Digital Watermarking

Dr. Shubhangi Sapkal

Classification

- Digital watermarking techniques are classified into various types. This classification based on several criteria.
- In the image watermarking domain based techniques are 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

According to perceptivity

Visible: Visible watermark can be in form of text or a logo identifying the owner. Television channels use visible watermark by superimposing respective logo.

Invisible: Invisible watermarks are embedded into the host signal such that it cannot be detected by human eye. Basically the embedding level is too small to notice and watermark can be retrieved by extraction software. It protects and authenticates the copyright owners well.

According to perceptivity

Invisible watermark can also be classified into two types:

1) Robust Watermark: A watermark is called robust if it resists a designated class of transformations. Means it aims to embed information in a file that cannot be easily destroyed by any manipulations on it. Robust watermarks have very significant importance in applications where more security is concern.

According to perceptivity

It can also be divided into following:

Public and Private Watermark: They are differentiated in accordance with the secrecy needs for the key accustomed insert and retrieve watermarks. If the original multimedia data is not known during detection phase then it is called a public or blind watermark otherwise it is called a private or non blind watermark.

Invertible/Noninvertible and Quasi/Non- Quasi Invertible watermark: Suppose that the copyright owner A embeds his watermark WA into the host medium I with an inserter EA. IA be watermarked image. Let B be any attacker consist of inserter EB and detector DB and is able to construct a watermark WB as well as a fake data I' from IA such that

(1) EB(I',WB)=IA,

(2) DB(IA ,WB)=1,

(here 1 means "watermarked", and 0 means "not watermarked"), and

(3) I' is similar to IA,

then the watermarking system (EB, DB) is claimed to be invertible. In Quasi-Invertible watermarking the attacker can find WB, I', and IB so that

(1)EB(I',WB)=IB,

(2)DB(IB,WB)=1, DB(IA,WB)=1, and

(3) both I' and IB are similar to IA.

Quasi-invertible is less flexible than full invertibility.

2) Fragile/Semi-fragile Watermark: A watermark is called *fragile* if it fails to be detected after the slightest modification however it is called *semi-fragile* if it resists beginning transformations but fails detection after malignant transformations.

According to type of host signal

- **Image Watermarking:** The watermark embed into the image as host signal which later on detect and extract in accordance to the copyright ownership.
- **Video Watermarking:** It is basically the extension of image watermarking and adds watermark in the video stream, hence needs real time extraction and strength for compression.
- **Audio Watermarking:** The embedded watermark in audio files should be lower than the perceptual threshold of human auditory system.
- **Text Watermarking:** Hiding watermark in the PDF, DOC and different document to forestall the frequent updates to the text is known as text watermarking.

According to working domain

Spatial Domain: These methods are based on direct modification of the values of the image pixels hence the watermark needs to be imbedded during this method. Such strategies are easy and computationally economical, so as they modify the colour, luminance or brightness values of digital image pixels hence their application is completed very simply, and requires less computational power. However, the spatial domain watermarking algorithms are generally fragile to signal processing operations or other attacks.

According to working domain –Spatial Domain

LSB technique is one of the oldest spatial domain method, includes insertion of watermark into the least significant bits (LSB) of pixel data.

One of the foremost limitation of spatial domain is that the capability of an image to carry the watermark since the effect of modification on pixel values to the cover image, applied by spatial methods like LSB of the data often visually indifferent.

According to working domain –Frequency Domain

- **Frequency (transform) Domain:** During watermarking in transform domain, the original host data is transformed according to the transform coefficients. These transform coefficients are perturbed slightly in several ways to represent the watermark.
- Coefficients identification during watermarking is the most severe problem in the frequency domain. Embedding can be done by adding a pseudorandom noise, quantization (threshold) or image (logo) fusion.
- Most algorithms consider HAS (human auditory system) and HVS (human visual system) for audio as well as image files respectively to minimize perceptibility. The goal is to incur more information bits so that they become robust to attack and are least noticeable. Hence the frequency-domain techniques infix the watermark by restraining the magnitude of coefficients in a transform domain, such as discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT).
- Although frequency-domain methods can yield more embedding information and more robustness against many common attacks, the computational cost is higher than spatial-domain watermarking strategies.

According to type of key

Symmetric or private-key: In such schemes, both watermark embedding and detection are performed using the same key K.

Asymmetric or public-key: These watermarks can be detected with a key that is different from the one that was used in the embedding stage. A pair of keys is used in this case: a private key to generate the watermark for embedding, and a public one for detection. For each private key, many public keys may be produced.

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.*