Digital Image Watermarking: A Review

RINA A. RAM
Dept. of Electronics and Communication
Noble Group of Institute
Junagadh, India
reenajnd@gmail.com

Prof. Ashis kothari
Dept. of Electronics and Communication
Atmiya Institute of Technology & Science
Rajkot, India
amkothari@aits.edu.in

Prof. Divyag Shah
Dept. of Electronics and Communication
Noble Group of Institute
Junagadh, India
Divyag303@Gmail.com

Abstract

Digital watermarking is the act of hiding a message related to a digital signal in different forms like an image, song, video within the signal itself. In this paper, we present review on Image Watermarking for Good Robustness. In this paper, we discuss the various factors used in watermarking, application area where watermarking technique need to be used. Also a survey on the some new work is done in image watermarking field.

Index Terms — Digital Watermark, Steganography, Authentication, Frequency Domain, Spatial Domain

I. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark. For visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

The watermark may be intended for widespread use and thus is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove.

![Figure 1 Embedding Process – Digital Watermarking](image1)

![Figure 2 Extraction Process – Digital Watermarking](image2)
Robustness means that the watermarking scheme employed should be able to preserve the watermark under various attacks. The attack could be anything like rotation, translation, cropping, scaling or passing the image through various types of filters. There might be some noise introduced by this processing but this should not affect the retrieval of the watermark.

**Imperceptibility**

The imperceptibility refers to the perceptual transparency of the watermark. Watermarking should be done in a way such that it does not affect the quality of the image or the hidden data after watermarking. The changes in the image should not be noticeable to the naked eye. A straightforward way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host signal. However, this makes it easy for an attacker to alter the watermark information without being noticed.

**Payload Capacity**

Payload Capacity normally refers to the amount of information that can be embedded into a host signal. Various applications have different sizes of the data that is to be hidden. This directly affects the robustness and the perceptual impact. If too much of the data is hidden in the image (much more than the payload capacity) it is harmful for the quality of image as the resolution of the images reduces drastically.

II. TYPE OF WATERMARKING

- **Spatial Domain Watermarking**
  - In this method the pixel information of the two-dimensional image is altered so as to embed the hidden data.

- **Transform Domain Watermarking**
  - Transform domain watermarking techniques apply some invertible transforms to the host image before embedding the watermark. Then, the transform domain coefficients are modified to embed the watermark and finally the inverse transform is applied to obtain the marked image.

**Invisible Watermarking**

In this technique the watermark is embedded in the cover object in such a way that it cannot be perceptually visible.

**Visible Watermarking**

In this technique the watermark is superimposed on the cover object in such a way that it can be perceptually visible.

**Source Based Watermarking**

Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with.

**Destination Based Watermarking**

In Destination based each distributed copy gets a unique watermark identifying the particular buyer. The destination based watermark could be used to trace the buyer in the case of illegal reselling.

III. APPLICATION

A. **Copyright Protection**: Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.

B. **Content Archiving**: Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems.
C. Meta-data Insertion: Meta-data refers to the data that describes data. Images can be labelled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records.  

D. Broadcast Monitoring: Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. This has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.  

E. Tamper Detection: Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.  

IV. CONCLUSION  
In this paper we have obtainable various aspects for digital watermarking like introduction, outline, techniques, and applications. We also tried to classify the digital watermarking in all the known aspects like robustness, perpectivity, purpose, watermark type, domain, and detection process. In this paper we tried to give the whole information about the digital watermarking which will help the new researchers to get the maximum awareness in this domain.  

REFERENCES  


