IMAGE WATERMARKING- A REVIEW

Shivani Khurana

E-mail:shivani.khurana27@gmail.com

Abstract: Watermarking is a relatively an active research field. The invent of internet resulted in new opportunities for the creation and delivery of content in digitized form. Different applications can be included that is electronic advertising, real time video and audio delivery and Web publishing. An important issue that arises in these applications is the protection of the rights. It has been recognized that current copyright laws are not sufficient for dealing with digital data. One technical way is law enforcement and copyright protection for digital media and practical is digital watermarking which is aimed to automatically embed and detect copyright infringement. There has therefore been significant recent research into "watermarking" and "fingerprinting". The idea is to detect copyright violators, unethical hackers doing cyber crime and the former to prosecute them.

Keywords: Image-watermarking, Video, Copyright, Digital media, Fingerprinting.

I. INTRODUCTION

In the case of image watermarking the imperceptible watermark is added to the host image. The host image is modified by signature data to make the watermarked image. It is very important to have some kind of error or distortion, the watermarked image is distributed and may circulate from legitimate to illegitimate customers. Thereby, it is subjected to various kinds of image distortion. Image distortion may result from different kind of attacks, for example lossy image compression, re-sampling, quantization, scaling and cropping or from specific attacks on the embedded data.

II. General Framework for Watermarking

Watermarking is the process of embedding watermark in multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright.

As a method of Intellectual Property Rights (IPRs), digital watermarking have stimulated significant interest and become an active area of research. A digital document can be authenticated with what is known as a digital watermark. A watermark is a secret code or image incorporated into digital, original content which acts to verify both the owner and content of document. A watermark consists of 3 parts:

- Watermark
- Embedding Algorithm
- Extraction/Detection Algorithm

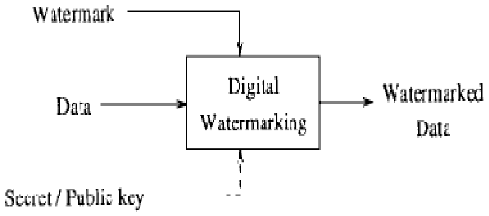

Figure 1 Process of Watermarking

In this process the watermark is generated first so as to add it into original image. A watermark is added to host image depending on the creator information with or without using a secret or public key. In watermarking algorithm the watermark is added robustly and imperceptibly to the image so as to have the watermarked image. The verification algorithm is designed for extraction method which recovers the watermark information from the signal mixture, perhaps with the help of the key and the original for the copyright protection and then the watermark is compared with the extracted watermark which can be further regarded as original ones and reconstructed ones.

III Classification of Watermarking

In contrast to visible watermarks, the watermarks can be classified as FRAGILE or ROBUST. The fragile watermark is used for detecting even the smallest alteration of an image, while the robust one is specially designed to withstand a wide range of "attacks", which basically are trying to remove the watermark, but without destroying the image/video. In the case of robust watermark the measures like false positive and false negative can be measured form the detectors side, This kind of watermark is considered as stable because different kind of tampering are placed and conversion of signals from D/A to A/D.

- ✓ **According to type of Document or by Media: T**ext, Image, Video, Audio
- ✓ **According to Human Perceptibility:** Visible and Invisible.
- ✓ **By goals and Imperceptibility:** Robust, Fragile and Semi-fragile.
- ✓ **By requirement of original for Extraction**: Blind, Non-Blind, Oblivious/Non-oblivious, Public and Private
- ✓ **By Embedding or according to Watermarking** : Spatial domain and Transform domain.
- ✓ **According to Application**: Source based and Destination based.

The two most important ways to classify watermarking methods are:

Spatial Domain – Watermarking schemes that directly perform some transformation on the image pixels are called spatial domain watermarks. The watermark is applied to the pixel or coordinate domain. No transforms are applied to the host signal during watermark embedding.

Transform Domain– Watermarking schemes that transform the image in the frequency domain and then modify the transform coefficients are called Transform domain. The main strength offered by transform domain to address the limitations of pixel based methods

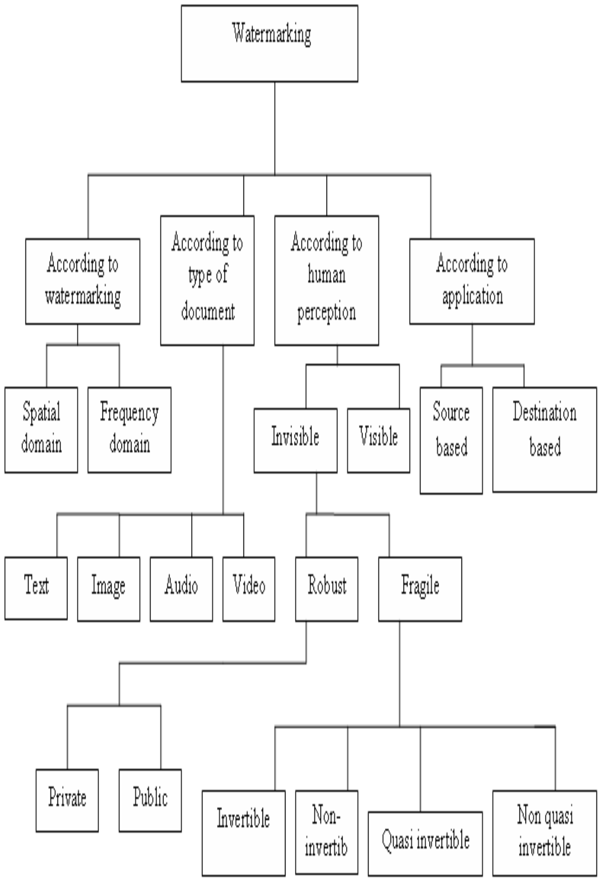

Figure 2 Classifications of Watermarks

IV. Video versus Image Watermarking

A video is generally regarded as a sequence of still images called frames presented at a particular rate (number of frames per second) to give the effect of animation hence video watermarking can be viewed as an extension of image watermarking but the two are not similar. Table summarizes the similarities and difference between the two. From the table we can say that the watermarking techniques for images can be applicable to video watermarking but with significant modifications.

Table 1 Difference between Image and Video

No	Image	Video
1.	The Uniform Jpeg compression commonly handled with various techniques watermarking and compression can be combined also	The Video compression techniques do not necessarily encode each frame of the sequence identically.
2.	Different attacks can be applied like filtering, resizing, contrast enhancement, cropping, and rotation.	Different attacks are frame averaging, frame dropping, frame swapping, statistical analysis, interpolation.
3.	Human perception of Visibility is accounted.	Human perception of motion is accounted.
4.	Watermarking can be combined with Steganography.	Synchronization of the audio with the video sequence may be a consideration for watermark protection
5.	Robust watermark must be detectable and Fragile one must detect Locations of Tampering.	The watermark has to be detectable anywhere in the movie and within a short time.
6.	Risky but not as sensitive as in video.	Embedding same watermark in all the frames of a video sequence is not secure.

V. Requirements of Video Watermarking

In order to be an efficient part of a reliable and secure image or video Copyright Protection system, a watermarking Algorithm must fulfill the following requirements

1. It must have low cross-correlation with image content.

2. The watermark has to be Secure so it's important to embed different watermark on each scene.

3. The extraction detection of watermark approach should can be blind i.e. It should be possible to extract and recover the watermark without the use of the original image and the video.

4. The watermark has to be perceptually invisible if the frame is dropped from the video and should not degrade the image or video quality.

5. The watermark detection must be reliable and robust, with no false detection and if possible no false rejection.

6. The watermark has to resist framing averaging, frame dropping collusion, cryptographic and removal attacks and other intentional watermark destruction attacks such as the jitter attack or statistical averaging attack.

7. The watermark should resist to different video compression schemes as well as to recompression in a different format.

.

8. There should be low cross-correlation between rows and between columns & between rows and columns.

9. Array diversity should be maintained.

10. It should have proper balance.

11 There should be compatibility with standard image transmission format such as JPEG, AVI.

12 It should take long span of time in order to prevent unauthorized cracking.

VI. **Strategies or Remedies for handling Attacks on Watermark**

A Video signal is a sequence of images. A point in a video is identified by its position (two-dimensional)and by the time at which it occurs, so a video signal has a three dimensional domain whereas analog video has one continuous domain dimension(across a scan-line)and two discrete dimensions(frame and line). Successive video frames are highly correlated, an attacker can exploit this to estimate and remove a watermark .The techniques for compressing video do not necessarily encode each frame of the sequence identically. The synchronization of the audio with the video sequence may be a consideration for watermark protection

There are different strategies for handling attacks on different watermarks:

1. Constant offset can be added for handling the attacks on the host image.
2. Some kind of Gaussians or non Gaussian noise can be added.
3. Linear Filtering, low pass or high pass filtering, non linear filtering can be applied.
4. Different compression schemes can be accounted. for e.g. by hybrid coding schemes like Mpeg or H.263
5. There should be local exchange of pixels (permutation of 2*2 pixels)
6. The grey values of pixels should be sampled and quantized.
7. Rotation and spatial scaling of the video frames can be done.
8. Removal or insertion of single pixels or pixels in rows and columns.
9. The averaging of the frames can be taken so as to measure the statistical probability with several versions of the same video with different embedded watermarks.

VII. **Conclusion**

From this review paper it can be concluded that there is a lot of difference between image and video, Images can be considered as still pictures and named as **Joint picture Expert group**, where as video can be taken as group of frames and named as **Motion Picture Expert group**. In the case of images they are more susceptible to attacks like, Cropping, Scaling, Translation, whereas in the case of video they are more prone to attacks like Frame- averaging, Frame-dropping, Forgery, Active and Passive attacks, Low error probability, and Statistical analysis. Similar to that it is very easy to embed the watermark in images as compared to video, because video is moving. At last it can be said that it is an effective measure for the copyright protection, as people are becoming more addicted of internet and multimedia so we can save and protect our data through the schemes like **Watermarking.**

VII. **References**

[1]Deepak Sharma, “Classification of Image Watermarking Schemes”

[2]Frederic Degguilaume, Gabreila Cburka, Joseph O’Runaidh Thierry Pun, “Robust 3 D DFT video watermarking”

[3] Saraju P. Mohanty □ Dept of Comp Sc and Eng. Unversity of South Florida Tampa, FL 33620 smohanty@csee.usf.edu “Digital Watermarking: A Tutorial Review”

[4] Edward J. Delp Purdue University School of Electrical and Computer Engineering Purdue Multimedia Testbed Video and Image Processing Laboratory (*VIPER)*, “Scene Adaptive Video Watermarking”

[5] Vivek Kumar Agrawal” Perceptual Watermarking of Digital video using the variable temporal length 3D-DCT”

[6]Xin Li, Yonatan Shoshan, Alexander Fish, Graham Jullien, Orly Yadid-Pecht, “Hardware implementation of video watermarking”

[7] Anatol.Z.Tirkel (Senior Member), Charles F Osborne,” Image watermarking –“A Spread Spectum application”