International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Digital Image Security Using Digital Watermarking

Prof.A.S.Kapse[1], Sharayu Belokar[2], Yogita Gorde[3], Radha Rane[4], Shrutika Yewtkar[5]

[1]*Professor. A.S.Kapse, Dept. Computer Science & Engineering, P.R. Pote College of Engineering & Tech, Amravati, Maharashtra, India.*
[2,3,4,5] *BE student, Dept. of Computer Science & Engineering, P.R. Pote College of Engineering & Tech, Amravati, Maharashtra, India.*

Abstract - *Digital image watermarking process is definite as to insert information of digital into digital signal. In watermarking is defined as a technique which embeds data into digital contents such as text, still images, video and audio data without degrading the overall quality of the digital media. This is an efficient solution to avoid illegal copying of information from multimedia networks. Digital image safety and integrity the top prioritized issue in today's information explosion. Watermarking is a popular technique that is used for copyright protection and authentication. Watermark should be robust and imperceptible. Robustness of watermark can be explained in terms of successful recovery of watermark from recovered content which may contain different types of noises and compression effects. This paper presents an overview of the various concepts and research works in the field of image watermark authentication.*

Key Words **Watermarking, Spatial domain, Image Transforms, Discrete Wavelet Transform, Discrete Cosine Transform, Discrete Fourier Transform.**

1.INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

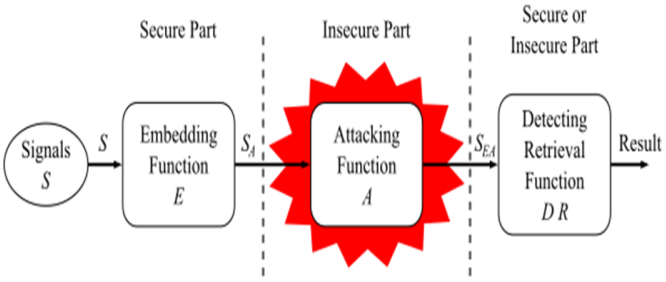

Fig-1 General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

Digital watermarking is the process of embedding information, call digital signature or watermarking, into a digital signal in a way that is difficult to remove. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Like traditional watermarks, digital watermarks are only perceptible under certain conditions. A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key. Special attention has to be paid to the kind of attacks as they can help to develop better watermarking techniques and defined better benchmarks [1].

Several types of watermarking schemes have been proposed for handling different applications. Examples include

1. Copyright-related applications where the embedded watermark are robust
2. Medical, forensic, and intelligence or military applications where the watermark are usually fragile or semi-fragile
3. Content authentication applications where any tiny change to the content are not acceptable, the embedding distortion has to be compensated for perfectly.

The watermarking algorithms are mainly classified into spatial watermarking algorithms and spectral watermarking algorithms. Spatial domain watermarking is a low level encoding which includes only simple operations such as edge detection, color separation, etc. Spectral domain watermarking algorithm has high complexity but is very

robust against signal processing attacks. These Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) are different spectral domain transform. [2]

2. CLASSIFICATION OF DIGITAL WATERMARKING TECHNIQUE

Digital watermarking techniques may be classified in several ways.

- Robustness
- Perceptibility
- Capacity

Robustness: A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal. A digital watermark is "fragile" if it fails to be detectable after the slightest modification. It is commonly used for tamper detection (integrity proof).A digital watermark is called semi-fragile if it resists benign transformations, but fails detection after malignant transformations. It is commonly are used to detect malignant transformations Robust watermarks may be used in copy protection applications to carry copy and no access control information. So the watermark is not destroyed after some attacks and can easily detected to provide certification.

Perception: A digital watermark is called perceptible if its presence in the marked signal is noticeable On videos and images, some are made transparent/translucent for convenience for consumers due to the fact that they block portion of the view; therefore degrading it.

Capacity: It can be defined as number of information bits a watermark encodes within a unit of time or work. Watermark should be able to carry enough information that can represent the uniqueness of image.

3. DIGITAL WATERMARKING TECHNIQUE

The process of embedding a watermark in a multimedia object is termed as watermarking. Watermark can be considered as a kind of a signature that reveals the owner of the multimedia object. A watermarking algorithm embeds a visible or invisible watermark in a given multimedia object. The embedding process is guided by use of a secret key which decided the locations within the multimedia object (image) where the watermark would be embedded. The entire digital image watermarking techniques always works in two domains either spatial domain or transform domain. The transform domain image is represented in terms of its frequencies; however, in spatial domain it is represented by pixels.

3.1 Spatial Domain Watermarking Techniques

Spatial domain digital watermarking algorithms directly load the raw data into the original image. It can also be applied using color separation. The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks.

Additive watermarking: It is the direct method used in spatial domain for embedding the watermark. It is done by adding pseudo random noise pattern to the intensity of image pixels.

Least Significant bit: The watermarking is done by choosing a subset of image pixels and substituting the LSB of each of the chosen pixels with watermark bits. In this technique we embed the watermark in the LSB of pixels.

- Simplicity.
- Very low computational complexity.
- Less time consuming.

3.2 Frequency Domain Watermarking Techniques

In frequency domain the watermark is embedded in the spectral coefficient of the image. The commonly used algorithms in frequency domain are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT).

DCT Domain Watermarking: DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques. DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. DCT domain watermarking can be categorized into Global DCT watermarking and Block based DCT water-marking.

Steps in DCT Block Based Watermarking Algorithm.

1. Segment the image into non-overlapping blocks of 8x8
2. Apply forward DCT to each of these blocks
3. Apply some block selection criteria (e.g. HVS)
4. Apply coefficient selection criteria (e.g. highest)
5. Embed watermark by modifying the selected coefficients.
6. Apply inverse DCT transform on each block

DWT Domain Watermarking: DWT based watermarking schemes follow the same guidelines as DCT based schemes, i.e. the underlying concept is the same; however, the process to transform the image into its transform domain varies and hence the resulting coefficients are different. Wavelet transforms use wavelet filters to transform the image.

Discrete Wavelet Transform (DWT) is widely is used in image processing applications as it encourages time-frequency signal decompositions. Using DWT, a signal can be decomposed into different sub-frequency bands. DWT uses both low pass filter and high pass filter to decompose the signal into different levels.

Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL). [3][4]

DFT Domain Watermarking: DFT domain has been explored by researches because it offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. In this section we discuss some watermarking algorithms based on the DFT domain.

DFT of a real image is generally complex valued, DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation. [5]

DFT is also resistant to cropping because effect of cropping leads to the blurring of spectrum. Scaling in the spatial domain causes inverse scaling in the frequency domain. Rotation in the spatial domain causes the same rotation in the frequency domain. [6]

4. COMPARATIVE ANALYSIS OF DIFFERENT WATERMARKING TECHNIQUES

The comparison between advantages and dis-advantages of different watermarking technique is given table1. [7][8]

Table -1: Comparative Analysis of Different watermarking techniques

Algorithm	Advantages	Disadvantages
DCT	1. More robust against digital Processing operations. 2 .Watermark cannot be removed by any attacks because of embedding. Water-mark into middle frequency coefficient.	1. Certain higher frequency components tend to be suppressed during the quantization process. 2. Block wise DCT destroys the invariance properties of the sys-tem. 3. Vulnerable to crop-ping, scaling.
DWT	1. Higher compression ratio which is relevant to human perception. 2 .Allows good localization both in time and spatial frequency domain. 3. Vulnerable to cropping, scaling.	1. Cost of computing may be higher. 2. Computational complexity is more. 3. Compression time may be longer. 4. Noise may appear near the edges of image.
DFT	DFT is rotation, scaling and translation (RST).So, it is used to recover from geometric distortions.	1. Complex implementations. 2 .Computing cost may be higher.
LSB	1. Low degradation of image quality. 2. Easy to implement and understand. 3. High perceptual transparency.	1. Very sensitive to noise. 2. Vulnerable to cropping, scaling attacks. 3. Very less robust against attacks.
Correlation	Increases the robustness of watermark by increasing the gain factor.	Due to very high increment In gain factor, image quality may decrease.
Patchwork	.High level of robustness against many types of at-tacks.	Very small amount of in-formation can be hidden.

5. APPLICATION OF WATERMARK TECHNIQUE

Digital watermarking may be used for a wide range of applications, such as:

1 .Copyright protection.

2. Source tracking (different recipients get differently watermarked content).

3. Broadcast monitoring (television news often contains watermarked video from international agencies).

4. Video authentication.

5. Software crippling on screen casting and video editing software programs, to encourage users to purchase the full version to remove it.

6. Content management on social networks.

6. CONCLUSION

In this paper, we surveyed the various aspects for digital watermarking techniques and its applications. A brief and comparative analysis of watermarking techniques is also presented which can help in the new researches in related areas. We also classified the watermarking algorithms based on spatial and transform domain. Watermarking, which belong to the information hiding field, has seen a lot of research interest recently. There is a lot of work begin conducted in different branches in this field. We classify the techniques based on different domains in which data is embedded. Here we limit the survey to images only.

REFERENCES

[1] Hartung, F. and Kutter, M.(1999) Multimedia Watermarking Techniques, Proc. of IEEE, Tutorial,

Survey, and Special Issue on Data Hiding & Security, pp.1079-1107.

[2] NavnidhiChaturvedi , Dr.S.J.Basha, "Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR", International Journal of Innovative Research in Science, Engineering and Technology Vol. 1, Issue 2, December 2012.

[3] Vidyasagar M. Potdar, Song Han, Elizabeth Chang," A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics Aug. 2005.

[4] Lakshmi Priya C V and Nelwin Raj N R," Digital watermarking scheme for image authentication", International Conference on Communication and Signal Processing, April 6-8, 2017, India.

[5] Pereira, S., Pun, T., "Robust Template Matching for Affine Resistant Image Watermarks," in IEEE Transactions on Inage Processing, vol. 9, no. 6, pp. 1123-1129, June 2000.

[6] Solachidis, V & Pitas, I 2001, 'Circularly Symmetric Watermark Embedding in 2-D DFT Domain', in IEEE Transactions on Itnage Processing, vol. 10, no. 11, pp. 1741-1753.

[7] Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[8] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, ―A Novel Technique for Digital Image Watermarking in Spatial Domain‖, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[9] Hend A. Elsayed; Yasir Khalid Jadaan; Shawkat K. Guirguis," Image Security Using Quantum Rivest-Shamir-Adleman Cryptosystem Algorithm and Digital Watermarking", Progress in Electromagnetic Research Symposium (PIERS), Aug. 2016.

[10] Mohd Aliff Faiz bin Jeffry,Hazinah Kutty Mammi," A Study on Image Security in Social Media using Digital Watermarking with Metadata", IEEE Conference on Application, Information and Network Security (AINS) 14 Nov. 2017

[11] U. Eze Peter; Udaya Parampalli; C. Iwuchukwu Uchechi; Onuekwusi Nnaemeka," Challenges and Prospects of Blind Spread Spectrum Medical Image Watermarking", IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON) Nov 2017.

[12] Ali Al-Haj, Hiba Abdel-Nabi," Digital image security based on data hiding and cryptography", 3rd International Conference on Information Management (ICIM), April 2017.

[13] Gururaj Kulkarni, Suresh Kuri," Robust Digital Image Watermarking using DWT, DCT and Probabilistic Neural Network", International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT) Dec 2017.

[14] S. Radharani Dr. M.L. Valarmathi," A Study on Watermarking Schemes for Image Authentication", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.4, June 2010.

[15] Upasana Yadav, J.P.Sharma, Dinesh.Sharma, Purnima K Sharma," Different Watermarking Techniques & its Applications: A Review", International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014.

[16] Seyed Mohammad Mousavi," Image Authentication Scheme using Digital Signature and Digital Watermarking", IJCEM International Journal of Computational Engineering & Management, Vol. 16 Issue 3, May 2013.