ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 2 Issue 3; July-August-2015; Page No.01-04

A Review on Digital Watermarking For Copyright Protection of Digital Data

Reeta Chainani[1], Prof (Dr) Harsh Sadawarti[2], Member IEEE, G.S. Kalra[3], Member IEEE

[1]*M.Tech (CSE) student, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan*

[2]*Director at RIMT Institute of Engineering and Technology, Punjab, India*

ARTICLE INFO

Received: 10 May 2015
Accepted 28 June 2015

Corresponding Author:

Reeta Chainani

[1]*M.Tech (CSE) student, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan*

Email: reetachainani@gmail.com

ABSTRACT

In the present position of global networking, we want to protect our digital contents i.e. audios, videos, pictures and texts from unauthorized copying. For this reason, Digital Image watermarking Techniques have been developed to the copyright protection of digital data from illegal modification and reproduction. It is used in various areas like broadcast monitoring, copyright protection and also for owner identification. This paper highlights the basic model of Digital watermarking including its types and applications and also about various attacks on watermarked images. In this paper we also discussed about two methods i. e spatial domain and frequency domain.

Keywords: Watermarking images, Audios, Videos, Texts, Frequency domain, DCT, DWT.

1. Introduction-

Digital Watermarking is a process of embedding information into a digital signal in a way that is difficult to remove, these signal may be images, texts, videos and audios. At the same time different watermarks can be applied on a signal. Without altering the file digital watermarking is embedded the information within any multimedia object. The main purpose of digital watermarking is for copyright protection of multimedia data from being misused. Through digital watermarking we can identify the prohibited copies of digital media and also the authentication of owner. Digital Watermarking is created by inserting a digital pattern into digital content or data. It is nothing but the process of assigning information by invisibly embedding it into digital media or multimedia object. Digital Watermarking is not only used for owner identification or copyright protection but it is also used to determine whether the data is changed from its original form or not.

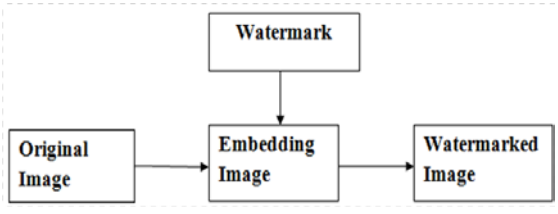

Figure 1:

Digital contents consists images, audio clips, videos but due to some delimit they become inefficient to use. **These delimit are** – Illegal copying, duplication, no copyright protection and no ownership authentication.

2. Characteristics of Digital Watermarking:

Robustness – Digital watermark should be robust for different attacks through which it may difficult to remove. Embedded watermark should not be eliminated by illegal distributors.

Fidelity – The watermark should not be visible in a watermarked image/video because if it is introduced then it reduces the commercial rate of digital object/data. And the digital watermarked should not affect the quality of the original data after it is watermarked.

Data Payload – Data payload represents the number of bits embedded into the digital content as which watermarked successfully detect during extraction process. For representing the uniqueness of the digital data watermark should be able to carry a sufficient amount of information.

Security – The information of watermark itself is a unique correct sign to identify only the authorized user can found it, extract it and even modify the watermark. The watermarking procedure is rely on secret keys so that pirates could not remove or detect the watermark

from a set of images/files or any digital contents even he/she knows the secret key which control the embedding procedure.

3. Some application of Digital Watermarking are:

- Ownership Protection
- Broadcast Monitoring
- Temper Detection
- Content Description
- Copyright Protection
- Digital Fingerprinting
- Medical Application
- Data hiding
- Convert Communication
- Encoding

4. Types of Digital Watermarking:

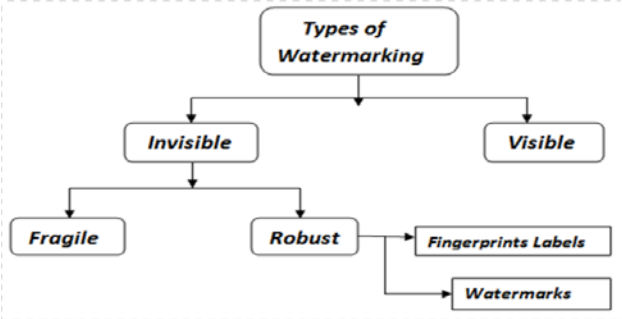

Figure 2:

4.1 Visible Watermark:

A Visible Watermark is accurately a text or a logo that clearly identify its copyright and the owner of the digital image. For "Copyright Protection" of image or video files we can use visible watermark. In visible watermark, ownership mark will be visually noticeable on the image but it does not stop the image being used for other purpose. So that the images are available on the internet and it will be used commercially without expense of royalty and the content owner desires to indicate the ownership of the primary material.

Requirements of Visible Watermarking:

- **Perceptibility of host image details -** Contents should not be rendered useless after being visibly watermarked.
- **Visibility of watermarked patterns in embedded contents -** No explicit watermark techniques are required.
- **Robustness -** Difficult to remove unless exhaustive and expensive human intervention is involved.

A General Model of Visible Watermarking-

$$I' = K_1 * I + K_2 * W$$

$$D(E_I(I'), E_I(I)) < Thershold_I$$

$$D(E_W(W'), E_w(W)) < Thershold_W$$

I'= the watermarked content

I = the un-watermarked original content

W = the watermark pattern

K_i = the weighting factor

D = a distance function measuring the perceptual difference of its two parameters

$Thershold_I$ = the largest allowable distortion of image details that observers can tolerate and, the same time, the signature of can be maintained.

$Thershold_W$ = the largest allowable distortion of the embedded watermark pattern that the copyright information can be clearly recognized.

4.2 Invisible Watermarking:

In invisible watermarking, information is embedded as digital data to image, audio clips or video but it cannot be apparent.

Invisible Robust Watermarking – Robust watermarking is mainly used for copyright protection and to detect misappropriate images.

Invisible Fragile Watermarking – Fragile watermarking is mainly embedded into the image for image verification and it is used to detect if the alteration of image stored in digital library.

5. Attacks on Watermarking:

5.1 Geometric Attack – These attacks may include cropping, wrapping, scaling, rotation, translation etc to destroy the synchronization of detection. Geometric attack manipulate the watermark in a manner that detector cannot discover the watermarked data. Mosaic attack is an example of geometric attack in which the watermarked image is divided into numerous parts and then rearranged using the appropriate coding of HTML and constructing watermark through which detector will fail to provide the desired outcome.

5.2 Removal & Interference Attack – Without cracking the security of watermarked algorithm, removal attack completely remove the watermark information from watermarked data. In some cases these methods are not always achieve their goal of removing watermark but they may nonetheless damage the watermark information extensively. These categories contain collision attacks, quantization and demodulation.

5.3 Cryptographic Attack – Find out the secret watermarking key by using exhaustive brute force method is known as cryptographic attack. Removal and Geometric attack do not break the security of the watermarking algorithm whereas the cryptographic attack deals with the cracking of the security.

5.4 Disabling Attack – The main goal of this attack is to split the association between the watermarks and cover image.

5.5 Ambiguity Attack – This attack is used to embedded a fake watermark in the place of original embedded mark. The main goal of this attack is to confuse the receptor.

6. Different Techniques of Digital Watermarking:

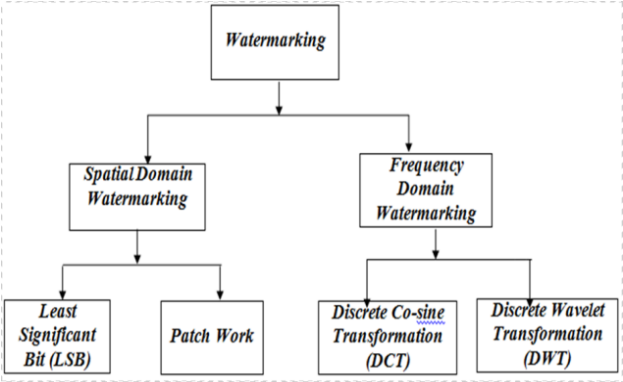

Figure 3:

6.1 Spatial Domain Watermarking:

In this technique, the watermark is inserted in the cover image altering pixels. The algorithm should be carefully weighing the changes of bits in the pixels against the chance of watermark becoming visible. Some of the Spatial Technique of watermarking are:

Least Significant Bit (LSB) – Earlier in this method digital image watermarking schemes embedded watermarks in the least significant bit of the pixels. Each pixel being represented by an 8-bit series and the watermarks are implanted in the last bit of the selected pixel of the image. This method is not very robust against attacks also it is easy to execute and does not produce any grave distortion to the image.

SSM-Modulation Based Technique – In this method energy generated one or more discrete frequencies are deliberately spread in time. This is done by variety of reason like growing resistance of natural interference and jamming, also with the establishment of secure communication. SSM based watermarking algorithm insert information by linearly combining the host image with a small simulated noise signal that is modulated by the embedded watermark.

6.2 Frequency Domain Watermarking:

Frequency domain watermarking is more widely used as compared to spatial domain watermarking. The main aim of this method is to embed the watermark in the spectral coefficient of the image because the human visual system (HVS) is better captured by spectral coefficient. Human visual system is more sensitive to low frequency coefficient and less sensitive to high frequency coefficient. Low frequency are perceptually coefficient which means the modification of components might cause severe distortion to the original image whereas high frequency coefficient are measured insignificant thus processing technique tend to eliminate high frequency coefficients aggressively. In Frequency domain watermarking the most commonly used transforms are Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

Discrete Cosine Transform(DCT) – This technique are robust as compared to spatial domain technique and also against simple image processing operations like low pass filtering, contrast adjustment, blurring and brightness etc. They are difficult to implement and computationally more expensive and at the same time they are also weak against geometric attack like rotation, cropping, scaling etc. Embedding in the perceptual significant portion of the image has its own advantage because most processing techniques such as compression remove the perceptually insignificant portion of the image.

Discrete Wavelet Transform (DWT) – This technique is extensively used in the signal processing application such as in audio & video compression, removal of noise and simulation of wireless antenna distribution. Wavelet Transform suited for the analysis of transient and time-varying signals.

7. Conclusion:

The incredible demand of networked multimedia system has created the need of "Copyright Protection" for the safety communication issue of digital data. Internet playing an important role of digital data transfer. In this paper a clear overview of watermarking concept is provided, we discussed the types of watermarking. Next it mentioned the possible attacks on the Digital Image Watermarking. Finally, discussed the different domains of Digital Watermarking technique.

References:

1. G.S Kalra, Dr. R.Talwar, Dr. H.Sadawarti, "Protecting Copyright Multimedia Files by Means of Digital Watermarking: A Review" *5th IEEE International Conference on Advanced Computing and Communication Technologies [ICACCT-2011] ISBN 81-8788503-3.* http://www.apiit.edu.in/downloads/all%20chapters/CHAPTER-55.pdf
2. Prachi khanzode, Siddharth Ladhake, Shreya Tank, "Digital Watermarking for Protection of Intellectual Property", *International Journal of Computational Engineering and Management, Vol 12, April 2011,ISSN(Online): 2230-7893.* http://www.ijcem.org /papers42011/42011_03.pdf
3. Jobenjit Singh Chahal, Shivani Khurana,"A Review on Digital Image Watermarking", *International Journal of Emerging Technology and Advanced Engineering, Vol 3, Issue 12, December 2013.* http://www.ijetae.com/files/Volume3Issue12/IJETAE_1213_87.pdf
4. D.G.Rindhe, Dr.G.S.Sable,"A Review of Digital Watermarking", *International Journal of Application or Innovation in Engineering and Management, Vol 2, Issue 5, May 2013.* http://www.ijaiem.org/Volume2Issue5/IJAIEM-2013-05-15-023.pdf

5. R. Chandramouli, Nassir Memon, Majid Rabbani, "Digital Watermarking". http://www.vis.uky.edu/~cheung/courses/ee639_fall04/readings/intro_watermark.pdf

6. Shradha S.Katariya (Patni),"Digital Watermarking: Review", *International Journal of Engineering and Innovative Technology, Vol 1, Issue 2, February 2012.* http://ijeit.com/vol%201/Issue%202/IJEIT1412201202_26.pdf

7. Vinita Gupta, Mr. Atul Barve, "A Review on Image Watermarking and Its Technique" *International Journal of Advanced Research in computer Science and Software Engineering, Vol 4, Issue 1, January 2014.* http://www.ijarcsse.com/docs/papers/Volume_4/1_January2014/V4I1-0117.pdf

8. Frank Hurtang, Martin Kutter (Member IEEE). "Multimedia Watermarking Technique". http://ir.nmu.org.ua/bitstream/handle/123456789/125543/fd64612ffc44edfebfe990dc194bd41f.pdf?sequence=1