International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 08 | Aug-2016 www.irjet.net p-ISSN: 2395-0072

Review on Digital Watermarking

Sarita[1], Sudesh Nandal[2]
[1] *Student, Department of Electronics and Communication Engineering, B.P.S.M.V, Khanpur Kalan, Sonipat (Haryana), India*
[2] *Assistant Professor, Department of Electronics and Communication Engineering, B.P.S.M.V, Khanpur Kalan, Sonipat (Haryana), India*

ABSTRACT - *Today is the time of digitization. Digitization has its own boon or bane. On one hand digitization makes our work simple, easy and less time consuming, On the other hand security of the digital data become a serious issue. Digital watermarking hides the secret data into the cover image and provide authentication and security to the digital data. This paper includes the study of the various watermarking techniques, its properties, attacks on the watermark and application. Different parameters for evaluation of various watermarking techniques are also discussed. Our main focus is on image watermarking.*

Key words: Watermarking, Working, Classification, Attacks, Application, Parameters

1. INTRODUCTION

Digital watermarking is the technique through which security, authentication and copyright protection is provided to the digital data. Watermarking is used since thirteenth century. It was firstly used to differentiate one brand to other in the form of brand logo which was visible. Now invisible watermark are use for security purpose. The invisible watermark is not visible to the human visual system.

Digital watermarking is a process of embedding the secret information either a text or image into a host image by making some modification in its pixel values. It is use for the copyright protection, data authentication, fingerprinting, broadcast monitoring, digital right management and many more.

2. DIGITAL WATERMARKING WORKING

Digital image watermarking technique is carried into three steps and these are as follows

- Embedding
- Noise / attack
- Detection

2.1 Embedding

It is the starting stage of the watermarking process. In this the water mark is embed into the cover image by using specific algorithm and key. Watermarked image is the output of this stage and it is ready to transmit over the communication channel.

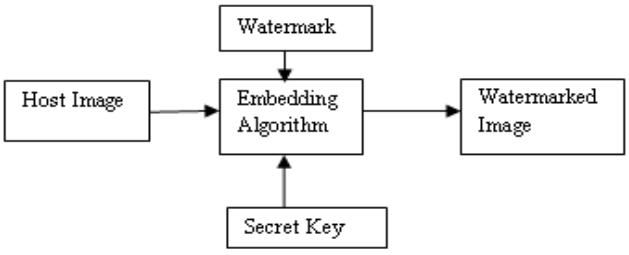

Fig - 1: Embedding process

2.2 Noise And Attack

When the watermarked image is transferred over the channel, some noise may add to the watermarked image. Attacks or noise added due to transferring the watermarked image will alter the watermarked image.

2.3 Detection

In this step watermark is retrieved from the watermarked image by using some detecting algorithm and/or secret key

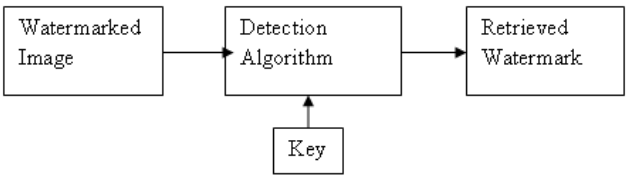

Fig -2: Detection Process

3. TYPES OF DIGITAL WATERMARKING

Digital watermarking techniques are classified into number of groups according to the application

3.1 Visible and Invisible Watermarking

Digital watermarking in which the embedded data is visible to the human through naked eyes is known as the visible watermarking where as in the invisible watermarking the embedded data is not visible through naked eyes. Example of visible watermarking is logo or digital signature which can be easily seen by humans [1]

3.2 Fragile and Robust Watermarking

In the fragile watermarking a slight change in watermark distorts the original watermark and the distortion can be easily detected by comparing the original and distorted watermark. Data manipulation can distort the fragile watermark. Robust watermark are not easy to remove from the host image in which it is embedded [2].

3.3 Private and Public Watermarking

In the private watermarking scheme requires host image to recover the watermark, where as in the public watermarking technique does not require host image and embedded watermark to recover the watermark.

3.4 Blind, Non-Blind and Semi Blind Watermarking

On the basis of watermark detection it is categorized into non-blind, semi blind and blind. In the non blind, secret key and the original image both are needed for the extraction. For the semi blind, secret key with the bit sequence of the watermark is used for extraction. And in the blind watermarking scheme only secret key is needed.

TABLE -1: WATERMARK TECHNIQUES CLASSIFICATION

S.No.	Watermarking Technique	Classification
1.	Data	▪ Video ▪ Audio ▪ Text ▪ Image
2.	Human Perception	▪ Visible ▪ Non Visible
3.	Extraction Of Data	▪ Blind ▪ Semi Blind ▪ Non Blind
4.	Watermark Insertion	▪ Noise(Gaussian, Pseudo And Chaotic) ▪ Image Format(Logo, Label Or Binary Image)
5.	Robustness	▪ Fragile ▪ Semi Fragile ▪ Robust
6.	Processing	▪ Spatial Domain(Pixel, Block) ▪ Frequency Domain(DCT,DFT,DWT)

3.5 Spatial Domain Watermarking

In this watermarking, the watermark is embedded directly into the host image no image transformation needs to be performed. In this technique the watermark is embedded by changing the intensity of some specific pixels [3]. This technique is very simple and applicable to all images. Types of spatial domain watermarking are as follow

- Patch Work Based Watermarking
- Correlation Based Watermarking
- Additive Watermarking
- SSM Based Watermarking
- Least Significant Bit Watermarking

3.6 Transform Domain Watermarking

In this method the host image is first converted into the frequency domain and then the watermark is embedded into the transformed coefficients. This method is more successful as compared to the spatial domain watermarking.

Type of transform domain watermarking

- DCT- Discrete Cosine Transform
- DWT- Discrete Wavelet Transform
- DFT- Discrete Fourier Transform

4. REQUIREMENTS OF DIGITAL WATERMARKING

For the better watermarking technique it is important that it should fulfill certain characteristic or properties and these are as follows:

4.1 Security

For security purpose digital watermarking is used as this technique provides high security to the watermark or we can say that it should be difficult to remove the watermark from the cover image without damaging it [4].

4.2 Cost

The cost of designing and implementation of the watermarking technique should not be so high so that it will not create any Burdon on the originator. The inserting and extracting algorithm should be run at high speed

4.3 Imperceptible

Watermarked and the cover image/ signal should not have any perceptible difference[5] So the watermark should be added to that part of the image which is perceptually not important or insignificant [6].

4.4 Robustness

It refers to the ability of the watermark to exist in various manipulations. Watermark should be withstood with the different processing operations. Robustness should be provided against the various attacks like noise addition, transformation etc [7].

4.5 Capacity

It is refer to the amount of watermark information that can be easily store in the cover image. Security, imperceptible and capacity has mutual relation. For high capacity, other two factors will degrade.

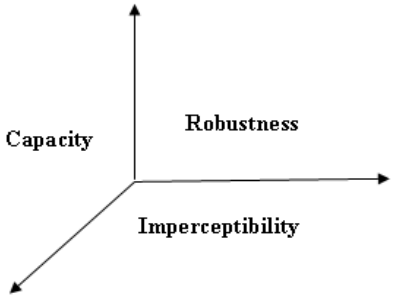

Fig -3: Relations between Capacity, Robustness and Imperceptibility

4.6 Invisibility

The watermark should be invisible to the human through the naked eyes.

Table -2: Comparison of Spatial Domain and Frequency Domain Watermarking

Factor	Spatial Domain	Freqency Domain
Computation cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Computational Complexity	Low	High
Computational Time	Less	High
Capacity	High	Low
Application	Authentication	Copy Right

5. ATTACKS

Attacks on watermark are broadly classified into two groups one is accidental attack and other is intentional attack. Accidental attacks are those which occur due to the image processing like compressing, enhancing, transforming etc where as intentional attacks are those which are performed for overwriting or removing the watermark. Various types of attacks are as follows:

5.1 Mosaic Attack

It is for confusing the watermark searching program. In this original image is divided into small images of random size and then display the resulted image on the Web.

5.2 Geometric Attack

This is due to the geometric change of the data and this can be done by flipping, rotating and cropping.

5.3 Forgery Attack

Attacker adds his/ her own watermark over the existing watermark and makes the data as their own data [8].

5.4 Cryptographic Attack

In this type of attack, attackers try to find the decryption key so that the watermark can be remove from the data [9]

6. APPLICATIONS OF DIGITAL WATERMARKING

6.1 Ownership claim

Watermark technique is use for claiming the ownership, for this the watermark is generated by using the secret key and then it is embedded into the original image and this watermarked image is available to the people [10]. If other person claims on it then the owner can produce the unmarked image instead of other person and can assert the ownership.

6.2 Fingerprinting

To save the digital content from the unauthorized person from misuse, the data must be watermarked. The watermark should be present in every replica of the data. If unauthorized replica of the data found then by using the fingerprint (watermark) origin can be found.

6.3 Prevent Replica Formation

It means that the watermark is inserted which indicate how many copies of it can be made. Digital content is copied through the specific hardware, when copy of the data is made then the hardware modified the watermark a little and after a limit the hardware would not able to made any replica of the content. Example DVD (digital versatile disc).

7. PARAMETER FOR EVALUATION

Different parameters are used to evaluate the watermarked image. These are as follows

- MSE
- PSNR
- Cross-correlation

MSE stands for the mean square error; it is the error matrix which is used to calculate the quality of the image [11]. It is calculated as

$$MSE = \frac{1}{ab}\sum_{i=0}^{a-1}\sum_{j=0}^{b-1}[X(i,j) - Y(i.j)]^2 \quad \text{(i)}$$

X(i,j) —Y(i,j) represent the error between the original and the compressed image.

Lower the value of MSE higher is the similarity between the original and the compressed image and vice-versa

PSNR (Peak Signal To Noise Ratio); it is used to calculate the difference in quality of the original image and the compressed image

$$PSNR = 10\log_{10}\frac{K^2}{MSE} \quad \text{(ii)}$$

Where K, represent the range of values of pixel.

Higher the value of PSNR greater is the similarity between the images. Typical values of PSNR is 30 to 50 dB

Cross-correlation is a measure of the two data series.

$$R_{xy} = \frac{\sum_x \sum_y (A_{xy} - \bar{A})(B_{xy} - \bar{B})}{\sqrt{\sum_x \sum_y \left((A_{xy} - \bar{A})\right)(B_{xy} - \bar{B})}} \quad \text{(iii)}$$

8. CONCLUSION

In this paper various concepts related to the digital watermarking have been studied like working, classification, Requirements, attacks and Applications of watermarking. A brief literature review of initial and recent work in this field is included. To evaluate the performance of different watermarking techniques parameters have been explained

We attempted to present the complete information about the digital watermarking so that new researchers will get the maximum information in this domain

9. REFRENCES

[1] Nidhi Rani "Digital Watermarking" , Global Journal Of Computer Science And Technology Graphics & Vision Volume 12 Issue 13 Version 1.0 Year 2012
[2] N. Chandrakar And J. Baggaa,"Performance Comparison Of Digital Image Watermarking Techniques: A Survey", International Journal Of Computer Application Technology And Research, Vol. 2, No. 2, (2013), pp. 126-130.
[3] De Li1 , Yingying Ji And Jongweon Kim "A Video Watermarking Scheme Based On 2d DWT And Pseudo 3D DCT" , International Conference On Information And Computer Applications, Vol. 24 , 2012 pp 147-150
[4] A. H. Tahernia, M. Jamzad, "A Robust Image Watermarking Using 2D DCT And Wavelet Packet Denoising ", International Conference On Availability, Reliability And Security, 2009, pp. 150-158, .
[5] C.-T. Li and F.M. Yang. "One-Dimensional Neighborhood Forming Strategy For Fragile Watermarking". In Journal Of Electronic Imaging, Vol. 12, No. 2,2003, pp. 284-291.
[6] C.-T. Li and F.M. Yang., "One-dimensional Neighborhood Forming Strategy for Fragile Watermarking" ,In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.
[7] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013
[8] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE "A Review of digital image watermarking in health care".
[9] C. Podilchuk And E. Delp. "Digital Watermarking Algorithms And Applications". In IEEE Signal Processing Magazine, Vol. 18, No. 4, July 2001.
[10] V. M. Potdar, S. Han And E. Chang, "A Survey Of Digital Image Watermarking Techniques", 3rd IEEE International Conference On Industrial Informatics (INDIN), 2005.
[11] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, "A Novel Technique for Digital Image Watermarking in Spatial Domain", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.