ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY

An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**

www.computerscijournal.org

ISSN: 0974-6471
April 2016,
Vol. 9, No. (1):
Pgs. 07-11

Digital Image Watermarking: An Overview

H. B BASANTH KUMAR

Pooja Bhagavat Memorial Mahajana Education Centre,
DoS in Computer Science, KRS Road, Metagalli, Mysuru – 570016, India.
*Corresponding author E-mail:basanth.10@gmail.com

http://dx.doi.org/10.13005/ojcst/901.02

(Received: January 25, 2016; Accepted: April 01, 2016)

ABSTRACT

Multimedia security is extremely significant concern for the internet technology because of the ease of the duplication, distribution and manipulation of the multimedia data. The digital watermarking is a field of information hiding which hide the crucial information in the original data for protection illegal duplication and distribution of multimedia data. The image watermarking techniques may divide on the basis of domain like spatial domain or transform domain or on the basis of wavelets. The spatial domain techniques directly work on the pixels and the frequency domain works on the transform coefficients of the image. This paper presents classification of watermarking, stages in watermarking, watermarking approaches and its applications.

Keywords: Authentication**,** Watermarking, Digital Image.

INTRODUCTION

In recent years, digitization plays a big role in human life as numerous applications in field of engineering, healthcare, communication, documentation and many more. Here, multimedia content like image and video is major content. Therefore, authentication, information security and other various issues are raised with multimedia sources and content. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using Computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original[1].

The above problem can be solved using digital watermarking. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

Classification of watermarking

Visible watermark

Visible watermarking technique generate a visible logo or symbol that clearly seen on watermarked image. This type of watermark used for show the ownership of content like TV channel.

Invisible Watermark

This type of watermark is used to find the ownership as well as prevention from authorized application of image or content. Here, a watermark can insert information into an image which cannot be seen, but can be interrogated with the watermark extraction algorithm.

Robust Watermark

Robustness watermarking scheme is used for sign copyright information of the digital works, the embedded watermark can resist the common edit processing and various attacks.

Fragile Watermark

Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. It can be determined whether the data has been tampered according to the state of fragile watermarking.

Semi fragile Watermark

Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise compression attacks.

Invisible-Robust Watermark

The invisible-robust watermark is embedding in such a way that processes made to the pixel level; which are perceptually not determine and it can be recovered only with appropriate decoding process.

Invisible-Fragile Watermark

The invisible-fragile watermark is embedded in such a way that any attacks of the image would alter or destroy the watermark[1].

Stages in watermarking

Digital Watermarking is a technique which is used in the digital signal processing of embedding hidden information into multimedia data. This information is not usually visible, only dedicated detector or extractor can seen and extracts that information. Digital Image Watermarking use digital image for embedding the hidden information, after embedding the watermarked image is generated and the watermarked image is more robust against attacks. Figure 1 shows the stages of digital watermarking. Basically working of digital image watermarking can be divided in three stages:

Embedding Stage

The embedding stage is the first stage in which the watermark is embedded in the original image by using the embedding algorithm and

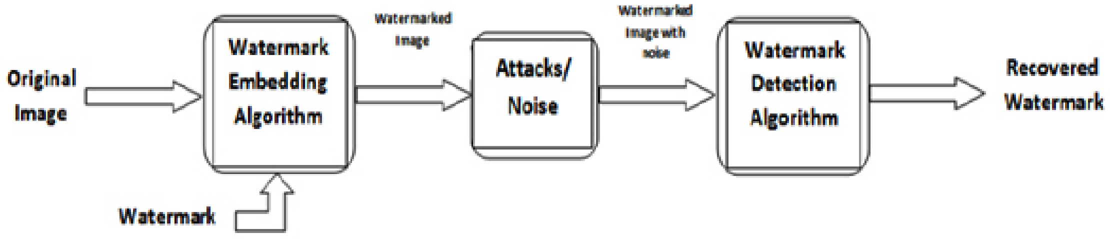
Original Image
Watermark Embedding Algorithm
Watermark
Watermarked Image
Attacks/ Noise
Watermarked Image with noise
Watermark Detection Algorithm
Recovered Watermark

Fig. 1: Stages in Digital Image Watermarking

the secret key. Then the watermarked image is generated. So the watermarked image is transmitted over the network.

Distortion/Attack Stage

In this stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.

Detection/Retrieval Stage

In the detection stage, the watermark is detected or extracted by the dedicated detector from the watermarked image by applying some detection algorithm and by using secret key. In addition to this, noise is also detected[2].

Watermarking approaches

There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

Spatial domain

Spatial domain digital watermarking algorithms directly load the raw data into the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image. Some of its main algorithms are as discussed below:

Additive Watermarking

The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low.

Least Significant Bit

Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

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 host image with a small pseudo noise signal that is modulated by the embedded watermark.

Texture mapping coding Technique

This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage), and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

Patchwork Algorithm

Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified).

Correlation-Based Technique

In this technique, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image I(x, y). Iw(x, y) = I(x, y) + k*W(x, y) Where K represent the gain factor, Iw represent watermarked image ant position x, y and I represent cover image. Here, if we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease.

Frequency domain

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. Some of its main algorithms are discussed below:

Discrete cosine transforms (DCT)

DCT like a Fourier Transform, 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 robust compared to spatial domain 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. 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.

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). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies.

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[3].

Watermarking applications

a) Ownership Assertion – Protects the ownership rights.

b) Fingerprinting – To avoid unauthorized duplication of copies and its distribution.

c) Authentication and Integrity Verification – A unique key is used to embed and extract, this verifies the integrity of the system.

d) Content labeling – Extra information like date, place etc can be added.

e) Usage control – Only a limited number of copies can be created.

f) Content protection – Visible watermark makes it very difficult to modify the contents.

CONCLUSION

In last few years, Digital watermarks have thus helped us to protect the ownership of digital data. In this paper, classification of watermarking, different stages in watermarking, several techniques based on spatial domain and frequency domain and its applications were discussed. Digital watermarking scheme is widely utilized for authentication of data, copyright protection and communication process. It provides a consistent robust performance on different original image and watermarked image in various analyses.

REFERENCES

1. Naina Choubey and Mahendra Kumar Pandey, “Transform based Digital Image Watermarking: An Overview”, in *Intl. Jrnl. of Computer Trends and Technology (IJCTT),* **24**(2); 80-83 (2015).
2. Preethi Parashar and Rajeev Kumar Singh, “A Survey: Digital Image Watermarking Techniques”, in Intl. Jrnl. of Signal Processing, *Image Processing and Pattern Recognition,* **7**(6): 111-124 (2014).
3. Prabhishek Singh and R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”, in Intl. *Jrnl. of Engineering and Innovative Technology (IJEIT)* **2**(9): 165-175 (2013).