Ultra Scientist Vol. 26(3)B, 221-226 (2014).

A Survey on Digital Image Watermarking Techniques and Attacks

DHIRAJ SINGH KUSHWAH and PRAGYESH KUMAR AGRAWAL

Department of Physics Govt. Nutan Girls College, Bhopal (India)

(Acceptance Date 29th September, 2014)

Abstract

Use of digitized media is increasing due to rapid growth of internet and there is a sincere need of copyright protection of digital images. In order to protect ownership or copyright of digital image digital image watermarking techniques have been designed and implemented. The performance of a digital watermarking technique is indicated by the robustness of embedded watermarks against various attacks. Digital image watermarking can be done both in spatial as well as frequency domain. A comparative study of different digital watermarking techniques in spatial and transform domain has been provided in this paper. LSB technique is commonly used in spatial domain based watermarking, and in frequency domain based watermarking techniques, DCT and DWT are commonly used. This paper focuses on the various domains of digital image watermarking techniques and various attacks on watermarked images.

Key words : Robustness, Spatial Domain, Frequency Domain, LSB, DCT, DWT, Watermark.

1. 1. Introduction

Digital images can be easily edited and distributed without owner's consent. The ways and means are required to detect copyright violations and control access to these digital media. Unfortunately the currently available formats for image in digital form do not allow any type of copyright protection. A potential solution to this kind of problem is an electronic stamp or digital watermarking which is intended to complement cryptographic process[1].

Digital image watermarking is one of the most widely used techniques for protection of ownership rights of digital images. Digital watermarking is a technique in which secret information called watermark is embedded to a particular digital media. Here, the watermark may be a logo or an image which can be proved who is right owner. The digital image water-marking system consist two functions, embedding

function, and extracting/detecting function. The embedding function embeds the secret message called watermark into the original image and then the watermarked image is passed onto the internet where it may be passed through general processing functions or attacked by an attacker either to remove or destroy the watermark. The extracting/ detecting function is used to extract the watermark for verification purposes or to check the presence of watermark for monitoring purposes[2]. In digital image watermarking technique, there are two domains for a embedding a watermark, namely frequency domain and spatial domain[3,4]. One of the famous spatial domain methods is LSB modification which covers low order bits of host image to cover watermark. It is most straight forward method and hence it is easy to implement and have low complexity. But it is less robust to various attacks.

The digital image watermarking is divided into two parts:

a) Watermark Embedding
b) Watermark Extraction

1.1 Watermark Embedding :

The process of image watermarking is done at the source end. In this process watermark is embedding in the cover image by using any watermarking algorithm or process. The whole process is shown in figure 1:

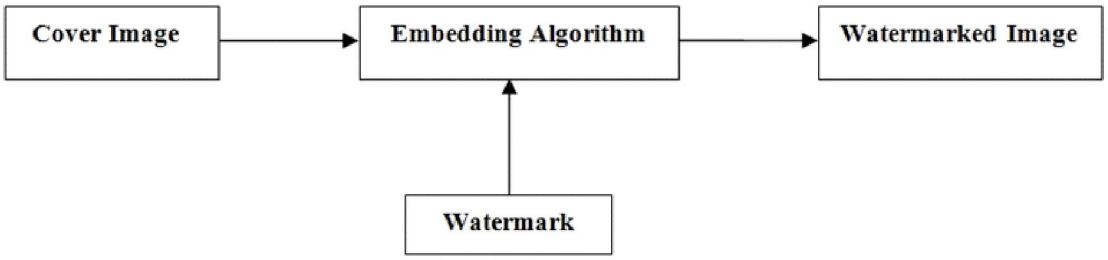

Figure 1: Watermark Embedding

1.2 Watermark Extraction :

This is the process of Extracting watermark from the watermarked image by reverse the embedding algorithm. The whole process is shown in figure 2:

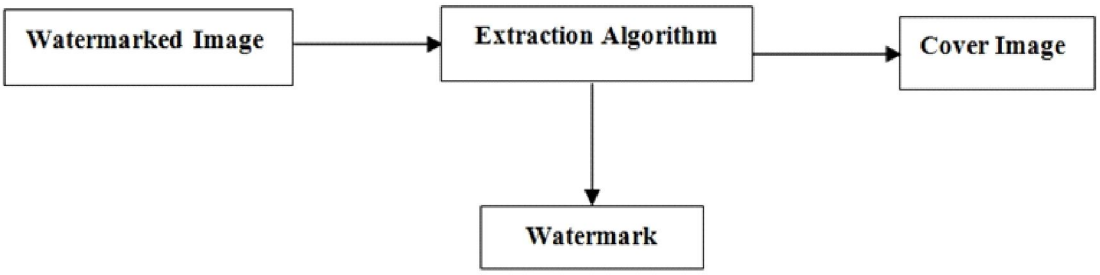

Figure 2: Watermark Extraction

2. Features of Digital Image Watermarking

For a watermark to be effective, it should satisfy the following features. They are[5]:

Imperceptibility: It should be perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it. A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un-watermarked content. The image must not be visibly degraded by the presence of watermark.

Readily Extractable: The data owner or an independent control authority should easily extract it.

Unambiguous: The watermark retrieval should unambiguously identify the data owner.

Robustness: It should tolerate some of the common image processing attacks. A watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copyright protection applications to carry copy and access control information.

Security: Unauthorized parties should not be able to read or alter the watermark. Ideally, the watermark should not even be detectable by unauthorized parties.

3. Watermarking Techniques :

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

A. Spatial Domain Watermarking

B. Frequency Domain Watermarking

A. Spatial Domain Watermarking :

The spatial-domain techniques directly modify the intensities or color values of some selected pixels. No transforms are applied to the host signal during watermark embedding. Spatial techniques are not very robust against attacks. The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. Spatial domain technique is less time consuming as compare to frequency domain techniques[6]. Least Significant Bit insertion is one of the examples of this category.

a) Least Significant Bit (LSB) :

The earliest work of digital image watermarking schemes embeds watermarks in the least-significant-bits of the cover image. 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[7]. This approach is not robust to attacks of most of the kinds.

b) 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[7].

B. Frequency (Transform) Domain Watermarking :

Compared to spatial domain techniques, frequency domain techniques are more applied. The target of this technique is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). The discrete wavelet transforms (DWT) and the discrete cosine transforms (DCT) are implemented very effectively in numerous digital images watermarking scheme[8].

a) 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.[9]. The equivalent transform for discrete valued function requires 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[10].

b) 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[11,12].

c) 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[13]. The wavelet transform decomposes image into three spatial directions, i.e. horizontal, vertical and diagonal.

4. Attacks on Watermarking :

Attacks are the factors or processes that can degrade the digital watermark strength. Attacks can be broadly classified into these main categories.

- Removal Attacks
- Geometric Attacks
- Cryptographic Attacks
- Protocol Attacks

4.1 Removal Attacks :

These type of attacks are affected the watermark in such a way that it a complete or nearly about to removed or destroyed watermark data. Examples of these attacks are denoising, averaging, quantization, remodulation, and collusion attacks.

4.2 Geometric Attacks :

Geometric attacks are specific to images and videos. Geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data. Examples of these attacks are pixels shifting, scaling of image, rotation of image without any higher visual changes. The aim of these kinds of attacks is degrade the quality of watermark.

4.3 Cryptographic Attacks :

Cryptographic attacks aim at cracking the security methods in watermarking schemes and remove the watermark information. Examples are brute force attack and oracle attack. But if the embedding algorithm is complex then these attacks are easily restricted.

4.4 Protocol Attacks :

These attacks are intentionally done by attackers to change or destroy the ownership information from the watermarked image. Example of these attacks is copy attack and changing of watermark.

5. Conclusion

The purpose of this paper is to present a survey of digital image watermarking techniques and attacks. Various types of watermarking techniques and attacks have been analyzed in this paper. We classified watermarking algorithms based on the spatial and transform domain in which the watermark is embedded. Also, study the watermarking properties and various attacks. 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 against attacks than the spatial domain techniques. On the other hand, spatial domain watermarking techniques have less computational overhead compared with frequency domain techniques and less time consuming as compare to frequency domain techniques.

6. References

1. Verma V., Singh J., "Digital Image Watermarking Techniques: A Comparative Study", *International Journal of Advances in Electrical and Electronics Engineering, 2(1)*, 173 (2013).
2. Bajaj A., "Comparative Analysis of Digital Image Watermarking Techniques - SVD based Algorithms in Different Wavelet Domains", *International Journal of Computer Science & Engineering Tech-*

nology (IJCSET), 5(6), 659 (2014).
3. Lee S.J., Jung S.H., "A survey of watermarking techniques applied to multimedia", *Proc. of ISIE 2001, Pusan, South Korea, 1,* 272 (2001).
4. Cox I.J., Miller M. L., and Bloom J. A., "Digital watermarking and Steganography", *Morgan Kaufmann Publishers,* (2002).
5. Sathik M.M. and Sujatha S.S., "Authentication of Digital Images by using a semi-Fragile Watermarking Technique", *International Journal of Advanced Research in Computer Science and Software Engineering, 2(11),* 39 (2012).
6. Chandrakar N., Bagga J., "Performance Comparison of Digital Image Watermarking Techniques: A Survey", *International Journal of Computer Applications Technology and Research, 2(2),* 126 (2013).
7. Singh P. and Chadha R. S., "A Survey of Digital Watermarking Techniques, Applications and Attacks", *International Journal of Engineering and Innovative Technology (IJEIT), 2(9),* 165 (2013).
8. Singh Y. S., Pushpa Devi B., and Singh K. M., "A Review of Different Techniques on Digital Image Watermarking Scheme", International Journal of Engineering Research, *2(3),* 193 (2013).
9. Rawat N. and Manchanda R., "Review of Methodologies and Techniques for Digital Watermarking", *International Journal of Emerging Technology and Advanced Engineering, 4(4),* 237 (2014).
10. Senthil Nathan M., Pandiarajan K. and Baegan U., "Digital Image Watermarking Basics", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), 8(1),* 7 (2013).
11. Mehta G. N., Kshirsagar Y. and Tankariya A., "Digital Image Watermarking: A Review", *International Journal of Scientific Engineering and Technology, 1(2),* 169 (2012).
12. Craig J., Sharma R., "Review Paper on Preserving Multimedia Data from Copyright Protection by Embedded Watermarking", *International Journal of Advanced Research in Computer Science and Software Engineering, 4(2),* 310 (2014).
13. Ram B., "Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", *International Journal of Advancements in Research & Technology, 2(4),* 19 (2013).