IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Digital Watermarking Techniques

Ritu Rawat[1], Nikita Kaushik[2], Soumya Tiwari[3]

Student, CSE, Graphic Era University, Dehradun, India [1,2,3]

Abstract: Watermarking is hiding digital information in a carrier signal. Digital Watermark verifies the Authenticity or Integrity of the Carrier Signals or shows Identity of its owners. Watermark works as Tag or Ownership Identifier. Basically watermark is a secondary image that is imposed on the original image for protecting that image. Today in the emerging world of internet digital watermarking is becoming very important. Digital watermarking is used in various applications like-copyright protection, tamper detection, broadcast monitoring, authentication, integrity, and verification. Image processing use voluminous methods for digital watermarking. This following paper is a survey of various watermarking techniques and presents a brief introduction to these methods used for watermarking.

Keywords: Digital watermarking, Spatial Domain Techniques, Frequency Domain Techniques, Least significant Bit, SSM Modulation, Discrete Cosine Transform, Discrete Wavelet Transformation, Discrete fourier Transform .

I. INTRODUCTION

Digital watermarking technology protects digital images from unauthorized changes or use [2]. Watermarking is basically used for providing security for several types of data like audio, video, image, etc. Embedding a message in the form of number, text or image on a host signal is called watermarking [2], it can be visible or invisible. Today development in e-commerce applications in world wide web needs to increase security of data communications over the internet [1]. For providing security to communication over internet encryption of data and information hiding methods were used. Many different methods such as Cryptography, Watermarking and Steganography are used for transferring the data/image without any manipulations [1]. A watermark is a secondary image that is imposed on the original image for protecting that image**.** Cryptography technique for encrypts and decrypts data for keeping the message secret.

Cryptography provides security only through encryption and decryption. It does not provide any security after decryption but in watermarking content is even protected after the decryption [1]. Watermarking is sequence of bits which is added in the digital image, audio or video for identifying file's copyright information [1]. Therefore watermarking assures the data is protected. The same algorithm that was used for inserting watermark in the image is used by the user for reading watermarked image. Digital image processing is a highly developing area with various rising applications in computer science field. Digital image processing has several valuable features over the analogue [4]. Digital image represents 2-dimensional images as a precise set of digital values called pixels. Thus, digital image processing using digital computer is known as digital image processing [4]. Digital watermarking is an application of digital image processing. This is also known as information hiding. Digital watermarking embeds secret and additional information into original image that can be extracted later or van be detected later for various prospects like authentication, owner identification, protection of content and copyright protection, Digital Fingerprinting [4], Transaction Tracking [4], and many more [4]. Digital watermarking maintains digital content security and protects the data from unauthorized users. Robustness and imperceptibility across several attacks is a feature of digital watermarking. The efficiency of watermarking algorithms is based on the robustness of the embedded watermark across several attacks [4]. Digital watermarking is one of the emerging fields and is used in many applications that have been established to be successful. Digital watermarking is widely used in several techniques of image processing. The objective of each and every application is to provide security of the digital content [4].

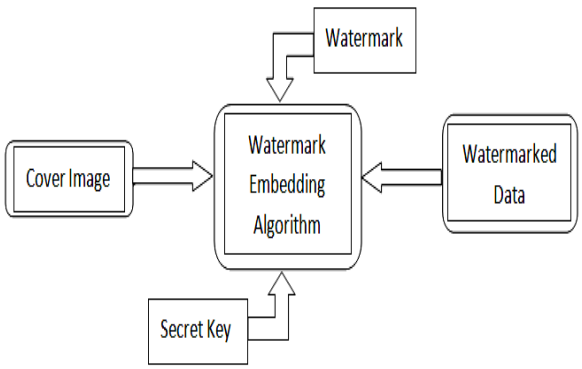

Fig 1: Watermark Embedding [4]

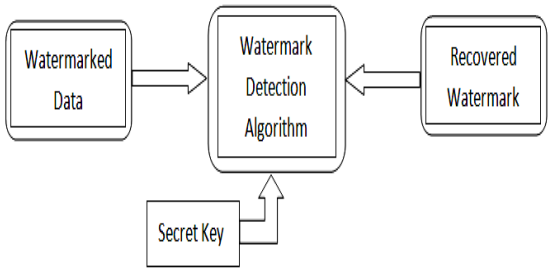

Fig 2: Watermark Detection [4]

DOI 10.17148/IJARCCE.2016.54123

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Digital watermarking process includes two algorithms: First is embedding algorithm and second is the detecting algorithm. Figure 1 represents watermark embedding process-in which watermark is embedded into the cover image using the embedding algorithm. And Figure 2 represents watermark detection process in which embedded watermark is retained by detection algorithm [4].

II. WORKING OF DIGITAL IMAGE PROCESSING

In Digital Watermarking digital image embeds hidden information, which gives a watermarked image as a result. Figure 3 represents the three phases of digital image watermark working [4].

A. Embedding Phase
In this phase embedding algorithm and secret key are used for embedding the watermark in original image and produce watermarked image as result that will be transmitted over the network [4].

B. Distortion Phase
In this phase, noise is inserted or some attacks are performed on the transmitted watermarked imaged over the network for either modifying or destroying the watermarked data [4].

C. Detection Phase
In this phase, detection algorithm and secret key are used to detect the watermark; even noise is also detected [4].

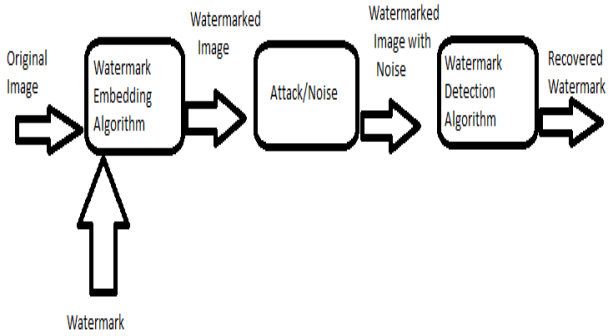

Fig 3: working of digital image watermarking

III. DIGITAL WATERMARKING CHARACTERISTICS

Three main characteristics of digital watermarking are [2]:
A. Fidelity: The image quality should not get altered after it is watermarked; even watermarking should not make the distortions visible as it will reduce economic value of image.

B. Robustness: Watermarks are removed knowingly or unknowingly by image processing operations. It should be robust across several attacks.

C. Capacity: This characteristic defines amount of data that has to be embedded as a watermark for successfully detection during extraction.

D. *Security:* Watermark should be secret so that it cannot be identified by the unwanted users.

IV. APPLICATIONS OF WATERMARKING

The main applications of watermarking are [2]:
A. Copyright Protection: Watermarking protects redistribution of copyrighted material over the unreliable network [2].

B. Content Archiving: Watermarking inserts digital object descriptive or serial number for archiving video, audio or images. It is also used for classification and organization of digital contents [2].

C. Broadcast Monitoring: It is a cross-verification technique for verifying the data that was supposed to be broadcasted has been broadcasted or not [2].

D. Tamper Detection: With the help of watermarking, tampering with digital content is detected easily. For tampering detection fragile watermarks are added in the digital content and if added watermark is found to be degraded, indicate tampering with content [2].

E. Digital Fingerprinting: This technique detects the owner of the digital content on the basis of fingerprints that are unique [2].

F. Authentication and Integrity Verification: Watermarking also maintains authentication of data and verification of integrity through the use of fragile watermark [6].

V. DIGITAL WATERMARKS TYPES

Watermarking techniques are classified into the following:
A. On the basis of document that has to be watermarked, watermarking techniques are divided into the four types:
- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

B. *In other way, digital watermarks techniques are divided as follows:*
- Visible watermark: It is basically a secondary image that is imposed on original image for protection of that image. In this changes that are made to original image are visible. For example Figure 4 (a) and (b) shows the original and visible watermarked image [10].
- Invisible-Robust watermark: In this type of watermarking technique the changes that are made to original image in the form of a watermark are unnoticeable and the changes made are easily recovered later with the help of suitable decoding algorithm.
- Invisible-Fragile watermark: Invisible fragile watermarks are added in digital content and if the added watermark is found to be degraded or altered, it indicates tampering with content or modification of image.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Fig 4(a): original image [10]
Fig 4(b): Watermarked image [10]

VI. WATERMARKING TECHNIQUES

Digital watermarking consists of several different techniques for protection of digital content [4]. The digital image watermarking falls in two main broad categories:

- Spatial domain techniques
- Frequency domain techniques

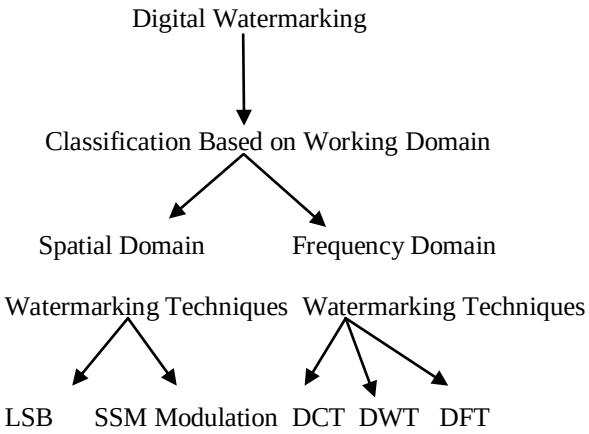

Fig 5: Classification of Watermarking Domain

Spatial domain techniques works on pixels and pixel value are modified for embedding the watermark. The commonly used spatial domain technique is LSB. Whereas frequency domain coefficient are modified by Frequency domain techniques for embedding watermark. DCT, DWT and DFT are commonly used frequency domain technique. In case of robustness and imperceptibility, frequency domain techniques are more reliable than spatial domain technique.

A .Spatial Domain Techniques

This technique presents the image in form of pixels. In this technique, watermark is embedded in the cover image by changing values, intensity and the color of the selected pixels [5]. The key benefits of spatial domain watermarking are its simplicity, low computational complexity and it consumes less time [4]. The estimation speed of spatial domain techniques is very fast in comparison with frequency domain techniques and simply can be applied to any image but it is less robust to attacks than frequency domain techniques [4]. The commonly used method of spatial domain is LSB [4, 7].

• Least Significant Bit (LSB)

This is the simplest spatial domain method, as LSB carries less appropriate information and their modification does not cause visible changes [5]. It is simple to embed a watermark in LSB of randomly selected pixels of the original image [4]. An image is given, where each pixel of image is represented by an 8-bit stream, the watermarks are added in the LSB, of selected pixels of the image. This method is easy from implementation point of view and does not produce severe distortion to the image but, it is not very robust across attacks [7]. Example of LSB watermarking [4]:

Image:
10010101 00111010 11001100 01010100….

Watermark:
0 1 0 1…..

Watermarked Image:
1001010**0** 0011101**1** 1100110**0** 0101010**1**…..

The steps of LSB technique for watermark embedding in cover image are [4]:

1) First Converting RGB image into grey scale image.
2) Making double exactness for image.
3) Shifting MSB to LSB of watermark image.
4) Making LSB of cover image zero.
5) Adding shifted version (step 3) of watermarked image to modified (step 4) host image.

The main benefits of LSB method is that it can be simply applied on images. And it does not deteriorate the quality of image after embedding the watermark. The main drawback of LSB method is it is not very robust against signal processing operations and attacks [4].

• SSM Modulation Based Techniques:

In Spread-spectrum Modulation techniques the energy generated at different discrete frequencies is purposively dispersed or appropriated in time, for secure communications establishment, increasing resistance to natural interference and jamming, and for preventing detection. SSM watermarking algorithm embeds information in context of image watermarking and when it is applied to the context of image watermarking, it embeds message by combining the cover image with a small pseudo noise signal modulated by the added watermark [5].

B. Frequency Domain Techniques

The frequency domain techniques are more successful than spatial domain techniques. In frequency domain techniques, the image is illustrated in the form of frequency [4].Frequency domain techniques are more applied than spatial domain techniques. The aim of this technique is to embed the watermarks in the spectral coefficients of the image. Discrete Cosine Transform (DCT), Discrete wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are the commonly used frequency domain technique [4]

DOI 10.17148/IJARCCE.2016.54123

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

• Discrete Cosine Transform (DCT)

DCT is used for signal processing. It basically helps in transforming signal from spatial domain to the frequency domain. DCT is used in many fields like compression of data, recognition of pattern and in almost every field of image processing. DCT watermarking is more robust in comparison with spatial domain watermarking [4]. Discrete Cosine Transform is similar to Discrete Fourier Transform; therefore it represents data in terms of frequency space rather than an amplitude space [7]. It converts signal into elementary frequency components [5]. This type of algorithms are more robust on image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However they are not robust across geometric attacks like rotation, scaling, cropping etc [5]. Global DCT watermarking and Block based DCT watermarking are sub-categories of DCT watermarking [5]. The main steps of DCT [4, 5]:

1) Image is segmented into non-overlapping blocks of 8x8.
2) Forward DCT is applied to these blocks.
3) Block selection criteria like HVS are applied.
4) Coefficient selection criteria like
5) Selected Co-efficient is modified for embedding watermark.
6) Inverse DCT transform is applied on each block.

DCT divides image into different frequency band for adding the watermark. The DCT due to selection of perceptually significant frequency domain coefficients is more robust across different signal processing attacks [4].

• Discrete Wavelet Transformation (DWT)

Today DWT is widely used in variety of signal processing applications, like in audio and video compression, removing noise in audio, and the simulation of wireless antenna distribution. The energy of Wavelets is centered in time and are appropriate for analysis of transient, time-varying signals. DWT is well suited for many applications as most of the signals in nature changes with time. The biggest challenge in watermarking is to achieve a good tradeoff between robustness and perceptivity. But if strength of enclosed watermark is increased robustness will be achieved but visible damage will also get increased simultaneously [7]. DWT is preferred more as it gives both spatial localization and frequency spread of the watermark within the original image [7]. The main concept of DCT is to decompose the image into sub-image having different spatial domain and independent frequencies [7]. DWT of image gives multi resolution representation of image that provides simple framework for describing image information. Signal is analyzed at different resolutions by DWT. DWT breaks image into high low frequency quadrants and low frequency quadrant is further divided into two more high and low frequencies and this is continued until the signal is completely decomposed [4]. DWT are scalable in nature. DWT are mostly used in image watermarking because of its good spatial localization and multi resolution techniques [4]. The main disadvantages of DWT are: it is more complex than DCT, computation cost is higher and computation time is longer.

• Discrete Fourier Transform (DFT):

DFT is robust across geometric attacks such as cropping, scaling, rotation, translation etc. DFT divides an image in sine and cosine form. DFT techniques are categorized into two types: first is direct embedding and another one is the template based embedding. In direct embedding DFT magnitude and phase coefficients are modified for embedding the watermark, whereas template based embedding propose the idea of templates. Basically template is a structure that is embedded in DFT domain for calculating transformation factor and as the image goes under transformation the template is looked for resynchronizing the image, and then for extracting the embedded watermark detector is used. Central component that consist of low frequency is the main component of DFT [4].

The main benefit of DFT over DCT and DWT is that DCT is found to be Rotation Scaling Translation (RST) invariant. Hence it can easily overcome from geometric distortion, whereas DCT and DWT are not RST invariant. Therefore they are not able to easily overcome from geometric distortions [4]. And the main drawback is the output of DFT that is always a complex value and more frequency rate is required and even computational efficiency of DFT is very bad. So due to these reasons DFT is not used [4].

VII. COMPARISON BETWEEN SPATIAL AND FREQUENCY WATERMARKING DOMAIN

Table I: Comparison between Watermarking Domains [8]

S.no	Factors	Spatial Domain	Frequency Domain
1.	Cost	Very Low	Very High
2.	Robustness	Fragile	Low Robust
3.	Perceptually	Highly Controllable	Low Controllable
4.	Computational complexity	Low	High
5.	Time Consumption	Less	More

VIII. CONCLUSION

Today Digital image Watermarking has become important research topic for researchers. This survey paper detailed spatial domain (LSB, SSM) and Frequency domain (DCT, DWT, DFT) techniques of digital image watermarking. Different techniques used for watermarking have their own advantages and disadvantages. Digital image watermarking is still a challenging research area and lot of research work needs to be done in the field of watermarking. Future work could include the development of more robust and secure watermarking technique than the existing ones.

DOI 10.17148/IJARCCE.2016.54123

ACKNOWLEDGMENT

We would like to thank all our mentors, friends and family members for their support. We would also like to mention that it would not have been possible without the timely help and support of Computer Science and Engineering Department.

REFERENCES

[1] Namita Chandrakar, Jaspal Bagga. "Performance Comparison of Digital Image", International Journal of Computer Applications Technology and Research, Volume 2– Issue 2, 126 - 130, 2013.

[2] Vinita Gupta**,** Mr. Atul Barve, " A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

[3] *Saraju P. Mohanty*, K.R. Ramakrishnan, Mohan S Kankanhalli, "* A DCT Domain VisibleWatermarking Technique for Images"

[4] Preeti Parashar, Rajeev Kumar Singh, "A Survey: Digital Image Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124.

[5] Y. Shantikumar Singh, B. Pushpa Devi, Kh. Manglem Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme", International Journal of Engineering Research (ISSN : 2319-6890)Volume No.2, Issue No.3, pp : 193-199 01 July 2013.

[6] Navnidhi Chaturvedi, "Various Digital Image Watermarking Techniques And Wavelet Transforms", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 5, May 2012).

[7] Manpreet Kaur ,Sonika Jindal ,Sunny Behal, " A STUDY OF DIGITAL IMAGE WATERMARKING", Volume 2, Issue 2 (February 2012).

[8] Shivanjali Kashyap, " Digital Watermarking Techniques and Various Attacks Study for Copyright Protection", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

[9] frank hartung, student member, ieee, and martin kutter, "Multimedia Watermarking Techniques"

[10] Tsung-Yuan Liu, *Student Member, IEEE*, and Wen-Hsiang Tsai, *Senior Member, IEEE, "*Generic Lossless Visible Watermarking—A New Approach", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 19, NO. 5, MAY 2010.

DOI 10.17148/IJARCCE.2016.54123