International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue 5 pp 120-123 August 2012 www.ijsret.org ISSN 2278 - 0882

DIGITAL IMAGE WATERMARKING

[1]Kirtika Goel, [2]Akhil Kaushik, [3]Achal Agarwal, [4]Sakshi Goel
[1](Student of M. Tech, CSE Department, NIMS University, Jaipur, Rajasthan
Email: Kirtikagoel_88@yahoo.co.in, kirtika.goel@gmail.com)
[2](CSE Department, SIT Meerut, UP
Email: akhil.cse.07@gmail.com)
[3](CSE Department, Teerthankar Mahaveer University, Moradabad, UP
Email: achalagarwal3@gmail.com)
[4](CSE Department, IIMT Meerut, UP
Email: sakshi.kur15@gmail.com)

ABSTRACT
In the past, duplicating art work was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights, artists of today can watermark their work by hiding their name within the image. Hence, the embedded watermark permits identification of the owner of the work. The aim of this paper is to make review of Digital Watermarking.

Keywords: *Watermark, Embedded, Metadata, Cryptography*

1. INTRODUCTION
Digital Watermarking is the technique used by researchers to hide user defined information along with important information that may be visible or invisible depending upon the requirements of the user. Now Digital Watermarking is concerned with the ownership of the information. Absence of Digital Watermark in the information results in loss of revenue. The Digital Watermark packed with the information should be inseparable.

A digital watermark is digital data that can be embedded into all forms of media content, including digital images, audio, video and even certain objects. Special software is available for embedding imperceptible information via subtle changes to the data of the original digital content. Digital watermarks can be easily detected and read by computers, networks and a variety of digital devices, validating the original content and/or initiating actions.

2. WHAT IS WATERMARK
A watermark is a visible embedded overlay on a digital photo consisting of text, a logo, or a copyright notice. The purpose of a watermark is to identify the work and discourage its unauthorized use. Though a visible watermark can't prevent unauthorized use, it makes it more difficult for those who may want to claim someone else's photo or art work as their own.

3. STRUCTURE OF A DIGITAL WATERMARK
The structure of a digital watermark is shown in the following figures.

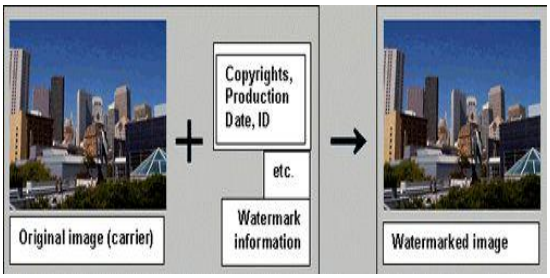

Fig 1: Applying Watermark on the Image

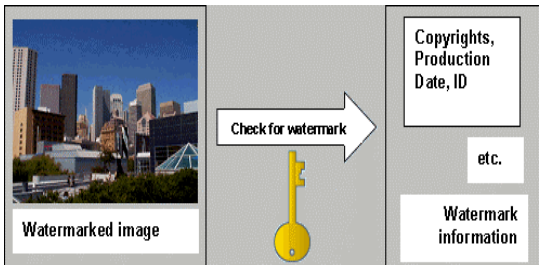

Fig: 2 Detection of Watermark

The material that contains a digital watermark is called a carrier. A digital watermark is not provided as a separate

file or a link. It is information that is directly embedded in the carrier file. Therefore, the digital watermark cannot be identified by simply viewing the carrier image containing it.

4. GENERAL FEATURES REQUIRED FOR DIGITAL WATERMARKS

a. Elements of digital content can be directly manipulated and information can be embedded in them.

b. Deterioration of the quality of digital content is minimized.

c. Watermarks are retained and detectable after the digital content is edited, compressed, or converted.

d. The structure of a watermark makes it difficult to detect or overwrite (alter) the embedded information (watermark contents).

e. Processing required for watermarking and detection is simple.

f. Embedded watermark information cannot be eliminated without diminishing the quality of the digital content that carries the watermark.

g. The watermark information embedded in digital content can be detected as required.

5. CLASSIFICATIONS OF DIGITAL IMAGE WATERMARKING

Digital image watermarking can be divided into two main groups – *visible* and *invisible* watermarks.

5.1. Visible Watermarks

A visible watermark, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. It is a visible semi-transparent text or image overlaid on the original image. It allows the original image to be viewed, but it still provides copyright protection by marking the image as its owner's property. *Visible* watermarks are more robust against image transformation. Thus they are preferable for strong copyright protection of intellectual property that's in digital format.

5.2. Invisible Watermarks

Invisible watermark information is added as digital data to audio, picture or video. An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. While some file formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself. Invisible watermarks are used to mark a specialized digital content (text, images or even audio content) to prove its authenticity.

S No.	Purpose	Invisible Watermark	Visible Watermark
1	Validation of intended recipient	Primary	–
2	Non repudiable transmission	Primary	–
3	Theft Deterrence	Primary	Primary
4	Reducing commercial value but not utility	Primary	Secondary
5	Discouragement of unauthorized duplication	Primary	Secondary
6	Digital notarization and authentication	Secondary	Primary
7	Discouragement of analog duplication	Primary	–

Table 1. Comparison of visible and invisible watermarks.

6. CHARACTERISTICS OF DIGITAL WATERMARK

6.1. Robustness

The watermark should be able to withstand after normal signal processing operations such as image cropping, transformation, compression etc.

6.2. Imperceptibility

The watermarked image should look like same as the original image to the normal eye. The viewer cannot detect that watermark is embedded in it.

6.3. Security

An unauthorized person cannot detect, retrieve or modify the embedded watermark.

7. CONTRIBUTED AREA IN DIGITAL WATERMARKING

The areas that contribute to the development of digital watermarking include at the very least the following:

a) Information and Communication Theory
b) Decision and Detection Theory
c) Signal Processing
d) Cryptography and Cryptographic Protocols

Each of these areas deals with a particular aspect of the digital watermarking problem.

Generally speaking, information and communication theoretic methods deal with the data embedding (encoder) side of the problem. For example, information theoretic methods are useful in the computation of the amount of data that can be embedded in a given signal subject to various constraints such as peak power (square of the amplitude) of the embedded data or the embedding induced distortion. The host signal can be treated as a communication channel and various operations such as compression / decompression, filtering etc. can be treated as noise. Using this framework, many results from classical information theory can be and indeed have been successfully applied to compute the data embedding capacity of a signal.

8. SCOPE OF DIGITAL WATERMARKING

The watermarking system can localize the portions of image that have been tampered maliciously, with high accuracy. In particular, the watermarking scheme is very sensitive to any texture alteration in the watermarked images, which is crucial for crime scene image authentication. Simulation results are presented to demonstrate the effectiveness of the proposed method and its possible applications in the field of crime scene analysis. The proposed method of watermarking authentication could potentially prove useful when digital photographs are presented as evidence in the court of law Digital Watermarking can be used for a wide range of applications such as:

a) Copyright protection
b) Fingerprinting(Different recipients get differently watermarked content)
c) Broadcast Monitoring (Television news often contains watermarked video from international agencies)
d) Covert Communication

9. APPLICATION OF DIGITAL WATERMARKING

Digital watermarking has been broadly and very successfully applied in lots of media objects across a wide range of applications. In this section we have mention some applications of digital watermarking in both traditional and novel areas. Fig.3 is the basic workflow of digital watermarking.

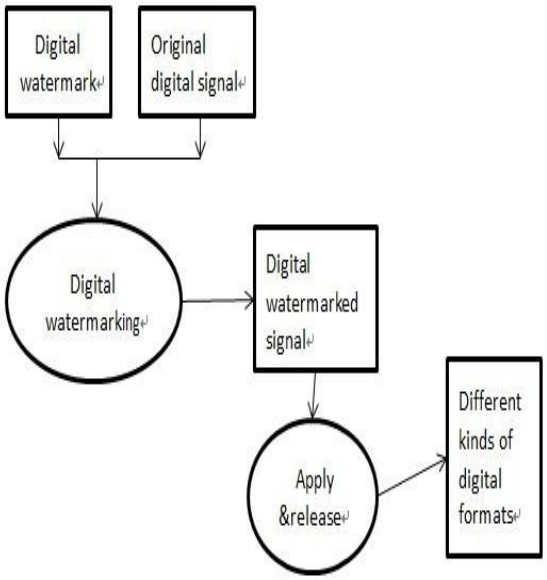

Fig.3 workflow of digital watermarking Application

9.1. Application of watermarking in traditional area

9.1.1 Ownership and copyrights

Digital watermarking can ensure our ownership and contact information are attached to our content, and can add automated licensing to increase revenues, automated remind us when there is an unauthorized use.

9.1.2 Document and image security

Using digital watermarking, it is easy to trace back to the source when any information is leaked. Besides, companies can use software to add or detect digital watermarks, and even can use the devices with watermark detector. For instance, we can prevent someone from attempting to copy our security documents with watermarks by using a printer with watermark detector.

9.1.3 Protection for audio and video content
In global entertainment industry, piracy of music, film and video is a multi-billion dollar big problem. Digital watermarking can help limit the unauthorized copy and redistribute, it can provide an added layer of security to the content protection.

9.2. Application of watermarking in novel area

9.2.1 Locating content online
Using digital watermarking can help we get fair compensation for our content usage, make sure that the right content is used on the right sites at the right time, gather information by where and what are accessed, give us a warning when unauthorized usage is detected.

9.2.2 Rich media enhancement for mobile phones
Digital watermarking can help companies engage and retain more consumers, create brand preference and loyalty, bring traditional printed like newspaper and magazines to the Internet.

10. DETECTION OF WATERMARKS

The first step in the determination of whether a stamp has a particular watermark is to remove any hinges or other foreign particles (please consult an experienced collector about removing hinges and foreign matter, many a stamp has been damaged by the careless removal of such), gently place the stamp in your tongs and hold it against a strong light source face forward at various angles, being careful not to damage the stamp from the heat of the light source. Often the watermark will come into view, particularly if the watermark is in an area that is not inked. Stamps with a large margin or selvage are prime candidates for this. You have probably seen a photo or scan of a block of stamps where the watermark is clearly visible in the selvage. You should also be aware of abnormalities in the stamp itself: thins, creases, tears, lines in the gum, a heavy cancel, heavy ink or lack thereof, and make a note of where on the stamp these abnormalities occur in order that you not confuse them with a watermark when using a technique outlined below.

The importance of viewing the stamp from many angles cannot be over-emphasized. This applies to any method described in this article. If the watermark does not come into view when held to a strong light, the stamp should be dipped in fluid, preferably face down.

11. CONCLUSIONS

Digital watermarking is a rapidly evolving area of research and development. We only discuss the key problems in this area and presented some known solutions in this chapter. One key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio.

Another key problem is the development of semi-fragile authentication techniques. The solution to this problem will require application of known results and development of new results in the fields of information and coding theory, adaptive signal processing, game theory, statistical decision theory, and cryptography. Although a lot of progress has already been made, there still remain many open issues that need attention before this area becomes mature.

REFERENCE

[1] R. Chandramouli. Data hiding capacity in the presence of an imperfectly known channel. Proc.SPIE Security and Watermarking of Multimedia Contents III, 2001.
[2] R. Chandramouli. Watermarking capacity in the presence of multiple watermarks and partially known channel. Proc. of SPIE Multimedia Systems and Applications IV, 4518, Aug. 2001.
[3] Ehsan Syed; "Final Report of Digital Watermarking"; University of Texas at Arlington; 2011;
[4]http://www.ee.uta.edu/Dip/Courses/EE5359/2011SpringFinalReportPPT/Syed_EE5359Spring2011FinalPPT.pdf
[5] Franklin Rajkumar.V, Manekandan.GRS, V.Santhi; "Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique"; International Journal of Computer Applications; Number 9 - Article 4; Date:2011;http://www.ijcaonline.org/volume12/number9/pxc3872293.pdf