded with little visible distortion. The remainder area between the upper left corner and lower right corner of the DCT matrix is called middle band, depicted in *Figure 8*.

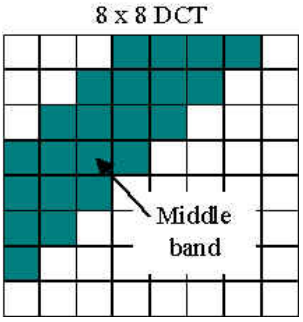

Figure 8 Definition of middle band frequency area in 8x8 DCT matrix [11]

The insertion process of watermark involving DCT can be seen in the Figure 9 below:

1. First the original image is transformed with FFT or DCT (FDCT), resulting a DCT transformed image.
2. Then the perceptually significant region is determined, and the watermark is inserted to the selected region.
3. After the watermark is inserted, then the watermarked DCT transformed image, together with the inserted watermark, is transformed by using the Inverse FFT or IDCT.
4. The watermarked image is produced.

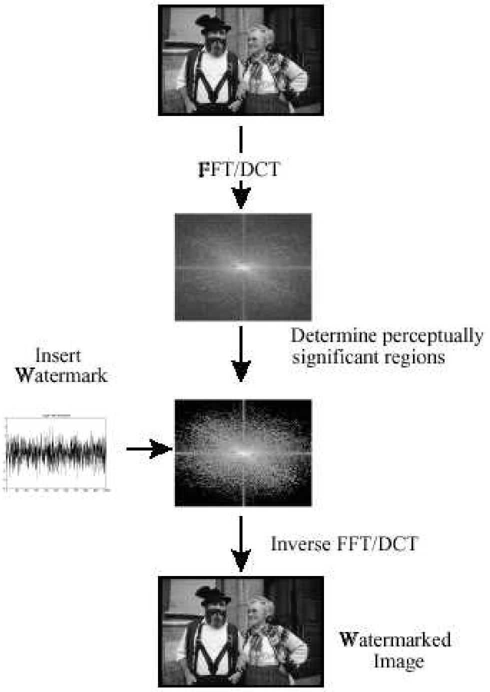

Figure 9. Stages of watermark insertion process [6]

3.2.1.4 Watermark Detection with DCT

DCT is also involved in the detection process of watermark, i.e. in evaluation of similarity of watermark. The usage of DCT in detecting watermark is intended to support the image authentication application.

The process of evaluating similarity of watermarks involving DCT can be seen in the Figure 10 below:

1. First the recovered image is transformed with FFT or DCT (FDCT), resulting a DCT transformed recovered image (let us call it image (a)). Concurrently, the original watermarked image is also transformed with FFT or DCT (FDCT), resulting a DCT transformed original watermarked image (let us call it image (b)).
2. Then image (b) is subtracted from image (a), resulting an extracted watermark.
3. Then the extracted watermark is compared with the original watermark, to evaluate its similarity

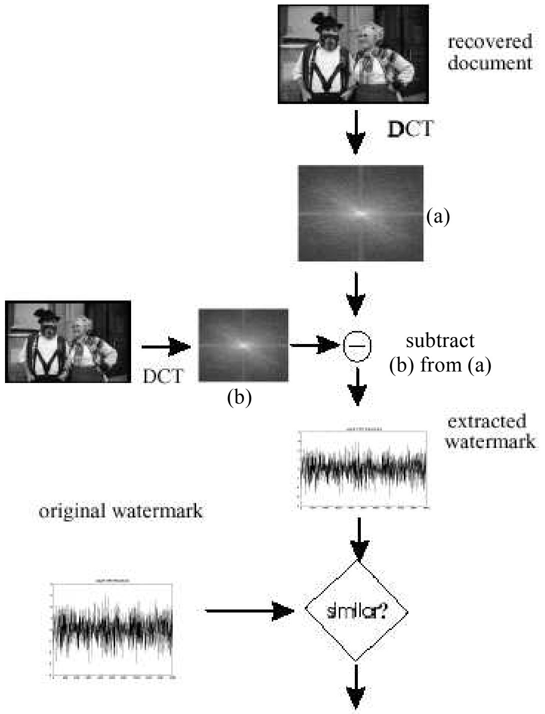

Figure 10. Evaluating the similarity of Watermark [6]

3.2.2 Spread Spectrum

The idea of spread spectrum watermarking techniques is adopted from the spread spectrum technique in communication. In the spread spectrum communication technique, a narrow band signal (the message to be transmitted) is modulated by a broadband carrier signal, which broadens (spreads) the original narrow band spectrum, such that the presence of any signal energy in any frequency is undetectable. This characteristic of spread spectrum technique is particularly well suited for the watermarking process.

3.2.2.1 The Role of Spread Spectrum in Watermarking

A watermark should be placed in the perceptually significant area of the image, due to the fact that most of digital images may experience lossy compression. However, placing the watermark in the perceptually significant area of the image does not fully guarantee that the watermark will be robust. This is due to the fact that lossy compression is not the only modification an image may experience. Most of images will also very likely experience some geometric modifications, such as cropping, scaling, and filtering. These modifications can affect the watermark. Moreover, common signal processing, such as analog-to-digital and digital-to-analog conversions can also cause a distortion to the watermark.

To overcome the problem discussed above, the spread spectrum watermarking is proposed. In the spread spectrum watermarking technique, the frequency domain of the image or sound is viewed as a communication channel and the watermark is viewed as a signal that is transmitted through the channel. Likewise, any modifications or distortions are treated as noise that the signal has to be resistant to.

Similar to the spread spectrum technique in communication, the watermark is spread over a lot of frequency blocks, throughout the spectrum of the image, so that the energy in each block is very small and certainly undetectable. This way, the watermark will be very likely undetectable since the location of the watermark is opaque.

The spread-spectrum-watermark is then embedded to the image, placed in the most perceptually significant region of the image. Embedding and recovery process of spread-spectrum-watermark may involve any transform domain techniques, such as FFT or DCT, as can be seen in Figure 9 and Figure 10.

3.2.2.2 Spread Spectrum Watermarking

In its most basic level of implementation, a watermark consists of a sequence X of real numbers, $X = (x_1, \ldots, x_n)$. In practice, each value x_i is chosen independently according to $N(0,1)$ distribution ($N(0,1)$ denotes a normal distribution $N(\mu , \sigma ^2)$ with mean μ and variance $\sigma ^2$) [6]. It can also be done with Gaussian distribution, which will more robust than normal distribution when n is large. The value of n determines the degree to which the watermark is spread over the spectrum of the data.

From each document D, a sequence V of real numbers, V = ($v_1, \ldots, v_n$) is extracted and the watermark X = ($x_1, \ldots, x_n$) is inserted, so that an adjusted sequence of values V’ = ($v'_1, \ldots v'_n$) is obtained. Then, V’ is inserted back into the document replacing V and resulting a watermarked document D’. The insertion process can be implemented using one of the natural formulae for computing V’, which are given in Formula 3.

$$v'_i = v_i + \alpha x_i \qquad (1)$$

$$v'_i = v_i (1 + \alpha x_i) \qquad (2)$$

$$v'_i = v_i (e^{\alpha x_i}) \qquad (3)$$

Formula 3 – Three natural formulae for computing V’ [6]

Here α is a real scaling parameter. The first equation (1) is always invertible, but it may not be appropriate when the v_i values vary wide. The others (2) and (3) are invertible if $v_i \neq 0$. These two equations are more robust against such differences in scale, they will give a similar result when αx_i is small.

4. Attacks and Obstacles to Digital Watermarking

4.1 Attacks

As the watermarking technology grows, there are some efforts trying to attack the watermarked data. The attacks try to remove or to destroy the watermark, or to hide the watermark beyond any detection.

Basically, the attacks to watermarks can be classified into two types: unintentional attacks and intentional attacks.

4.1.1 Unintentional attacks

There are some modifications that are normally performed on preparing images for publication. These modifications are considered as unintentional attacks as they are not intended to attack the copyright protection on the data. Some modifications that can be considered as unintentional attacks are:

- **Common signal processing:** It is very likely that digital data experience signal processing, such as digital-to-analog and analog-to-digital conversion. For example, image is converted from analog to digital by scanning and from digital to analog by printing. These conversions might affect the watermark as the image may become blurred, and correspondingly, the watermark may become distorted.
- **Resizing (scaling):** Normally, image resizing (scaling) does not affect the watermark in an image. But when the scale is too large, it may distort the watermark. For example, when an image is shrunk, it will lose some of its parts.
- **Rotation and flipping:** Rotation and flipping are meant to arrange the position of an image. One often does a small angle rotation or horizontal / vertical flipping on an image in preparation before publishing the image. Sometimes rotation or flipping may cause that the watermark in the image will be undetected.
- **Cropping:** Cropping is used when someone is only interested in a certain part, usually the most significant part, of the image. Thus, cropping cuts and takes only some part of the image. Therefore there is a possibility that cropping may remove or destroy the watermark.
- **Filtering:** Filtering is used for image restoration and improvement. Some examples of filtering are sharpening and highlighting edges or details in an image. Normally, this kind of modification will not affect the watermark in the image. But when the filtering level is too high, the watermark may be altered.
- **Contrast and brightness adjustment:** Contrast and brightness adjustment are used for color improvement of an image. Similar like filtering, normally, this kind of modification will not affect the watermark in the image, unless the adjustment level is too high.
- **Lossy compression:**Lossy compression is a compression method, applied to digital image or audio, which eliminates the redundant or perceptually insignificant part of the digital data. It is possible that watermark will be altered in the process.

4.1.2 Intentional attacks

Some attacks are done intentionally. The attacks try to remove, destroy, or replace the watermark, or try to hide the watermark beyond any detection. Below we discuss some common intentional attacks:

- **Blind modification:** This kind of intentional attack is similar with the unintentional attacks, but it is done intentionally. For example, the attacker tries to crop a part of the image and replace it with something else. Therefore it is important for a fragile or semi fragile watermark to identify the area of modification.
- **Noise:** The attacker tries to attack the watermark by adding a random value to each pixel in the image. The random values chosen must be small enough so that the attacks will not be obviously seen. The purpose of this attack is to make the watermark undetectable by the watermark detector. This kind of attack is weaker than the others. Before detecting the watermark, a pre-processing can be performed by the watermark detector, such as filtering. Then the watermark can be detected by the watermark detector.
- **Overmarking:** This attack tries to destroy the original watermark on a data and replace the original watermark with other watermark from other data, that will be accepted as a valid watermark by the watermark detector.
- **Iterative attack:** This attack is done iteratively, tries to destroy or remove the watermark little by little. The attacker makes some modifications several times, either on the whole data or on parts of the data, trying to find the weakness of the watermark. This attack can also be done by embedding watermark to the data several times.
- **Conspiracy attack:** Several people that have the same images with different watermarks, collect the images they have, and try to calculate the average value of every pixel in the picture. The calculation will result on a new similar image, with no watermark or distorted watermark.

- **Inversion attack:** Before doing this attack, the attacker first has to detect and determine the watermark. From the characteristics of the watermark, the attacker may know how the watermark was embedded to the data. Then the attacker can remove the watermark by processing the watermark with the inverse of the watermark embedding process.
- **Key attack:** An attacker may be interested in finding the key involved in the watermarking process. To do so, an exhaustive trial can be used, to guess the key. If the key is found, then the watermark can be manipulated.

4.2 Obstacles

As watermarking technology grows and is widely used, it has to face some obstacles. Some obstacles have been determined, such as:

- There is no specific standard defined for watermarking. Since different watermarking techniques involve different multimedia formats and different manufacturers, it is difficult to make the watermarking techniques to be interoperable each other. As an aggravation, the multimedia standards evolve rapidly.
- The development of watermarking techniques and products has to compete with the development of attacks. While the watermarking technology grows, attackers also try to develop new ways to attack watermark.
- The variety of watermark leads to difficulty in evaluating the performance of a watermarking system. It is difficult to determine the robustness level to which a watermarking system should survive, since the robustness level may depend on the user's requirement.
- Development of new watermarking technology has to be accompanied by development of watermark detector technology. Without being accompanied by development of watermark detector technology, a new technology watermark may be undetected. This should not happen, because once a watermark is undetected, it may be misused by unauthorized parties.

5. Conclusions

Digital watermarking is a process in digital domain, which embeds a watermark into a copyrighted digital data, to protect its value, so that it cannot be used by unauthorized parties. Digital watermarking technology has an important role in content protection issues as it strongly supports (or replaces) the functionality of copyright laws to protect intellectual property rights.

However, as this technology grows, attacks against this technology are also developed. There are various attacks trying to defeat watermarking technology. A watermarking technique or application has to be robust against these attacks in order to achieve its main goal: protecting the copyrighted content.

Some obstacles are also had to be faced by this technology; the main obstacle is that there is no standard available for watermarking techniques. Without any specific standard, it is difficult to determine how robust a watermarking technique should be.

However, digital watermarking is a relatively new area; there is still a lot of opportunity in developing standards and better development in the future.

References

[1] Katzenbeisser, S., and Petitcolas, F. A. P., "*Information Hiding – Technique for steganography and digital watermarking",* Computer Security Series, Boston, London, 1999.

[2] Lin, E.T., and Delp, E.J., *"A Review of Fragile Watermarks"*, 1999, URL: ftp://skynet.ecn.purdue.edu/pub/dist/delp/acm99/paper.pdf

[3] Lin, E.T., Podilchuk, C.I., and Delp, E.J., *"Detection of Image Alterations using Semi-fragile Watermarks"*, 2000, URL: ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei00-water/paper.pdf

[4] Mintzer, F. Braudaway, G.W., and Bell, A.E., "Opportunities for Watermarking Standards", *Communication of the ACM*, vol. 41, 7, 1998, pp. 56 – 64.

[5] Mintzer, F. Braudaway, G.W., and Yeung, M.M., "Effective and Ineffective Digital Watermark", *Proc. ICIP'97IEEE Int. Conf. on Image Processing,* Santa Barbara, CA, vol. III, 10, 1997, pp.223-226.

[6] Cox, I.J., Kilian, J., Leighton, T., and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia", *IEEE*

Transaction on Image Processing, vol. 6, 12, 1997, pp. 1673-1687

[7] Petitcolas, F.A. and Anderson, R.J., "Evaluation of Copyright Marking Systems", *Proceedings of IEEE Multimedia Systems'99*, Florence, Italy, vol.1, 6, 1999, pp. 574-579,

[8] Sowers, S. and Youssef, A., *"Testing Digital Watermark Resistance to Destruction"*, 1998, URL: http://link.springer.de/link/service/series/0558/papers/1525/15250239.pdf

[9] Wolfgang, R.B. and Delp, E.J. "Overview of Image Security Techniques with Applications in Multimedia Systems", *Proceedings of the SPIE International Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways*, Vol. 3228, November 4-5, 1997, Dallas, TX, pp. 297-308.

[10] Ferrill, E., and Moyer, M. *"A Survey of Digital Watermarking,* 1999, URL: http://www.cc.gatech.edu/~mjm/dw/watermarking.html

[11] Jeong, S. and Hong, K. *"Dual Detection of A Watermark Embedded in DCT Domain",* 2001, URL: http://www-ise.stanford.edu/class/ee368a-proj01/dropbox/project06/

[12] Saha, S., 2000, "*Image Compression – From DCT to Wavelets: A Review"* URL: http://www.acm.org/crossroads/xrds6-3/sahaimgcoding.html