Survey on Watermarking Techniques

Sadhna Rana
Dept. of CSE, Guru Nanak Dev University, Amritsar, Punjab, India

Abstract
This paper deals with digital watermarking, to protect the digital media such as videos, images and audio from copyright. With the growing and rapid use of internet services, issues like integrity, authenticity, copyright protection have become more important, since the duplication and unauthorized use of the digital content has become easier results in development of various watermarking techniques to maintain originality of data. For different techniques, different algorithms are used such as for image watermarking we divide the image into two parts ROI and RONI, then RONI into three parts and embed watermark into these areas, DWT, DFT and DCT in video watermark and in audio watermark phase coding and sonic watermarking techniques used.Mainly this paper summarizes applications and properties of watermarking.

Keywords
Discrete Wavelets Transform (DWT); Discrete Cosine Transform (DCT); Hash Key; ROI and RONI.

I. Introduction

Security is used for protecting against danger, damage, loss and criminal activity. When an important and private message is to be delivered to a destination, authentication and confidentiality are required. Digital watermarking has to embed pieces of information into a digital media for protecting it against copyright and other unauthorized user. Digital media can be Image, audio, video and text documents. Later the embedded out to reveal the real identity of the digital media.

The watermarks can be of type visible and invisible.

1. **Visible:** In this type,the watemark is visible to casual viewer.
2. **Invisible:** In this type,the watermark is invisible to viewer. It is only visible to authorised user, it is visible by using some decoding mechanisim.

Image watermarking is a process of hiding digital data in the image. It is used to protect the photos over internet. The concept of video watermarking comes from the concept of image watermarking. A video is a collection of number of digital images, so video watermarking is hiding data in the frames of video. Any frame from the frames of video is selected and the data is embed in it, it is called video watermarking. Digital audio watermarking has to do with protecting digital audio file against illegal copying because they can be downloaded and copied with ease. Audio watermarks are special signals embedded into digital audio.

II. Historical Perspective

The term "Digital Watermark" was developed by Andrew Tirkel and Charles Osborne in December 1992. The first successful embedding and extraction of a watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin.[Watermarks are identification marks produced during the paper making process. During the 13th century, in Italy the first watermarks appeared but their use rapidly spread across Europe. They were used to identify the papermaker that manufactured the paper. The marks often were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

As Digital watermarking is divided into two main categories: visible and invisible. The visible watermark is very simple. It is just like to stamping a watermark on paper, and for this reason its sometimes calls digitally stamped.Though a lot of research has been done in the area of invisible watermarks, much less has been done for visible watermarks.Both visible and invisible watermarks are differ from each other so there are different methods to watermark both of these. Visible watermarks are especially used to show ownership,it is done by Mintzer, Braudaway & Yeung in1997. Invisible watermarks, where the ownership is not directly shown with naked eyes.On this, work done by Mintzer et al.in 1997; Swanson et al. in 1998.

III. Why Watermarking?

The basic requirements of the digital watermarking can be treated as properties. Different applications require singular properties of watermarking.

The different attributes of the watermarking take different place in application design. The basic properties of watermarking are as follows:

A. Robustness

Robustness refers to that the watermark embedded in data has the capability of detecting watermark after a variety of processing operations and attacks. The watermark should not removed by simple processing techniques. Hence watermark should be strong against some attack. Robust watermarks are designed to protect from normal processing.

B. Data Payload

Data payload is to embedded the number of bits into the original image. It is the highest quantity of information that can be hidden without modifying image quality. It can be calculated by the amount of hidden information in the original data. This property decides how much data should be embedded as a watermark so that it can be effectively detected during extraction process.

C. Security

If an unauthorized person cannot remove the watermark without having full awareness of embedding algorithm, detector and composition of watermark, then a watermark system is said to be secure. The security is most important property of watermarking system. Only the authorized person can detect watermark. Thus, the copyrights protection can achieve in watermarking system.

D. Computational Complexity

Computation complexity is the total amount of time taken by the watermarking algorithm for embedding and decoding process. For the strong security and validity of the watermark More computational difficulty is needed. On the other hand, real-time applications needs both efficiency and security.

IV. Techniques

A. Digital Audio Watermarking System

The watermarking system consists of two stages. The embedding process is defined as:

Sw= Embedding(So, W o, K w ,K s)

Where So is host signal
W o is original watermark
K w is watermark key
K s is secret key .
The second stage is extraction process, which is defined as

Sw= detection(Sa, So, Kw ,Ks)

Where Sa is attacked signal
So is host signal (optional)
Kw is watermark key
Ks is secret key

Audio Water Marking Techniques

The watermarking can be implemented in time domain and frequency domain. Time domain approach is rather easier to implement and requires less computation. But it is less robust to digital signal attacks.

1. Phase Coding

The HAS can perceive only the relative phase not the absolute phase. Therefore the watermark can be embedded into the phase of the original audio file.

Algorithm

Step 1: Split the host signal into Np frames with N samples.
Step 2: Generate the watermark. Here, binary watermark is used
Step 3: Calculate the magnitude & Phase spectrum using fast Fourier transform. Step4: Phase spectrum is modified according to the watermark.
If watermark bit =1 then phase is Π/2 If watermark bit = 0 then phase is (-Π/2)
Step5: reconstruct the watermarked frame.
Step6: Extract the watermark based on the phase spectrum.
If extracted phase is ≥0,then watermark bit = 1 If extracted phase is < 0 then watermark bit = 0

2. Sonic Watermarking

The challenge in watermarking field is embedding the watermark in real time not in digitally stored file. The sonic watermarking is proposed algorithm for live performance . In sonic watermarking, the watermark sound generated by a watermark generator is mixed with the host sound in the air.

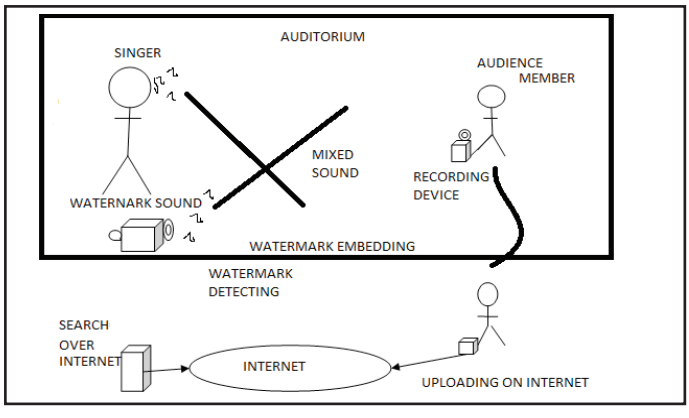


Fig. 1:

According to the author the problems in sonic watermarking are as follows:

- Real time embedding: As the watermark and host is mixed in air, there can be delay.
- Robustness: Reverberation, noises made by audience are the next major drawbacks for live embedding.
- Acoustic quality: The Strength and different location of sound sources also affect the embedding strength.

3. Analog and Digital Inter Conversion

The Analog and Digital Inter conversion module should consider the following:

- The audio frequency > 50Hz should be taken into account of watermarking.
- The noise in DA/AD process such as Quantization distortion and filtering process. Embedding should not use the high frequency also because of the above mentioned noise in DA/AD process.
- The record time may be earlier or later than the play time, so the starting position of the watermark should have synchronized signal.
- Analog and Digital Inter conversion for the different sound cards.

B. Digital Image Watermarking System

1. Embedding Algorithm

In the embedding algorithim the image is divided into two regions,called Region of interset (ROI)and Region of Non-interest (RONI).The Watermark should always be embedd in RONI. In RONI, it is divided into three parts called area1, area2, area3 and then divide the area1 and area2 into 8x8 sub-blocks. This technique mainly used in MRI medical images. Here use the discrete wavelet transform and second fragile hash-key watermark into the MRI image.

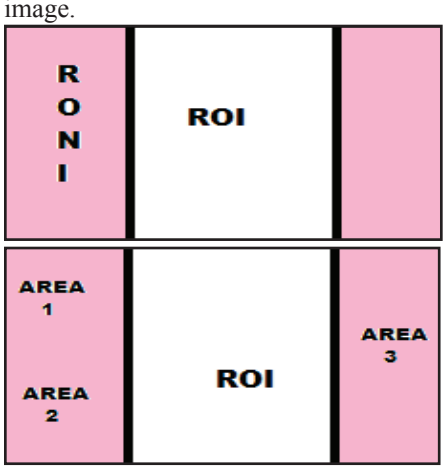


Fig. 2:

[LL, LH, HL, HH] = DWT {fk}
If w=1 then LL={Qo(LL/Δ)
If w=0 then LL={Qe(LL/Δ)
fk represents the 8x8 sub-block of area1 and area2 of RONI.
LL, LH, HL and HH represent an approximation (low frequency) and detail (high frequency) components of discrete wavelet transform decomposes 8x8 sub-blocks.
W represents the watermark information,
Qe indicates even quantization while
Qo indicates odd quantization to the nearest integer number.
The Δ is the DWT scaling factor.

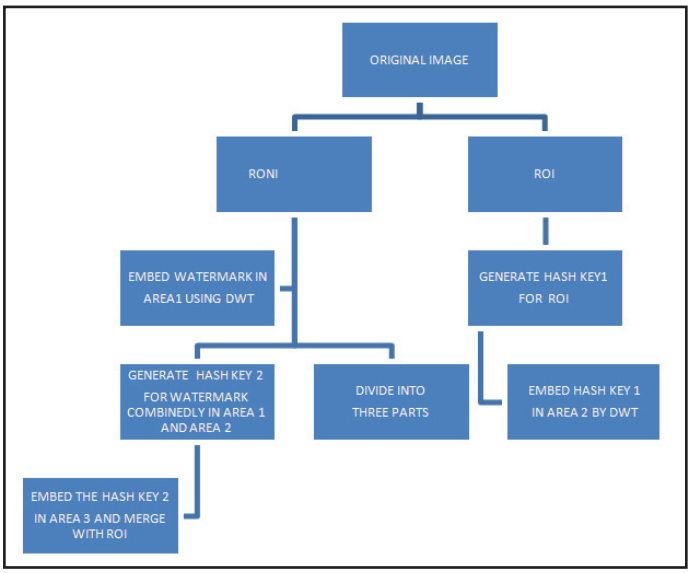
2. Algorithm For Watermarking Embedding

- Divide MRI image into two regions ROI and RONI.

Divide RONI into three regions called area1, area2 and area3.
Divide area1 and area2 into NHB 8×8 sub-blocks
Finding 2-level DWT(Discrete wavlet transform) of 8×8 sub-blocks

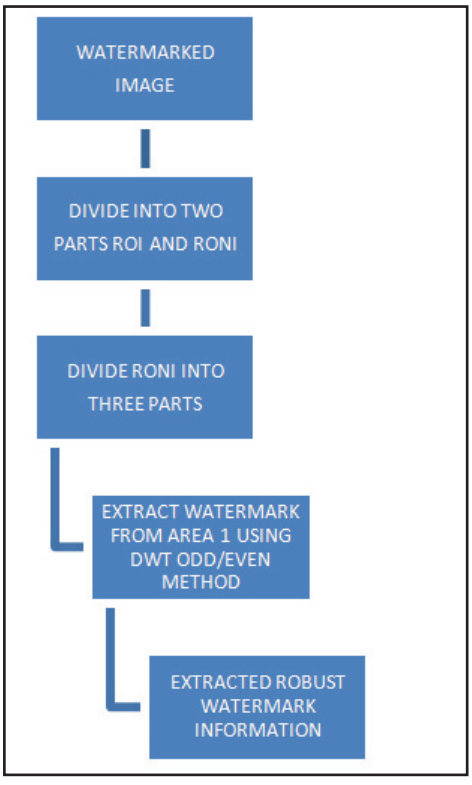
[LL1, LH1, HL1, HH1] = DWT[fkHB]
[LL2, LH2, HL2, HH2] = DWT[LL1]

- Robust watermark information is embedded into area1 in the wavelet domain.
- Fragile watermark information, hash-key1 is embedded into area2 in the wavelet domain.
- Fragile watermark information, hash-key2 is embedded into area3 in the spatial domain.

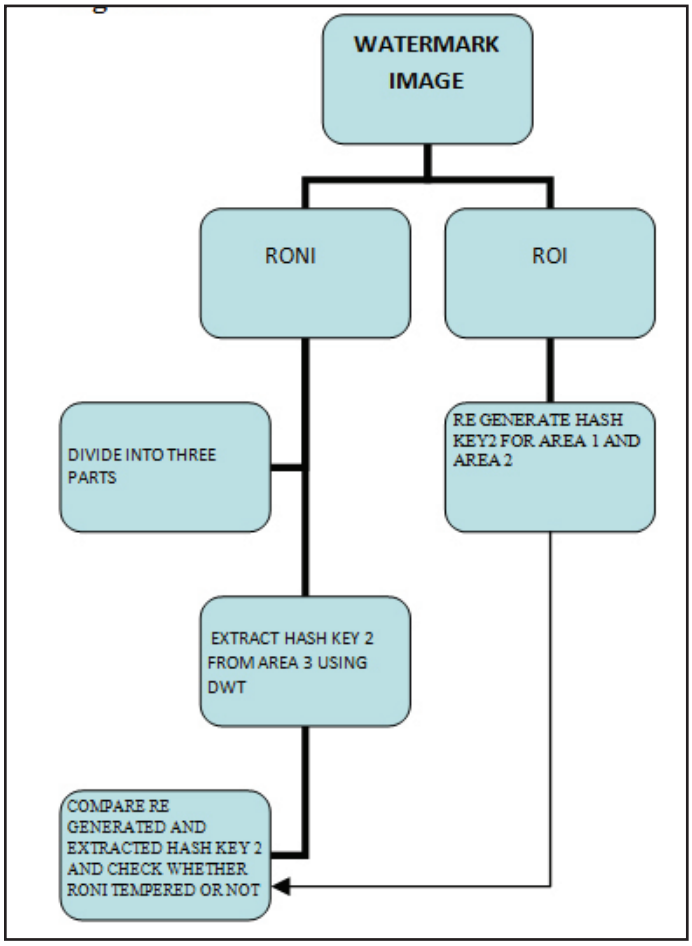


3. Extraction of Watermarks

1. Robust Watermark Extraction /Decoding Algorithm:



2. Hash-key2 Watermark Extraction Algorithm:



C. Digital Video Watermarking System

1. Embedding Process

This contains the selection of watermark which is going to embed on the digital data. The selection of watermark depends upon the kind of data it is, whether it is original data or compressed data and whether the watermark is visible .

2. Extraction Process

In this process to demonstrate or show the concern of copyright on the data and to make sure that the purpose of watermarking has been achieved the watermark is extracted from the watermarked digital data.

(i). Spatial Domain

This is the process of adding watermark to the data . It modifies the pixels of randomly selected data. In this the raw data is directly loaded to image pixels. It uses LSB (Least Significant Bit) algorithm and Patchwork technique.

- **Least Significant Bit Algorithm:** This algorithm is easy to implement and understand. It adds the watermark to the lowest order bit of each pixel of the image. As the watermark is embedded at the lowest bit of the pixel similarly the extraction is done by detecting the lowest bit of the pixel in the image and then the watermark is extracted from the data.
- **Patchwork Technique:** Patchwork technique is based on some statistical result because it embed the watermark in the data with a specific statistics by using Gaussian distribution. The extraction of watermark can be done by combining the received signals with expected form.

(ii). Frequency Domain

It is also known as Transform domain. It uses several frequencies to insert the watermark in the data. It uses domain methods to implement the watermark as:

- **DCT (Discrete Cosine Transformation):** It adds watermarks to a still digital image. In this the image is presented in the form of frequencies of cosine.

Then 8*8 blocks of the image s considered calculating the DCT of the image.

- **DWT (Discrete Wavelet Transform):** It generates a time frequency of particular signals at a given time. It converts the image into three dimensions Horizontal, vertical, diagonal respectively. The transformations are base4d on small waves namely wavelet.
- **DFT (Discrete Fourier Transform):** It converts the Unique functions into frequency components. In case of digital image, the even functions are considered as the frequency of sine or cosine and multiplied with the weighing function. It generates the coefficient of Fourier transform in the signal.

V. Applications

A. Copyright Protection

The one of the most important application of watermarking is copyright protection from the unauthorized user. Ownership of digital media can be established in the case of a copyright dispute by using the embedded data as a proof.

B. Broadcast Monitoring

This application is used to get the information of an unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

C. Authentication and Integrity Verification

The watermark is embedded to check is the image customized or not, this process is used for verification. Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness for modifying an image.

D. Fingerprinting

The main purpose of fingerprinting is to protect clients. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by embedding single robust watermark for each receiver.

E. Medical Applications

In medical field the watermarking is important for the purpose to protect the hospital's information such as patient's report from an unauthorized people.

VI. Conclusion

In this paper, we studies different techniques of watermarking. A great scope exists for more improvements. We have analyzed the phase audio watermarking. This watermarking can not be used for live embedding. In video watermarking , the combination of DCT and DWT domain can be one of the future aspects to have more secured watermarking. Copying photos from the Internet is just a matter of right clicking on a photo and saving it on the computer hence the security and authenticity of the image or data are cracks. The watermark is required to prevent the original images and other documents over the internet.

References

[1] [Online] Available: http://en.wikipedia.org/wiki/watermarking
[2] [Online] Available: http://www.scribd.com/doc/6816148/watermarking
[3] [Online] Available: http://ippr-practical.blogspot.in
[4] [Online] Available: http://www.scisstudyguides.addr.com
[5] [Online] Available: http://ieeexplore.ieee.org/document/watermarking
[6] [Online] Available: http://esatjournals.org
[7] International Journal of Computer Applications, Vol. 110 – No. 1, January 2015
[8] IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308