Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Various Techniques, Classification, Attacks and Applications of Digital Image Watermarking

Manjeet Kaur
M.Tech (IT), Department of CSE/IT,
CDAC, Noida, India

Ramneet Singh Chadha
Asst. Professor, Department of CSE/IT,
CDAC, Noida, India

Abstract— Amount of data over the internet is increasing day by day due to rapid growth in technology,requirement for security of these data like audio, video, image, text are also increasing. Digital image watermarking is used for image authentication; copyright protection, image verification, its ownership detectionetc. This study will deals with various watermarking techniques,requirements,various attacks on it, applications, its classifications in the digital image watermarking.

Keywords— DWT, Transform Domain, Spatial Domain, DCT, DFT

I. INTRODUCTION

The rapid growth of the technology over the internet is increasing day by day. Resulting the availability of large amount of digital data over the internet. Security of these data like audio, video, text and image becomes a big issue. For security of these data various techniques are used digital watermarking is one of them. Digital Watermarking is a technique to embed the watermark and various information's into various signals. Watermark information will be present in form of image and text. They have various authentications, copyright information to determine the owner of digital data, authenticate user of data and integrity of data. Digital watermarking has many applications in certificate distribution, copyright protection, telemedicine etc.Watermarking is the subset of Steganography but different in many aspects. In Steganography, data which is hidden has no relationship with the cover data whereas the data which is hidden has relationship with the cover data. Cryptography provides many solutions but insufficient to provide safety in transfer and processing of image over the internet. Digital watermarking is the emerging technique for maintaining integrity and authentication of image .In embedding process watermark is embed into cover image and for extraction process watermark is extracted from image as shown in figures below.

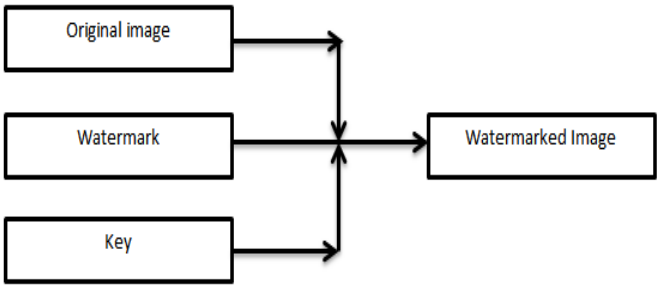

Fig.1. Watermark embedding process

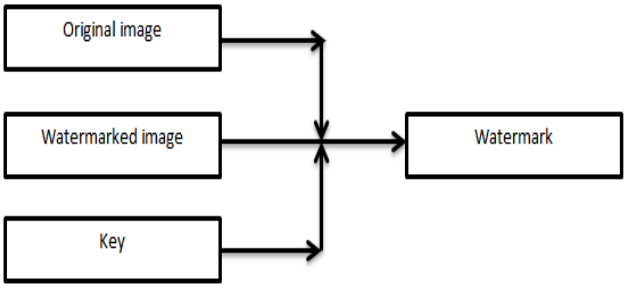

Fig.2. Watermark extraction process

II. REQUIREMENTS OF DIGITAL WATERMARKING

A. Robust: A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the watermarked signal, even if degraded by any number of transformations. Image degradations are rotation, scaling, JPEG compression, cropping, noising, and filtering. In video, there are temporal modifications and MPEG compression are present.

B. Imperceptible: A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original contents. A robust imperceptible watermark used as tool for the protection of digital multimedia contents.

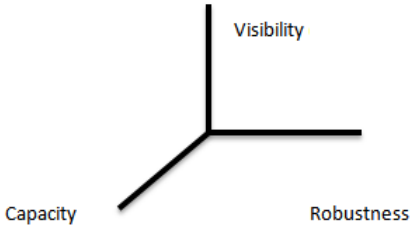

Fig.3.Requirement of digital watermarking

C.Capacity: Amount of data which is embedded into cover signals to successfully detection and extraction of watermark is determined by capacity.

III. CLASSIFICATION OFDIGITAL WATERMARKING TECHNIQUES

1. Based on human perception

Visible Watermark: These watermarks can be seen by the viewer and can also identify the logo or the owner. In the visible watermarking technique watermarked signal is different from the original signal

Invisible Watermark: These watermarks cannot be seen by the viewer. The output signal does not change much when compared to the original signal.

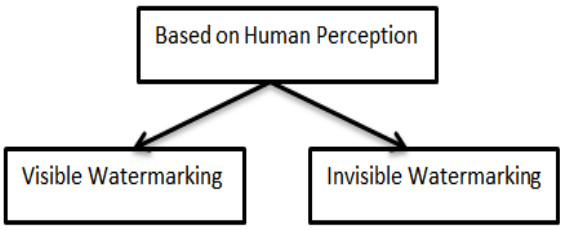

Fig. 4.Based on human perception

Fig. 5.Invisible and visible watermark

2. Based on Application point of view

Source Based: Watermark desirable for ownership identification or authentication.

Destination Based: It is used for trace the buyer.

3. Based on Robustness/Characteristics

Fragile watermarks: These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal as shown in figure multimedia authentication.

Semi-fragile watermarks: These watermarks are broken if the modifications to the watermarked signal exceed a pre-defined user threshold. If the threshold is set to zero, then it operates as a fragile watermark. This method can be used to ensure data integrity and also data authentication [Bender et al (1996)].

Robust watermarks: These watermarks cannot be broken easily as they withstand many signal processing attacks. Robust watermark should remain intact permanently in the embedded signal such that attempts to remove or destroy the robust watermark will degrade or even may destroy the quality of the image. This method can be used to ensure copyright protection of the signal. It can be used in different applicationsCopy Control, Evidence of Ownership, Fingerprinting

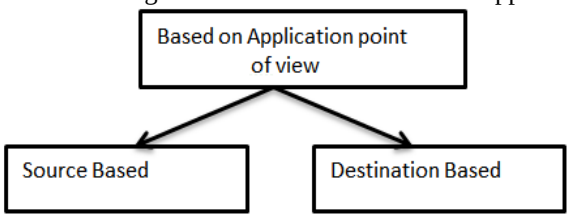

Fig.6. Based on Application point of views

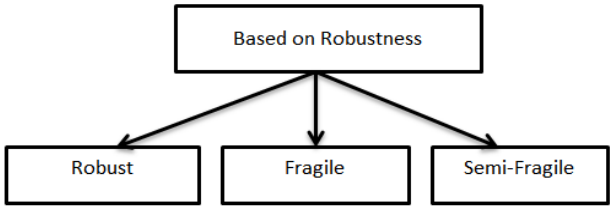

Fig.7. Based on Robustness/Characteristics

4. Division Based on The Watermarking extraction Process

Blind watermarks: These watermarks detect the embedded information without the use of original signal. It needs only a secret key and less robust to any attacks on the signal.

Semi-blind watermarks: These watermarks require secret key and watermark bit sequence to detect the watermarked signal.

Non-blind watermarks: These watermarks require the original signal and secret key to detect the embedded information in the watermarked signal. They are more robust to any attacks on the signal when compared to blind watermarks.

5. Based on User's Authorization to Detect the Watermark

This is sub-divided into public watermarks and private watermarks. Figure shows the classification of watermarks based on user's authorization to detect the watermark.

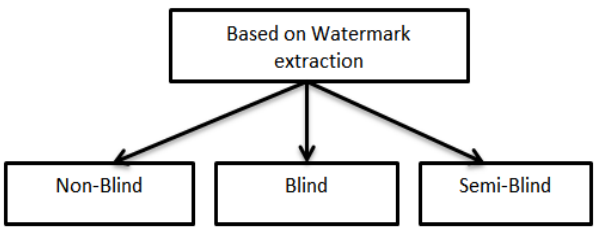

Fig.8. Based on The Watermarking extraction Process

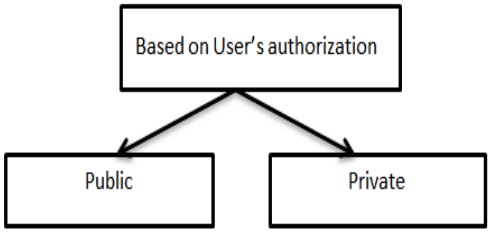

Fig.9. Based on User's Authorization to Detect the Watermark

Public watermarks: In this watermarking, the user is authorized to detect the watermark embedded in the original signal.
Private watermarks:In this watermarking, the user is not authorized to detect the watermark embedded in the original signal.

6. Based on type of digital media signal

Image watermarking: This is used to hide the special information into the image and to later detect and extract that special information for the author's ownership.
Video watermarking: This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.
Audio watermarking: This application area is one of the most popular and hot issue due to internet music, MP3.
Text watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

IV. DIGITAL WATERMARKING TECHNIQUES

Digital Watermarking is the technique used to embed or hide the secret information into the digital documentsby using various techniques. They have its own merits and demerits. The main techniques are explained as follows.
1.Spatial domain: In the Spatial domain we directly modify the original image by simply changing value or replace of value of the pixel. It is very easy in implementation but less robust towards the attacks.Some of its main algorithms are as discussed below:
1.1. Additive Watermarking: It is a simple method for embedding the watermark into the cover image. It adds pseudo random noise patterns to the intensity pixels of the cover image. The noise signals are usually integers like (-1, 0, 1) or can be floating point numbers. In order to ensure that the watermark can be detected, and noise is generated by a key, the correlation between the numbers of different keys has to be very low.
1.2. Least Significant Bit:It isthe earliest methods of the image watermarking. Two LSB techniques proposed by Van et al. In the first method the LSB of the image was replaced with a pseudo-noise (PN) sequence while in the second a PN sequence was added to the LSB..
1.3. SSM Modulation Based Technique: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the cover image with a small pseudo noise signal.
2.Transform domain: Frequency-domain techniques are more robust than spatial domain. The only aim is to embed the watermarks in the spectral coefficients of the image to increase the robustness. Some of its methods are discussed below:
*2.1. Discretecosinetransforms (DCT):*The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It is widely used in image compression. The discrete cosine transform (DCT) helps separate the image into parts spectral sub-bands of differing importance with respect to the image's visual quality.

$$S(u,v) = \frac{2}{\sqrt{nm}} C(u)C(v) \sum_{y=0}^{m-1} \sum_{x=0}^{n-1} s(x,y) \cos\frac{(2x+1)u\pi}{2n} \cos\frac{(2y+1)u\pi}{2m} \quad u = 0,..,n \quad v = 0,...,m$$

where $C(u) = 2^{-1/2}$ for $u = 0$
$= 1$ otherwise

Steps: DCT Block Based Watermarking Algorithm:
1) Segment or divide the image into non-overlapping blocks of 8x8 sizes.
2) Apply forward DCT to each block
3) Apply some block selection technique (e.g. HVS)
4) Apply coefficient selection criteria (e.g. high, middle, and low)
5) Embed watermark after modifying the selected coefficients.
6) Apply inverse DCT transform on each of these blocks.

Fig.10. DCTconversion to its frequency domain.

2. *Discrete wavelettransforms(DWT):*DWT is a wavelet transformin which the wavelets are discretely sampled. Key advantage of it over Fourier transforms is temporal resolution: it captures both frequency *and* location information.
Advantages of DWT over DCT: Wavelet transform understands the HVS better than the DCT.

Wavelet coded image is a multi-resolution of image; an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high.

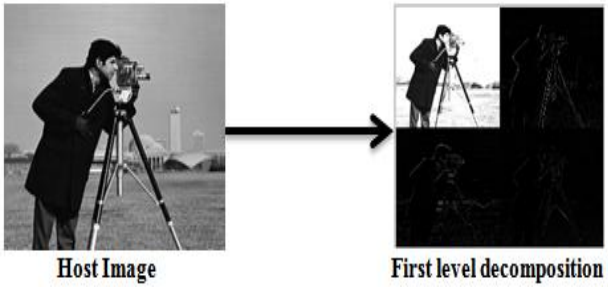

Fig.11.First Level Decomposition in DWT

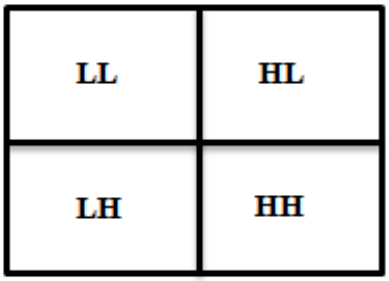

Fig.12.DWT based watermarking Scheme

Disadvantages of DWT over DCT: Computational complexity of DWT is more as compared to DCT'. Feig (1990) pointed out that, it only takes 54 multiplications to compute DCT for a block of 8x8, but in wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient of image.

3. *DiscreteFourier transform(DFT):* It transforms a continuous function into its frequency components. It has the robustness against geometric attacks like rotation, scaling, cropping and translation etc. DFT shows the translation robustness to attack. In spatial shifting in the image affects the phase representation of the image but not the magnitude representation and circular shifts in the spatial transform don't affect the magnitude of the Fourier transform.

Advantages of DFT over DWT and DCT: DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST robust and difficult to robust from geometric distortions.

V. DIGITAL WATERMARKING ATTACKS

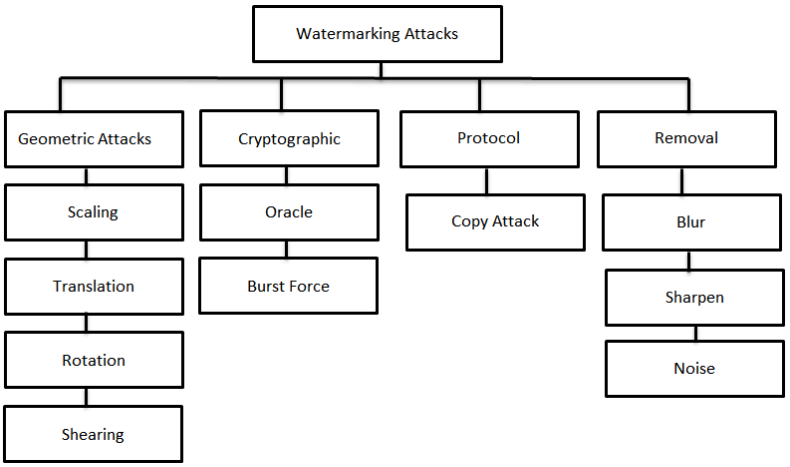

Fig.13. Watermarking attack's classification

A.Geometric attack: All these attacks affect the geometry of the image such as translation, rotation, cropping, etc. Cropping attack is overcome by DWT.

B. Removal Attack: Removal attacks wants to remove the watermark from the watermarked object. Such attacks include sharpen, blur, noise, and filter attacks. DWT will show robustness towards these attacks.

C. Interference attack: Interference attacks are those which add additional noise to the watermarked signals. Lossy compression, quantization, denoising, demodulation, collusion, averaging, and noise storm are some examples of this category of attacks. DCT shows some robustness towards these attacks.

D. Security Attack: In this, if watermarking algorithm is known, an attacker can modify the watermark.

E. Protocol Attack: This is also called copy attack, copying a watermark from one media into another without knowledge of the secret key is present.

F.Active Attacks: Attackers remove the watermark or can make it undetectable. Copyright protection, fingerprinting or copy control is problemsof it.

G.Passive Attacks: Protection against passive attacks is most importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grantby Cox et al (2002).

*H. Forgery Attacks:*The forgery attacks detected by watermarking and BAG method using grid.

VI. DIGITAL WATERMARKING APPLICATIONS

A.Forensics and Piracy Deterrence: Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used to gather or collect the evidence for the criminals. It is alsoused for contract between a contents owner and the persons or companies with which it shares their contents.

B. Fingerprinting: Fingerprints are the characteristics of an object that tends to distinguish them from the other objects by its uniqueness. In the applications of copyright protection, the watermark and finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally.

*C. Copyright Protection:*Copyright information can be inserted into image by mean of digital watermarking. It is used for ownership detection of data over the internet.

D. Telemedicine: For integrity, security, confidentiality of medical image digital watermarking playsgreat role in telemedicine fields.

E. Rich Media Enhancement for Mobile Phones: Now day's smart phones are becoming the most handheld computing device we carry with us 24/7 hours. We mostly look to the mobile phones in order to provide us instant information, and entertain us. Mobile is a core component of many strategies that are emerging to provide information to peoples.

VII. CONCLUSION

Digital watermarking can be achieve by using various method in both spatial and frequency domain. Spatial domain methods are easy to implement, but less robust towards attacks. Frequency domain methods are more robust. Digital watermarking has many applications in various fields. Creating more robust watermarking method is still a challenging research problem. Various techniques are present to increase robustness of data over the internet. All this study will help to open a new way for new ideas to overcome the existing limitations of different methods and explains various techniques, its classifications, attacks and applications of digital image watermarking.

REFERENCES

[1] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "*Multimedia data embedding and watermarking technologies* ", Proceeding of the IEE,Vol.86,No.6,1998,pp.1064-1087

[2] Kundur.Htzinakos, D.," *Digital Watermarking using Multiresolution Wavelet Decomposition*". Proc. IEEE Int. Cong. On Acoustics, Speech and Signal Processing,Seattle,Washington,vol.5,pp.2969-2972,May 1998

[3] Stefan Katzeneisser and Fabien A. P. Petitcoalas. "*Information Hiding Techniques for steganography and Digital Watermarking*" Artech house. Computer security series.pp.15-23.97-109.2000.

[4] The Watermarking Schemes, [Online], Available: http://cryptome.org/sdmi-attack.html

[5] Watermarking attack, [Online], Available: http://en.wikipedia.org/wiki/Watermarking_attack

[6] "Techniques for data hiding", by W. Bender, D. Gruhl, N. Morimoto, A. Lu

[7] "Communication and Information Theory in Watermarking: A Survey" by Adrian Sequeira and Deepa Kundur

[8] 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, pg. no. 165-175

[9] Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", 2010 International Conference on Intelligent Computation Technology and Automation

[10] www.networkworld.com

[11] www.digitalwatermarkingalliance.org

[12] www.wikipedia.org

[13] www.scisstudyguides.addr.com

[14] http://ippr-practical.blogspot.in

[15] www.scisstudyguides.addr.com

