Digital Watermarking

Dr. Shubhangi Sapkal

Digital Watermarking

- Digital data can be easily copied, modified and forgeries be created by anyone having a computer. Most prone to such malicious attacks are the digital images published in the Internet.
- Digital Watermarking can be used as a tool for discovering unauthorized data reuse and also for copyright protection.
- Digital Watermarking is the technique of embedding some identification information known as watermark into the digital data by its owner. On embedding or data hiding a watermarked data is generated.
- Large numbers of watermarking schemes are currently available. An acceptable Watermarking must possess certain qualities as robustness and imperceptibility.

Digital Watermarking

- Digital data storage has gained popularity over the analog counterparts for information storage and handling. Digital techniques are far superior to analog counterparts.
- However, a difficulty faced in digital world is that the manipulation and duplication of digitalized information is very easy. For instance, anyone who has a computer system can easily create forgeries and then redistribute the images and other data's through the Internet.
- Suitable techniques must be developed and made available to protect the data from unauthorized modifications and illegal reuse.
- Digital watermarking is proposed as a method for protecting the ownership rights of digitalized data. Digital watermarking integrates or embeds some information as the owner name or logo in to a digital media. Thus watermark information will serve as the identification mark of its owner. With the aid of this embedded watermark whenever we suspect the data or an image is illegally edited and copied it is possible to produce enough evidence to prove the ownership.

History

- Watermarking as technique for copyright protection evolved with the discovery of paper. The word Watermarking is coined from the conventional use of placing a visible watermark on paper. It was used as a method against counterfeiting books and currency notes.
- The origin of data hiding or invisible watermarking may be traced to the age of ancient Greeks who transferred their information after modifying the contents in a text by swapping the positions of alphabets.
- The Greeks thus were able to send secret information across the border without getting noticed. In Rome the heads of slaves were shaven and a message is tattooed. When the hairs are fully grown they are send to the destinations through the enemy lines.
- By 18th century Watermarking began to be used as anti-counterfeiting measure on money and other documents. The first patent in Watermarking was filed by Emil Hembrooke in 1954, titled “Identification of Sound and like Signals”.
- In early 1980s, Muzak Corporation used to watermark analog audio signal to identify their music. Their system used a notch filter to block the audio signal at 1 KHz for a varying duration to encode identification information using Morse code. About 1995, interest in digital Watermarking began to mushroom.

Steganography vs. Watermarking

- Steganography is a sub discipline of cryptography and means data hiding.
- Cryptography is about maintaining the secrecy of the information by encoding them. This forbids from being read by any unauthorized person.
- Steganography attempts to maintain the information secrecy by not getting noticed also at the same time. Steganography in Greek means covered writing or secret writing. In Steganography information is hidden in a harmless source, known as cover media, in a way that it is not known to others. The existence of the information thus goes unnoticed.
- Watermarking integrates information into a data without affecting its actual usage. Watermarking mostly uses same principles and techniques as Steganography for data insertion and hiding in a host media. However, information hiding as done in Steganography is many way different from cryptography where the chief concern is protecting the message content.

Steganography Vs Digital Image Watermarking

- In Digital Image Watermarking the watermark signal is embedded into a source image that is to be protected against abuses. Watermark can be a string of bits representing a text or owners name or an image such as a trademark symbol or logo.
- The main difference between these two processes is in steganography the hidden data is on highest priority for sender and receiver but in watermarking bot source image and hidden image, signature or data is on highest priority.

Process	Method Adopted	Purpose	Feature
Cryptography	Data is encrypted using a secret key.	Protects the contents in point to point communication.	Maintains the message secrecy.
Steganography	Uses a cover media to hide the data.	Existence of a message is kept as secret.	Hides actual messages from unauthorized listeners/viewers
Watermarking	Inserts an unique owners identification mark.	Copyright Protection, Authentication	Do not protect the content; the ownership rights could be established.

Table. 1 A Comparison of watermarking vs. others

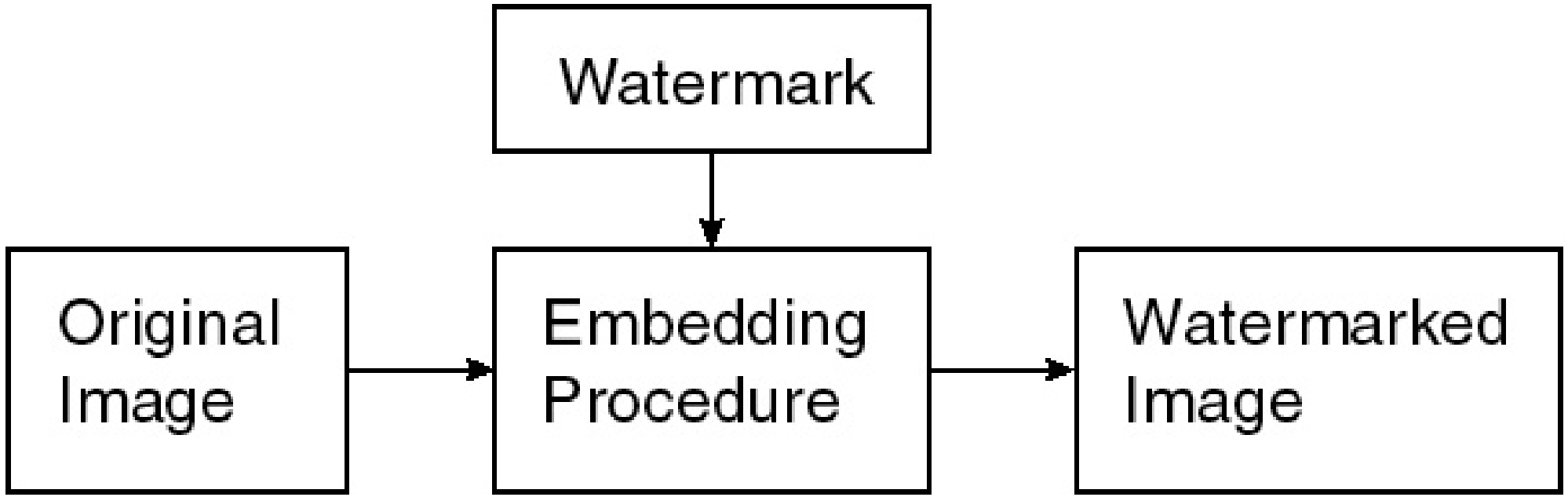
Process of Image Watermarking

The process of watermarking is divided into two parts:

a) Embedding of watermark into host image.
b) Extraction of watermark from image.

Watermarking Embedding

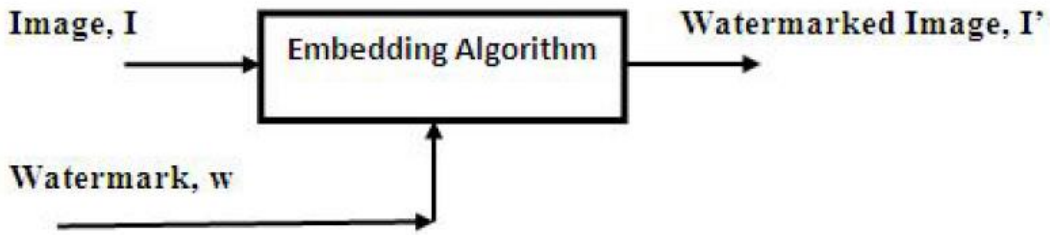
- The process of image watermarking is done at the source end. In this process watermark is embedding in the host image by using any watermarking algorithm or process. The whole process is shown in figure



Watermarking Process

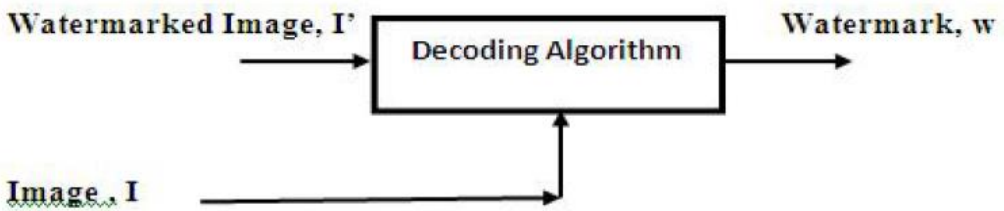
Watermarking System

- A Watermarking system comprises two distinct stages: Embedding and Detection. Watermark embedding needs an algorithm and a unique watermark that is encoded into the host media by the algorithm.
- The embedding algorithm E accepts the watermark w and embeds this in the image I to create the watermarked signal I'.



Watermarking Extraction

This is the process of Extracting watermark from the watermarked image by reverse the embedding algorithm.
The decoding section retrieves the watermark from the watermarked signal when it is required to of the owner to prove his ownership rights. Figure 2 illustrates the decoding operation.



The decoding algorithm retrieves the watermark w from I'. When decoding, there are techniques that do need the original image and others that do not need original images. The above is a blind watermarking technique that the original image to generate watermark w.

Watermarking Properties

Watermarking need some desirable properties based on the application of the watermarking system. Some of the properties are presented here:

Effectiveness:

This is the most important property of watermark that the watermark should be effective means it should surely be detective. If this will not happened the goal of the watermarking is not fulfilled.

Watermarking Properties

Host signal Quality:

This is also important property of watermarking. Everybody knows that in watermarking, watermark is embedded in host signal (image, video, audio etc.). This may put an effect on the host signal. So the watermarking system should be like as, it will minimum changes the host signal and it should be unnoticeable when watermark is invisible.

Watermarking Properties

Watermark Size

Watermark is often use to owner identification or security confirmation of host signal and it always use when data is transmitted. So it is important that the size of watermark should be minimum because it will increase the size of data to be transmitted.

Watermarking Properties

Robustness

- Robustness is crucial property for all watermarking systems. There are so many causes by which watermark is degraded, altered during transmission, attacked by hackers in paid media applications. So watermark should robust, So that it withstand against all the attacks and threats.
- By robust it means the watermarked image is able to survive manipulations and other attacks.
- Watermarking must also withstand severe signal processing attacks as compressing or scaling.
- Robustness is the ability of the watermarked signal to *resist* the attacks or distortions introduced by malicious data processing. This feature makes watermarked images acceptable for legal purpose.

Watermarking Properties

Imperceptibility

- A watermark, in fact has the effect of adding noise. However, the watermark must not distract the viewer from the image itself. The modifications introduced on watermark insertion should be below the perceptible threshold.
- After embedding, the watermarked image must be visibly appealing and identical to the original media. A watermark is called imperceptible if the original signal and marked signal is indistinguishable.

Watermarking Properties

Reversibility

- Reversibility is a measure of the extent to which watermark signal removal is possible from the watermarked media.
- In certain applications as forensic or medical, the watermark removal is desirable once the purpose is served. After authentication the image can be restored to their original form by removing the watermarking.

Watermarking Properties

Lossless embedding

- The embedding process usually transforms the images to some domain as cosine transform or wavelet transform for adding the watermark signal. Distortions are normally introduced as an after effect of this conversion.
- A good watermarking system should be lossless, in that it should not distort the original
- contents or in other words should not affect the functionality of the media.

Security

- Watermarks must exist undetectable. Even by use of known methods or algorithms the watermark removal should not possible to an intruder. Security means that even after the presence of the watermark is known to a malicious attacker it must not be possible for them to remove the same from the host media.

Classification

- Digital watermarking techniques are classified into various types. This classification based on several criteria.
- In the image watermarking domain based techniques is generally used. They are spatial domain and transfer domain. But transfer domain techniques are more used compared to spatial domain.

S.no	Criteria	Classification
1.	Watermark Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: Any logo, Stamp Image etc.
2.	Robustness	1. Fragile: Easily Manipulated. 2. Semi-Fragile: Resist from some type of Attacks 3. Robust: not affected from attack
3.	Domain	1. Spatial: LSB, Spread Spectrum 2. Frequency: DWT, DCT, DFT, SVD
4.	Perceptivity	1. Visible Watermarking: Channel logo 2. Invisible Watermarking: like Steganography
5.	Host Data	1. Image Watermarking 2. Text Watermarking 3. Audio Watermarking 4. Video Watermarking
6.	Data Extraction	1. Blind 2. Semi-Blind 3. Non- Blind

Table 1: Types of watermarking basis of different Criteria

Transfer Domain Techniques:

- In this technique the coefficients of transfer domain are modified of Digital Image not like as the pixels values which is changed in spatial domain. Reverse process will be used to extract the watermark from watermarked image.

Some of the main transfer Domain techniques are:

I. Discrete Cosine Transform

II. Discrete Wavelet Transform

III. Discrete Fourier Transform

- Anyone can use individual transform techniques for watermarking but recently combination of these techniques are also used by researchers. By these combinations developers can used best features of any individual technique.

Applications (uses) of watermarking

- Protecting the digital data in our databases or internet from unauthorized reuse is tedious. Practically, it may not be possible to stop the illegal data modification or copy generation. Using an embedded watermark in the source data the ownership rights can be established beyond doubt.
- Watermarking makes the duplications identifiable and thus reuse becomes almost impossible. For instance the currency notes are watermarked by the government as proof for their authenticity. This makes forgeries difficult and identifiable from the original.
- Another popular use of Watermarking is for tamper proofing. The content of the watermarked data is verifiable and can discover any manipulations and unacceptable modifications if any.
- Watermarking is now possible for any digital media as: text, audio, video or images. Digital watermarking is very much useful for varied application as: Proof of ownership, Means of tamper proofing, Labeling for user awareness, Covert communication, Broadcast Monitoring, device identification and controlled access.

Applications of watermarking

- Watermarking technologies is applied in every digital media whereas security and owner identification is needed. A few most common applications are listed hereby.

Owner Identification

- The application of watermarking to which he developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attackers.
- So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and removed.

Applications of watermarking

Copy Protection

Illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry.

Broadcast Monitoring

Broadcasting of TV channels and radio news is also monitoring by watermarking. It is generally done with the Paid media like sports broadcast or news broadcast.

Medical applications

Medical media and documents also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means.

Applications of watermarking

Fingerprinting

- A fingerprinting is a technique by which a work can be assigned a unique identification by storing some digital information in it in the form of watermark.
- Detecting the watermark from any illegal copy can lead to the identification of the person who has leaked the original content. In cinema halls the movies are played digitally through satellite which has the watermark having theater identification so if theater identification detected from a pirated copy then action against a theater can be taken.

Applications of watermarking

Data Authentication

- Authentication is the process of identify that the received content or data should be exact as it was sent.
- There should be no tampering done with it. So for that purpose sender embedded the digital watermark with the host data and it would be extracted at the receivers end and verified. Example like as CRC (cyclic redundancy check) or parity check.

Threats and Challenges

- Digital data can be easily copied, edited and transferred. The use of Watermarking does not ensure that our digital data is protected from being copied and edited. However, watermarking permits us to prove the copyright of the authors and also in protecting the authenticity.
- Any operation, intentional or unintentional, upon the watermarked data that impairs the watermark can be called as an Attack.
- Digital Images are subject to varied attacks as cropping, scaling, rotating, compression and noise.
- Most of the proposed conventional watermarks in literature are easily broken on attacks or on multiple attacks.

Threats and Challenges

- Robustness to attacks is thus the most desired feature if the ownership right has to be established in the court.
- The watermarks are weakened by signal processing as signal enhancement or D/A and A/D conversion. Many watermarks are unable to withstand strong lossy compression.
- Content-based watermarking approach that uses geometric wrapping to embed watermarks offers high robustness against lossy compressions to some extent.
- Intentional attacks as removal of watermarks are possible if an attacker procures many copies of differently watermarked images and tries by averaging all copies. An attacker may also attempt to remove the watermark by trying to estimate the original image.
- Another possible attack that can create ambiguity is, when an attacker re-watermarks the image using his logo. The attacker will be able to generate his watermark from the watermarked data and can claim to be the real owner.

References:

- Lalit Kumar Saini, Vishal Shrivastava, ” A Survey of Digital Watermarking Techniques and its Applications”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.
- *Jobin Abraham, “*Digital Image Watermarking: An Overview*”, National seminar on modern trends in EC&SP, 2011.*