Digital Watermarking: Techniques, Applications, Attacks

[1]Mr. Rushit K Chokashi, [2]Gautam D. Makawana

[1]PG Scholar, [2]Assistant Professor
E&C Department, Sankalchand Patel College of Engineering, Visnagar
Gujarat Technology University, Gujarat, India.
[1]rushitc98@yahoo.co.in, [2]gdmakwana.ec@spcevng.ac.in

***Abstract*—Due to the rapid evolution in internet technology and high speed networks the use of digital data has been increased. Digital data such as audio, video and images are easily created, copied, processed, stored and distributed among the users. To ensure security and protection of digital data new technology has been developed called as a digital watermarking. Digital watermarking is a technology which embeds additional information in the host image to ensure security and protection of the digital data without effecting original data. The purpose of digital watermarking is not to restrict use of digital data but it can be provide copyright protection and authentication against unauthorized uses. In this paper detail study of watermarking definition, concept and the main contribution of watermarking process in which watermarking should be used, features, techniques, Application, challenges and performance metrics of watermarking and comparative analysis of watermarking techniques are included.**

Keywords-Digital Image Watermarking, Wavelet Transform, Discrete Cosine Transform, Attacks

I. INTRODUCTION

Digital Watermarking is defined as the process of imperceptibly hiding ownership information inside digital resource such as an image, audio or video. Digital media can be copied and modified easily so protecting the copyright of digital media has become an important task. Watermarking is used to make sure of the protection of the data. Watermarking is the process of bits inserted into digital image, audio or video which specify the copyright information of data, such as author, owner etc. the actual data which cannot be detected or tampered by unauthorized person. There are two common methods for watermarking: spatial domain and transform domain. In spatial domain pixels of an image are modified depending upon perceptual analysis of an image. But in transform domain some frequencies are selected and modified from their original values according to certain rules. The transform domain methods are more popular because watermark embedding is more robust in this domain as compared to spatial domain. It also provides more security and imperceptibility Perceptual transparency, security, capacity, robustness, verifiability of watermark are the important aspects or requirements for design of watermarking systems. Section 2 describe basic block diagram of digital image watermarking. Also discuss host image, noise, attack and watermark keys. Section 3 describes classification of Different types of digital watermarking system. Section 4 describes requirements of digital image watermarking system. Section 5 describes different types of digital watermarking techniques. Section 6 describes different types of digital image watermarking applications. Section 7 describes different types watermarking attacks. Section 8 describes performance analysis parameters of watermarking system.

II. DIGITAL WATERMARKING TECHNOLOGY

This mo Digital watermarking hides the copyright information into the digital data using different algorithms. The secrete information to be embedded can be some text, author's serial number, company logo, image with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection.[2] The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own advantages and disadvantages. Host image can be watermarked using message image. Also we can add secrete key to provide more secure watermarking. Capacity of the watermarking system is defined as the maximum amount of information that can be embedded in the cover work. The number of watermark bits in a message in data payload and the maximum repetition of data payload within an image is the watermark capacity. Simple digital watermarking system is shown in figure.

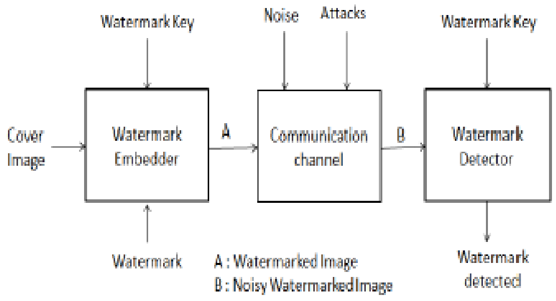

Figure: 01 Simplified Digital Watermarking System

III. CLASSIFICATION OF DIGITAL WATERMARKING

a) According to the types of the document

1. Text Watermarking
2. Image Watermarking
3. Audio Watermarking
4. Video Watermarking

b) According to the human perception

1. Visible Watermarking
2. Invisible Watermarking

c) According to Domain

1. Spatial Domain
2. Frequency Domain

d) According to the application

1. Source Based
2. Destination Based

IV. THE REQUIREMENT FOR WATERAMRKING

Following are the basic requirement to be taken into consideration while designing watermarking techniques.

a) *Imperceptibility:* One of the most important requirements is the visual transparency of the watermark. In some system the watermark need to be visible according to the requirement. But in the most of the application invisible watermarking techniques are preferred.

b) *Robustness:* Robust watermarking technique developed to provide the protection against any kind of alternation or intentional removal attacks by standard or other malicious attack. Secure watermark are designed to resist any kind of unauthorized attack .So, robustness is necessary property if a watermark is to be secure.

c) *Watermark keys:* A secret key has to be used for embedding and detecting purpose in the watermarking system. Mainly three types of keys are used in watermark system. A private key is available only to the author nobody can get this key without author's permission. The detection key is used when owner property authentication is required. The public key is the key which can be used by public and no need to get permission.

d) *Capacity:* In watermark system capacity should be high. If capacity of a data is high then more secure transmission is possible and more data can be transmitted.

V. WATERMARKING TECHNIQUES

a) Spatial domain

Least Significant Bit (LSB): In the spatial domain watermarking techniques embed the watermark by modifying the pixel vales of the host image. Least significant bit (LSB) technique is the most frequently used method in this domain. This technique is the most straight forward method and uses the entire cover image to store the watermark, which enables a smaller object to be embedded multiple times. They are robust against attacks like cropping, noise, lossy, compression. But an attack that is set on a pixel to pixel basis can fully uncover the watermark, which is the major drawback of the system. The main advantages of pixel based methods are that they are conceptually simple and have very low computational complexities and therefore are widely used in image and video watermarking where real-time performance is a primary concern.

b) Frequency domain

Discrete cosine transforms (DCT): DCT is a frequency domain based transforms techniques. It represents data in terms of frequency domain rather than an amplitude space as compare to Fourier transform.DCT based watermarking techniques are robust compared to spatial domain techniques.DCT based techniques provides robustness against low pass filtering, brightness and contrast adjustment ,blurring but they are difficult to implement and more expansive. DCT not provides robustness against geometric attacks like rotation, scaling and cropping. DCT domain classified into Global DCT watermarking and Block based DCT watermarking. [4] [8]

Discrete wavelet transform (DWT): Discrete wavelet transform is a frequency based transform technique which is widely used. In discrete wavelet transform images and video frames decomposes into sub images, 3details and 1 approximation. The approximation sub image is lower resolution called as LL band. And detail sub images are horizontal (HL), vertical (LH) and diagonal (HH) detail components. [6] The main advantage of the wavelet transform is its compatibility with a model aspect of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive, such as the high resolution detail bands. Embedding watermarks in these regions allow us to increase the robustness of our watermark without any visible impact on the image quality. Embedding the watermark in high frequency sub-bands makes the watermark more Imperceptible while embedding in low frequencies makes it more robust against a variety of attacks. Embedding watermark using wavelet transform provides robustness against attacks like filtering, lossy, compression and geometric distortions. [7]

TABLE: 01 COMPARISON BETWEEN SPATIAL DOMAIN AND FREQUENCY DOMAIN [1] [2]

Factors	**Spatial domain**	**Frequency Domain**
Computation Cost	Low	High
Robustness	Low	More Robust
Perceptual quality	High control	Low control
Computational Time	Less	Higher
Capacity	High	Low
Application	Mainly Authentication	Copy rights

TABLE: 02 COMPARISONS OF DIFFERENT WATERMARKING TECHNIQUES [1] [3] [4]

Algorithm	**Advantages**	**Disadvantages**
LSB(Least Significant Bit)	-Easy to implement -Low degradation of image quality -Highly perceptual transparency	-Less robustness -Not reliable to noise -Not reliable against cropping, scaling.
DCT (Discrete Cosine Transform)	-The watermark is embedded into the coefficient of the middle frequency, so the visibility of image will not get affected and watermark will not be removed by any kind of attack. -More robust as compare to LSB.	-Higher frequency component tend to be suppressed during the quantization. -Block wise DCT destroys the invariance properties of the system.
DWT (Discrete Wavelet Transform)	-Higher compression ratio which is relevant to human perception. -Allow good localization both in time and spatial frequency domain. -More Robust as compare to DCT and LSB	-Cost of computing may be higher. -Longer compression time. -Noise / Blur near edges of images.

VI. WATERMARKING APPLICATION

Main application of digital watermarking is the copyright protection and user authentication. But digital watermarking provides wide range of different application in the different field as explained below: [4] [8]

a) *Copyright protection:* To provide the protection against intellectual property rights. Owner can embed a watermark into his data which can represent copyright information in it. This watermark can help in the court to prove his ownership when someone has tried to use his data without prior permission of his copyright material.

b) *Fingerprinting:* To trace the distribution source of illegal copies, the owner can use a fingerprint technique. In this technique owner can add different watermarking information in the copies of the data that are supplied to different customers. Fingerprint can be compared to embedding serial number that is related to the customer's identity in the data. Using this technique owner can identify customer who can break their license agreement by supplying the data to third parties.

c) *Broadcast Monitoring:* By embedding watermarks in the commercial advertisements, an automated monitoring system can verify whether advertisements are broadcasted as per contracted. And also provides the protection of the protection against unauthorized content copy and actors can ensure that they can receive accurate royalties for their performance in the broadcasts.

d) *Data Authentication*: If in the transmission medium someone try to modify the content or tamper data watermark can be changed so from this change in watermark user can identify about the tampering. As a solution a fragile watermark technique is developed which provides the detection of whether the content of the digital data has changed.

e) *Covert Communication:* The watermark is also used as tool of sharing secrete information. Secret message can be embedded to the digital image or video to communicate information from the sender to the intended receiver. This application is widely used in military where always required secure medium to communicate the message.

f) *Medical application:* Embedding patient's name and date in the medical image like X-Ray and MRI scan so identify of the patient's detail easily.

VII. WATERMARKING ATTACKS

There are various possible attacks intentional or unintentional that affects the watermark object. For the robust system prevention of this kind of malicious attack is necessary. A brief introduction to various types of watermarking attacks is as under. [5]

a) *Interference attack:* Interference is produced due to addition of additional noise into the watermarked object which affects the watermark. Lossy compression, averaging, collusion, denoising, remodulation, quantization are some examples of interference attacks.

b) *Removal attack*: This kind of attack produced due to intention to remove the watermark data from the watermark object. These kinds of attack exploit the fact that the watermark is usually an additive noise signal present in the host signal.

c) *Geometric attack:* Rotation, cropping, flipping are called as geometric attacks. This can affect the geometry of the image. Geometric attacks should be detectable using frequency domain techniques and provides robustness against this kind of attacks.

d) *Security attack:* If an attacker known watermarking algorithm attacker can further try to perform modification into the watermark using invalid or estimate method. The watermarking technique consider as a secure if the embedded information cannot be destroyed, detected by the attacker.

e) *Cryptographic attacks:* If an unauthorized user tries to crack the security cryptography deals with this kind of attack. To find the secrete watermark attacker can try exhaustive burst force method is called as a cryptographic attack. These attacks are similar to the attacks used in cryptography.

VIII. PERFORMANCE EVOLUTION PARAMETERS

For evaluate the performance of the watermarked images, there are some measurement parameters such as SNR, PSNR, MSE and BER used.

The MSE (mean square error) is defined as average squared difference between a host image and distorted image. It is calculated by the formula given below

$$MSE = 1/XY\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}\big(c(i,j) - e(i,j)\big) \wedge 2\right]$$

Where, X and Y are respectively height and width of the image. The c (i, j) is the pixel value of the host image and e (i, j) is the pixel value of the embed image.

SNR (Signal to Noise ratio) measures the sensitivity of the imaging. The signal strength relative to the background noise is calculated by following formula

$$SNR(db) = 10\log_{10}(Psignal \,/\, Pnoise)$$

The PSNR (peak signal to noise ratio) is used to determine the degradation in the embedded image with respect to the host image. It is calculated by the formula as

$$PSNR = 10\log_{10}(L * L/MSE)$$

L is the peak signal value of the host image which is equal to 255 for 8 bit images.

The BER (bit error ratio) is the ratio that describes how many bits received in error over the number of the total bits received. It is calculated by comparing bit values of embed and cover image.

$$BER = P/(H * W)$$

Where and W are height and width of the watermarked image. P is the count number initialized to zero and it increments by one if there is any bit difference between host and embed image.

REFERENCES

[1] Mahomoud El-Gayyari-"Watermarking Techniques Spatial Domain Digital Rights Seminar@, Media Informatics, University of Bonn Germany.

[2] J Xuehuna-"Digital Watermarking and Its Application in Image Copyright Protectional, 2010 International Conference on Intelligent Computation Technology and Automation.

[3] A Kumar Singh, N Sharma , M dave , A Mohan –"A Novel Technique for Digital Image Watermarking in Spatial Domain,2012 2nd IEEE International Conference on Parallel Distributed and Grid Computing.

[4] P Singh, R Chadha-"A survey of Digital Watermarking Techniques, Applications and Attacks,2013 IJEIT Vol-2 Issue-9

[5] T jayamalar, V radha-"Survey on Digital Watermarking Techniques and Attacks On Watermarks,2010 IJEST Vol-2(12)

[6] N.I.Yassin,M. Salem, M.I.El Adawy"Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012

[7] Jim G. Bouridane, M.K.Ibrahim,"Digital Image watermarking Using Balanced Multi wavelets",IEEE Transaction on Signal Processing 54(4),2006

[8] B.Ram " Digital Image watermarking technique using DWT and DCT"International Jouurnal of Advancements in Research & Technology,vol.2, Issue-4, April 2013, ISSN: 2278-7763