Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review Paper on Preserving Multimedia Data from Copyright Protection by Embedded Watermarking

Monika Craig[*], **Prof. Richa Sharma**

Department of C.S.E., GHRAET, Nagpur

Nagpur University, India

Abstract- Due to the rapid development of network technology, Multimedia such as text, image, video and audio has now been widely used. Humans can easily access or distribute any multimedia data from networks. Hence, the protection of intellectual property becomes more and more attentive and important for the society. Digital watermarking have been proposed for resolving copyright protection of multimedia. In this paper, we explained different transform domain techniques based on this various algorithm are proposed for copyright protection of digital products. Also infers their characteristics to resolve the issue of digital products.

Keywords— Digital watermarking, characteristic, attacks, watermarking techniques.

I. INTRODUCTION

The amount of digital products have been widely used over the network. Any unauthorized user easily access this digital content over the network, so we need to protect the digital products over the network from copyright protection of multimedia products. The access of copyright digital products causes the major concern to the content provider of digital products. To maintain the ownership of the digital content various efforts have been applied. Copyright protection of multimedia data has been accomplished by means of cryptography algorithms to provide control over data access and to make data unreadable to non-authorized users. However, encryption systems do not completely solve the problem, because once encryption is removed there is no more control on the dissemination of data. The main method which works well and efficiently is the method of applying digital watermarking. The concept of digital watermarking is an efficient way to solve the problems related to the copyright of intellectual property in digital media. It is used as a means to identify the owner or distributor of digital data. . Digital watermarking has attracted considerable attention and has numerous applications, including copyright protection, authentication, secret communication.

A. Digital Watermarking Concepts:

What is Digital Watermarking?

Digital watermarking refers to act of embedding a mark through a certain algorithm in multimedia information such as digital images, Audio, Video, Text etc. Mark is a secret information to be embedded can be some text, author‘s serial number, company logo, images 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. Later the embedded information is detected and extracted out to reveal the real owner/identity of the digital media. Watermarking is used for following reasons, Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication, Data Hiding. Watermarking consists of two modules watermark embedding module and watermark detection and extraction module. For a strong watermark embedding, a good watermarking technique is needed to be applied.

Why Digital Watermarking?

Digital watermarking is an enabling technology for e-commerce strategies: conditional and user-specific access to services and resources. Digital watermarking offers several advantages. The details of a good digital watermarking algorithm can be made public knowledge. Digital watermarking provides the owner of a piece of digital data the means to mark the data invisibly. The mark could be used to serialize a piece of data as it is sold or used as a method to mark a valuable image. For example, this marking allows an owner to safely post an image for viewing but legally provides an embedded copyright to prohibit others from posting the same image. Watermarks and attacks on watermarks are two sides of the same coin. The goal of both is to preserve the value of the digital data. However, the goal of a watermark is to be robust enough to resist attack but not at the expense of altering the value of the data being protected. On the other hand, the goal of the attack is to remove the watermark without destroying the value of the protected data. The contents of the image can be marked without visible loss of value or dependence on specific formats. For example a bitmap (BMP) image can be compressed to a JPEG image. The result is an image that requires less storage space but cannot be distinguished from the original. Generally, a JPEG compression level of 70% can be applied without humanly visible degradation. This property of digital images allows insertion of additional data in the image without altering the value of the image. The message is hidden in unused “visual space in the image and stays below the human visible threshold for the image.

The watermark can be hidden in the digital data either in visible or invisible form:
1) Visible: In visible watermarking, the embedded watermark can be visually observed i.e the information is visible in the picture or video. It is equivalent to stamping a watermark on paper, and for this reason is sometimes said to be digitally stamped. Typically, the information is text or a logo, which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. The advantage of visible watermarking is that it is easy to recognize the owner of the image without any calculation, but its disadvantage is that the embedded watermark can also be easily removed or destroyed.
2) Invisible: An Invisible watermark is intended to be imperceptible but is detected and extracted by an appropriate piece of software when the need arises. An image containing an invisible watermark should look similar to the original unmarked image.
watermarking can be classified again into two types:
*1) Fragile watermarks :*In contrast to image authentication, fragile watermarks are designed to detect any unauthorized modification such as distortion under the slightest changes to the image. We can determine whether the data has been tampered according to the state of fragile watermarking.
2) Semifragile or Robust watermarking: Semifragile watermarkings are usually Designed to resist the attacks such as image scaling, bending, cropping, lossy ,compression ,etc. It is also used in copyright protection to declare the rightful ownership. semifragile watermarks are designed to break under all the changes that exceed the user-specified threshold. the watermark is not destroyed after some attack and can still be detected to provide certification.

B. Basic Characteristics of Digital Watermarking

The basic requirement of digital watermarking is closely related to its purpose of applications, different application has different demand. In general, the characteristics of digital watermarking are as follows.
1) Robustness: Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking; annotation watermarking do not need resist malicious attacks.
2) Non-perceptibility: Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.
3) Verifiability: Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.
4) Security: Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.
5) Capacity: Image watermarking capacity is an evaluation of how much information can be hidden with in a digital image. Watermarking capacity is determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder.

II. DIGITAL WATERMARKING TECHNIQUES

The watermarking techniques are divided into two major categories :

A. Spatial Domain: This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels.

B. Frequency Domain: This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods today, such as

1) Discrete cosine transforms (DCT): It represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image[6].
Yong Zhu et. al [1] proposes an algorithm of color image watermarking based on DCT.The algorithm encrypts the binary watermarked images by Arnold transformation and DES which are also embedded in grayscale image in R and G channel decomposed by color image. The algorithm increases the amount of watermark embedded and solves the interference problem of embedding multiple watermarks.The algorithm of embedding watermark in the frequency domain has better robustness to resist Shearing attack, Gaussian noise attack and JPEG compression attack.

2) Discrete wavelet transforms (DWT): Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL)[4][5] . Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution. The larger the magnitude of the wavelet coefficient the more significant it is. Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved. High resolution subbands helps to easily locate edge and textures patterns in an image. DWT based watermarking techniques improve the watermarks of the robustness, It had strong robustness for the cutting, JPEG compression, plus noise and other signal attacking.

B.Sridhar, Dr.C.Arun [3] proposed a robust and secure image watermarking algorithm that embeds watermark in the deinterlace images using wavelet transform. The proposed scheme provides very high payloads and imperceptibility when compared to similar transform-domain techniques.

Advantages of DWT over DCT

- Wavelet transform understands the HVS more closely than the DCT.
- Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels Of resolution and can be sequentially processed from low resolution to high resolution.
- Visual artifacts introduced by wavelet coded images are less evident compared to DCT because wavelet transform doesn't decompose the image into blocks for processing. At high compression ratios blocking artifacts are noticeable in DCT; however, in wavelet coded images it is much clearer.
- DFT and DCT are full frame transform, and hence any change in the transform coefficients affects the entire image except if DCT is implemented using a block based approach. However DWT has spatial frequency locality, which means if signal is embedded it will affect the image locally in [12]. Hence a wavelet transform provides both frequency and spatial description for an image.

Disadvantages of DWT over DCT

- Computational complexity of DWT is more compared to DCT . As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient .

3) Discrete Fourier transform (DFT): Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform. DFT is also resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, which are normalized coordinates, there is no need of any synchronization. The strongest components of the DFT are the central components which contain the low frequencies.Scaling of image results in amplification of extracted signal and can be detected by correlation coefficient. Translation of image has no result on extracted signal. Rotation of image results in cyclic shifts of extracted signal and can be detected by exhaustive search. 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 .

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 invariant and hence it is difficult to overcome from geometric distortions.

4) Singular Value Decomposition(SVD): Singular Value Decomposition(SVD) is a numerical technique for diagonalizing matrices in which the transformed domain consists of basis states that is optimal in some sense. The SVD of an N x N matrix

A is defined by the operation:

A = U S V T

Where ***U*** and ***V*** Є ***R N x N*** are unitary, and ***S*** Є ***R N x N*** is a diagonal matrix. The diagonal entries of ***S*** are called the singular values of A and are assumed to be arranged in decreasing order ***σi > σi +1***. The columns of the ***U*** matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of ***A.*** Each singular value ***σi*** specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer [13,14]. In SVD-based watermarking, a frame image is treated as a matrix decomposed into the three matrices;***S, U*** and ***V T,*** as shown below.

$$\mathrm{Svd}(A)=\begin{bmatrix} U_{1,1} & . & . & U_{1,n} \\ U_{2,1} & . & . & U_{2,n} \\ & . & . & . \quad . \\ U_{n,1} & . & . & U_{n,n} \end{bmatrix}\begin{bmatrix} S_{1,1} & 0 & 0 & 0 \\ 0 & S_{2,2} & 0 & 0 \\ & & . & . \\ 0 & 0 & 0 & S_{n,n} \end{bmatrix}\begin{bmatrix} V_{1,1} & . & . & V_{1,n} \\ V_{2,1} & . & . & V_{2,n} \\ . & . & . & . \\ Vn,1 & . & . & Vn,n \end{bmatrix} . \quad .$$

TABLE I
COMPARISON BETWEEN WATERMARKING TECHNIQUES

Factors	**Spatial domain**	**Frequency domain**
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Computational Complexity	Low	High
Computational Time	Less	More
Capacity	High	Low
Example of Application	Mainly Authentication	Copyright

III. WATERMARKING ATTACKS

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing software made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under,

A. Removal Attack: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.

B. Interference attack: Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks.

C. Geometric attack: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

D. Low pass filtering attack: A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

E. Security Attack: In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

F. Protocol Attack: The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark‘s implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key.

G. Cryptographic attacks: Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack . In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

H. Active Attacks: Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.

I. Passive Attacks: In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

J. Collusion Attacks: In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications *(e.g.* in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

K. Image Degradation: These type of attacks damage robust watermarks by removing parts of the image. The parts that are replaced may carry watermark information. Examples of these operations are partial cropping, row removal and column removal. Insertion of Gaussian noise also comes under this category, in which the image is degraded by adding noise controlled by its mean and its variance.

L. Image Enhancement: These attacks are convolution operations that desynchronize the watermark information in an image. These attacks include histogram equalization, sharpening, smoothing, median filtering and contrast enhancement.

M. Image Compression: In order to reduce the storage space and cut the cost of bandwidth required for transmitting images, images are generally compressed with JPEG and JPEG2000 compression techniques. These lossy compression methods are more harmful as compared to lossless compression methods. Lossless compression methods can recover the watermark information with inverse operation. However lossy compression techniques produce irreversible changes to the images. Therefore probability of recovering watermarked information is always very low.

N. Image Transformations: These types of attacks are also called synchronization attacks or geometrical attacks. The famous software Stir Mark uses small local geometrical distortions to invalidate watermark detection. Geometrical attacks include rotation, scaling and translation also called RST attacks. Some researchers focus on RST robustness while designing the robust watermarking systems, because it is fundamental problem. Besides RST transforms, image transformations also include other transforms such as aspect ratio change, shearing, reaction and projection.

IV. **CONCLUSION**

In this paper we have surveyed the different techniques of watermarking used for digital copyright protection. . These techniques are classified into several categories depending upon the domain. We have also explain the advantages and disadvantages of the technique. Then we have also discuss the Comparison between the techniques. The result indicates frequency domain is more robustness than spatial domain. The comprehensive review of literature made has uncovered various aspects of Digital Image watermarking. It is concluded that digital watermarking technique is very impressive for image authentication and for protection against attacks.

REFERENCES

[1] Yong Zhu, Xiaohong Yu, Xiaohuan Liu, *"An Image Authentication Technology Based on Digital Watermarking"* International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS) 2013 IEEE.

[2] 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**.**

[3] B. Sridhar ,Dr.C.Arun *"On Secure Multiple Image Watermarking Techniques using DWT"* 2012 IEEE.

[4] Ying Zhang, Jiqin Wang, Xuebo Chen *"Watermarking Technique Based On Wavelet Transform For Color Images"* 2012 IEEE.

[5] Qing Liu, Jun Ying *"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis"* 2012 IEEE.

[6] Manpreet Kaur, Sonika Jindal & Sunny Behal *" A Study of Digital Image Watermarking"* Volume 2, Issue 2(ISSN: 2249-3905) ,February 2012.

[7] Mehdi Khalili *"A Novel Secure, Imperceptible and Robust CDMA Digital Image Watermarking In Jpeg-Ycbcr Channel Using DWT2"*,lnternational Journal of Enterprise Computing and Business Systems Vol. 1 Issue 2 July 2011.

[8] Shraddha S. Katariya *"Digital Watermarking: Review"* International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 2, February 2012.

[9] Jun Sang and Mohammad S. Alam, *"Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/ Semifragile Digital Image Watermarking"* IEEE Trans. *Instrum. Meas.*., vol. 57, no. 03,march 2008.

[10] Chuhong Fei, Deepa Kundur, Raymond H. Kwong, *"Analysis and Design of Secure Watermark-Based Authentication Systems"* IEEE Trans. *Instrum. Meas.*,, vol. 1, no. 1,march 2006.

[11] Zhe-Ming Lu, Dian-Guo Xu, Sheng-He Sun, *"Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization"* IEEE Trans. *Instrum. Meas.*,, vol. 14, no. 06, june 2005.

[12] Lee, C., Lee, H., *"Geometric attack resistant watermarking in wavelet transform domain,"* in *Optics Express v*ol. 13, no. 4, pp. 1307-1321.2005

13] Liu, R., and T. Tan, 2002. *"A SVD-Based Watermarking Scheme for Protecting Rightful Ownership"*, IEEE Trans. Multimedia 4, pp.121-128.

[14] Wu, Y, 2005. *"On the Security of SVD-Based Ownership Watermarking"*, IEEE Trans. Multimedia 7, pp. 624-627.