International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN: 2349-9745
p-ISSN: 2393-8161

A Review on Digital Image Watermarking Techniques

Dhiraj Singh Kushwah[1], Pragyesh Kumar Agrawal[2]
[1]Research Scholor, Atal Bihari Vajpayi Hindi Vishwavidyala
[2]Professor of Physics, Sarojini Naidu Govt. Girls P.G. College

Abstract - Due to the rapid expansion in internet technology copyright protection and data authenticity are two major problems in handling digital multimedia. Watermarking is a very important field for copyrights of various electronic documents and media. A variety of techniques have been proposed for copyright protection of digital images which include spatial domain and transform domain watermarking. This paper aims to provide some basic concepts of digital image watermarking techniques and comparisons between them.

Keywords - Copyright Protection, Digital Image Watermarking, Spatial domain, Transform domain, Watermarking Techniques

I. INTRODUCTION

Digital watermarking has been a popular topic for both research and applications in last decade. Due to the rapid growth of using digital image, there is a sincere need of copyright protection. A watermark is a digital data embedded in multimedia objects such that the watermark can be detected to make an assertion about the objects. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information [1]. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. The digital image watermarking process embeds a signal into the host image without significantly degrading its visual quality.

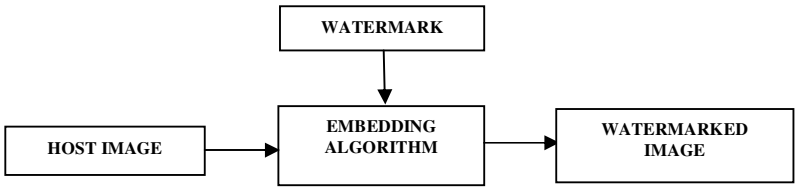

Figure 1. Schematic Flow of Digital Image Watermarking

Watermarking is very similar to steganography in a number of respects. Both methods seek to embed information inside a cover message with very little to no degradation of the cover-object. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties, but neither technology alone is ideal and can be compromised [2].

e-ISSN: 2349-9745
p-ISSN: 2393-8161

Watermarking can be further classified as follows on the basis of various criteria [3,4]:

According to Embedding Domain:
- Spatial domain,
- Frequency/transform domain, and
- Temporal domain

According to Extractor:
- Blind and
- Nonblind

According to Human Perception:
- Visible and
- Nonvisible:
    - Robust and Fragile

According to Application:
- Source-based and
- Application-based

On the basis of embedding or working domain watermarking techniques can be divided into two categories. The watermarks can be applied either in spatial domain or in the frequency domain.

II. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

Digital Image Watermarking is used in many applications. They are as follows:

1. **Digital Rights Management:** It concerns the management of digital rights and the enforcement of rights digitally.
2. **Copyright Protection:** Copyright protection is an important application of digital watermarking. It enables the identification of the copyright owner and thus protects his or her right in content distribution.
3. **Image and Content Authentication:** In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place.
4. **Tamper Detection:** Temper detection is used to disclose alterations made into an image. It is closely related to authentication. If tampering is detected in an image, then the image is considered inauthentic.
5. **Broadcast Monitoring:** Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters [5].
6. **Fingerprinting:** The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained [6].
7. **Medical Application:** Patients Information can be printed on the X-ray reports and MRI scans using techniques of visible watermarking.

e-ISSN: 2349-9745
p-ISSN: 2393-8161

III. TECHNIQUES OF WATERMARKING

Digital image watermarking techniques can be broadly classified into two major categories:

- Spatial Domain Watermarking
- Frequency Domain Watermarking

3.1. Spatial Domain Watermarking

Early watermarking algorithms were introduced in the spatial domain, where copyrighted information is added by changing pixel values of host image. Least Significant Bit insertion is one of the examples of this category [7]. 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. However the spatial domain methods are generally fragile to image processing operations or other attacks [8]. Some of its algorithms are LSB, SSM Modulation based technique.

3.1.1. Least Significant Bit (LSB)

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant) bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information [9].

3.1.2. 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. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, 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 [10,11].

3.2. Frequency (Transform) Domain Watermarking

These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture [12]. In the Frequency domain the watermark is embedded into frequency coefficients of host image. Frequency domain watermarking is more robust than spatial domain watermarking due to embedding of watermark into the altered frequency coefficients of the transformed image [13]. Some most commonly used frequency domain watermarking techniques are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

3.2.1. Discrete Fourier Transform (DFT)

Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. [14]. The equivalent transform for discrete valued function requires

e-ISSN: 2349-9745
p-ISSN: 2393-8161

the Discrete Fourier Transform (DFT). In digital image processing, the even functions that are not periodic can be expressed as the integral of sine and/or cosine multiplied by a weighing function. This weighing function makes up the coefficients of the Fourier Transform of the signal. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients [15].

3.2.2. Discrete Cosine Transform (DCT)

Discrete Cosine Transform is related to DFT in a sense that it represents data in terms of frequency space rather than an amplitude space. 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 [16,17].

3.2.3. Discrete Wavelet Transformation (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. A wavelet series is a representation of a square-integrable function by a certain ortho-normal series generated by a wavelet. Furthermore, the properties of wavelet could decompose original signal into wavelet transform coefficients which contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in wavelet transform domain is generally a problem of embedding watermark in sub bands of cover image [18]. The wavelet transform decomposes image into three spatial directions, i.e. horizontal, vertical and diagonal.

IV. COMPARISON OF SPATIAL DOMAIN AND TRANSFORM DOMAIN WATERMARKING TECHNIQUES

The main advantage of spatial watermarking is its simplicity. The spatial domain watermarking technique is simple and has low computing complexity, because no frequency transform is needed. It needs less computational time because of low computing complexity. The disadvantage of spatial domain technology is limited robustness. This technique is not robust against compression and filtering. Also the information which can be embedded in spatial domain is very limited. In spatial domain watermarking technique embedded watermark can be easily destroyed and modified by attackers and hence, these techniques are rarely preferred over frequency domain watermarking techniques. The frequency domain techniques are more popular than spatial domain techniques because frequency domain techniques are more robust against any attacks such as rotation, cropping resize, flipping etc. and compatible with popular image compression standards.

Table 1. Comparison of Spatial Domain Watermarking and Frequency Domain Watermarking

S. No.	Factors	Spatial Domain Technique	Frequency Domain Technique
1.	Computational Cost	Less	More

2.	Robustness	Weak	Strong
3.	Perceptual Quality	High Control	Low Control
4.	Computational Complexity	Less	High
5.	Computational Time	Less	More
6.	Capacity	More	Less

V. CONCLUSION

Various types of watermarking techniques have been analyzed in this paper. Watermarking algorithms have been classified based on spatial and frequency domain in which the watermark is embedded. In terms of processing, frequency domain is better than the spatial domain techniques. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. On the other hand, spatial domain watermarking techniques have less computational overhead compared with frequency domain techniques. It is concluded that digital image watermarking technique is very impressive for image authentication and for copyright protection.

REFERENCES

[1] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE), Volume 6, Issue 1, Sep-Oct. 2012.

[2] Jagroop kaur, "Private key Steganography using DCT", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014.

[3] Abu-Errub, A, and Al-Haj, A, "Optimized DWT-based image watermarking", First International Conference on Applications of Digital Information and Web Technologies, IEEE, 4-6, 2008.

[4] E.Kougianos, S. P. Mohanty and R. N. Mahapatra, "Hardware Assisted Watermarking for Multimedia", Elsevier Journal on Computer and Electrical, 35(7), 339-358, 2008.

[5] Kusuma Kumari B. M, "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Science and Research (IJSR), Volume 2, Issue 12, December 2013.

[6] Vandana Tehlani, "A New Fragile Approach for Optimization in Invisible Image Watermarking by Using Symmetric Key Algorithms", International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 5, July 2012.

[7] Chirag Sharma, Deepak Prashar, "DWT based robust technique of watermarking applied on digital Images", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-2, May 2012.

[8] Satendra kumar, Ashwini Kumar Saini, Papendra Kumar, "SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform", International Journal of Computer Applications, Volume 45– No.10, May 2012.

[9] Keshav S Rawat, Dheerendra S Tomar, "Digital Watermarking Schemes for Authorization Against Copying or Piracy of Color Images", Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 295-300.

[10] Manpreet Kaur, Sonika Jindal, Sunny Behal, "Study of Digital Image Watermarking ", IJREAS Volume 2, Issue 2, February 2012.

e-ISSN: 2349-9745
p-ISSN: 2393-8161

[11] 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.
[12] Gurpreet Kaur, Kamaljeet Kaur, "Image Watermarking Using LSB (Least Significant Bit)", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
[13] Meenu Singh, Abhishek Singhal and Ankur Chaudhary, "Digital Image Watermarking Techniques: A Survey", International Journal of Computer Science and Telecommunications, Volume 4, Issue 6, June 2013.
[14] Jalpa M.Patel, Prayag Patel, "A Brief Survey on Digital Image Watermarking Techniques", International Journal For Technological Research In Engineering Volume 1, Issue 7, March-2014.
[15] Senthil Nathan.M, Pandiarajan.K, Baegan.U, "Digital Image Watermarking Basics", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 8, Issue 1, Sep. - Oct. 2013.
[16] Gaurav N Mehta, Yash Kshirsagar, Amish Tankariya, "Digital Image Watermarking: A Review", International Journal of Scientific Engineering and Technology, Volume No.1, Issue No.2 pg: 169-174, April 2012.
[17] Chhaya S. Gosavi, C.S. Warnekar, "Study of Multimedia Watermarking Techniques", International Journal of Computer Science and Information Security, Vol. 8, No.3, August 2010.
[18] Bhupendra Ram, "Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Volume 2, Issue 4, April-2013.

