A Review on Digital Image Watermarking and Its Techniques

Rajiv Vasudev
Department of Computer Science & Engineering, Anand College of Engineering & Management, Kapurthala, India
Email: rajiv.vasu@gmail.com

Abstract—**The enormous popularity of internet offers various multimedia resources through various digital networks. These multimedia resources or digital media should be protected against various unauthorized attacks so as to use them for profit or security. Digital Watermarking is a way of protecting the digital media from unauthorized usage.This paper is a review on the Watermarking process, Types of watermarks, Various Watermarking Techniques and Applications of Watermarking.**

Index Terms—**watermarking, types of watermarks, spatial watermarking, frequency domain watermarking and applications of watermarking**

I. Introduction

Watermarking is a process through which one can hide useful information by the use of any digital media. It is a process by which one can verify the authentication of the owner of a digital media. The digital media can be image, text, video or audio. Watermarking is very much related to Steganography. Because they both hide messages inside a digital signal. The basic difference between the two is: Watermarking tries to covert a message that is related to actual content of the digital signal. But Steganography has no contact to the message. It is used just as a cover to hide a message. For performing watermarking process, two images are required. The first image should be the original image and the second image should be the watermark image. The watermark image is the useful information which is to be hidden from the unauthorized author. The watermark image is useful for the sender level as well as for the receiving level. So it should be protected from the unauthorized access at the sending level as well as at the receiving level. After performing watermarking process, a third image is obtained which is called Watermarked image. The watermarked image can be identified by the authorized person with the use of a secret key. The secret key is only known to the authorized sender and the authorized receiver in case of a private watermark [1]. But if the watermarking process is not related to the security purposes then public watermarks are used and the watermarked image is easily accessed by anyone. The whole watermarking process should follow two steps: embedding and extracting. In the embedding process, the watermark media is embedded or inserted into the original image. After embedding, a watermarked image is obtained. In the extracted process, the watermark is extracted from the watermarked image by following an inverse of embedding technique. That extracted watermark is required at the receiver level for obtaining the useful information (watermark). Watermarking is done by following a particular method. The quality of the watermarked image is highly depends upon the watermarking technique used. Spatial Domain techniques are used for performing watermarking. The watermarking is done by changing the least significant bits of the image in most of the spatial domain techniques. But these techniques are not robust and imperceptible. So for obtaining good quality of watermarked image, frequency domain techniques are used. In frequency domain techniques, coefficients values of the image are changed by following a particular frequency domain method. The frequency domain techniques are more robust and imperceptible than the spatial domain techniques. The quality of the watermarked image of the frequency domain techniques is much better than the quality of the watermarked image obtained by spatial domain techniques. This paper is decomposed into various sections. In Section 2 background of the watermarking is described. In Section 3 different types of watermarks are introduced. These watermarks should be used according to the requirement. In Section 4 different techniques are described through which watermarking process takes place. Section 5 contains various applications of the watermarking. These applications should apply on different areas.

II. Research Background

In 1999, Nikolaidis N., *et al.* gives an overview on the various data hiding techniques for copyright protection of still images. This paper describes that in spatial domain techniques data is embedded by directly manipulating the pixel values of the image. Though spatial domain methods are simple, less complex but these are not robust against various attacks. So a frequency domain technique eliminates the disadvantages of the spatial domain techniques [1].

In 1999, Hsu C-T., *et al.* proposed that watermarking is a technique for labeling digital pictures by hiding secret information into the images. Sophisticated watermark embedding is a potential method to discourage unauthorized copying or attest the origin of

Manuscript received February 1, 2016; revised September 13, 2016.

doi: 10.18178/joig.4.2.150-153

the images. The watermarks are embedded with visually recognizable patterns into the images by selectively modifying the middle-frequency parts of the image [2].

In 2002, Lihyang, *et al.* proposed detection algorithm which is applied to the attacked signal to attempt to extract the watermark from it. Results have proved that if the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if anychange is made to the signal [3].

In 2010, Mathew K, D., proposed the Singular Value Decomposition (SVD) based image watermarking scheme. The output result of SVD is more secure and robust. In the proposed scheme D and U components are used for embedding watermark. Unlike other transforms which uses fixed orthogonal bases, SVD uses non fixed orthogonal bases. It is concluded that the result of SVD gives good accuracy, good robustness and good imperceptibility in resolving rightful ownership of watermarked image [4].

In 2013, Kaur G., *et al.* presents a watermarking technique which Least Significant Bits (LSB), its steps and its process with Matlab images. LSB is applied on watermark for security of the image. But it is assumed that LSB is not a reliable technique of image watermarking as it works on spatial domain and one can easily identified the secret data in the LSB based watermarked image [5].

In 2014, Zargar A. J., *et al.* states that watermarking is done with the help of Least Significant Bit technique (LSB). As LSB technique is used as it has less effect on image. This new algorithm is using LSB of original image and doing '&&' operation with MSB of watermark image, and same watermarked image is then extracted from host image by replacing its LSB with MSB and making its LSB zeroes, so then watermark is extracted from host image. Based on LSB technique the author proposed a new watermarking algorithm, which is simple and resistant to number of attacks [6].

In 2016, Kaur S., *et al.* proposed a hybrid technique using SVD-DWT-DCT watermarking techniques of watermarking. Kalman Filtering is used for increasing the quality of the watermarked image. Diagonal components of SVD are used for embedding the watermark. After that LH filter of DWT is used this is then preceded by using the middle frequency level of DCT technique. Two performance parameters are used for measuring the quality of the watermarked image. For increasing the robustness of the watermarked image, Kalman Filtering is used which increases the peak signal to noise ratio at a great rate and decreases the mean square error from the image [7].

III. Types of Watermarks

The useful information which is used as a watermark in watermarking is of many types. The most used watermarks are written below:

Visible watermarks: These watermarks are applicable in images and cannot be removed by cropping. These watermarks can be used by anyone because these are not meant for security purposes.

Perceptual watermarks: These watermarks are mostly transparent and have high quality contents.

Invisible watermarks: These watermarks are used for security purposes only. Different techniques are used to perform watermarking in which invisible watermarks are obtained.

Fragile watermarks: These watermarks are easily destroyed by a small manipulation.

Private watermarks: These watermarks are only used at an individual level. When security is required for an individual level then these watermarks are used.

These different watermarks can be used for different purposes. If watermarking is performed for security purposes or for copyright protection only then last three watermarks are used in the experiments. But if watermarking process is not related to security purposes then first three watermarks are used in the watermarking process.

IV. Techniques of Watermarking

The watermarking process should follow a particular technique through which the whole process proceeds. That particular technique is sometimes called the secret key. A secret key is used at the embedding level to embed the watermark in the original image. This secret key is only known to the user. The inverse of this secret key (which is the inverse of the particular used technique) is used to extract the watermark from the watermarked image. Basically the watermarking techniques are decomposed into two domains. Spatial domain and Frequency domain.

A. Spatial Domain Techniques

In Spatial Domain, the alterations should apply on the pixels of the images only. The watermarking is performed by simply replacing the pixels of the original images with the watermark images. But in frequency domain the watermarking process should apply on the coefficients values of the images. Spatial Domain has following watermarking techniques.

1) SSM modulation based technique

This technique used the least significant bits for embedding watermarks. This method is robust against various attacks and is easy to implement. The embedding is performed by selecting a group of pixels and replaces this selected group with the pixels of watermarks. But this technique does not tolerate common signal processing attacks and is not used for practical applications.

2) Texture mapping coding technique

The images which have texture part in them should use texture mapping coding technique for watermarking. Because this technique hides the watermark in the texture part of the image.

3) Patchwork algorithm

This technique is highly based on the pseudorandom stastical model. This technique used Gaussian distribution as a stastical technique for hiding data.

4) Least significant bits

This is the simplest technique in which watermarking is performed by simply overwritten the least significant bits of the original image with the least significant bits of the watermark image. A third image is generated which is called the watermarked image. For example: if the value of the original image data is 10011100 and the pixel value of the watermark is 011, then after applying this technique a third pixels value is generated which is called the watermarked image having value 10011111.

Limitations of Spatial domain techniques: Spatial domain techniques are very simple but they lack robustness and imperceptibility. These techniques perform watermarking in a small time but the quality of the watermarked image is much lower that the quality of the watermarked image obtained by using the frequency domain techniques. These techniques were easily survived through simple operations like cropping and noising. But cannot survive through lossy compression and other techniques [8].

B. Frequency Domain Techniques

These techniques are widely applied as they are robust and imperceptible than other techniques. Also the watermarked image formed by using the frequency domain has high quality. Following are the various frequency domain techniques:

1) Discrete Cosine Transform (DCT)

DCT separates the images into three different parts of different frequencies. These frequencies are low, high and middle frequencies. While using this technique for image watermarking it is more frequent to embed watermark into the middle frequencies. This transfer helps in deciding the location at which the watermark should embed so that it should be robust enough. 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. DCT works by separating an image into different parts of different frequencies [9].

2) Discrete Wavelet Transform (DWT)

This technique is a modern one to perform digital image watermarking. This transform is based on small waves with varying frequencies. DWT is a system of filters. The filters in DWT decompose the image into four sub-bands. These sub-bands are varying from each other on the basis of their multiresolution. These sub-bands are named as LL, LH, HL and HH. LL consists of low resolution bands which is smaller than other bands. LH, HL, HH are the finest scale wavelet coefficients. This transform decomposes the original image into three directions such as horizontal, vertical and diagonal. Magnitude of DWT coefficients is larger in lowest bands (LL) and is smaller in other bands. Subbands with high resolution easily locate edges and patterns in an image. This technique is widely used in many areas [9].

3) SVD based image watermarking

Singular Value Decomposition is a stable technique which splits the image into three components. Horizontal components are denoted by U. Vertical components are denoted the V and the diagonal components are denoted by S.A digital Image X of size M×N, with M ≥ N, can be represented by its SVD as follows:

$$X = USV^T \quad (1)$$

$$U = [U1, U2\ldots\ldots Um] \quad (2)$$

$$V = [V1, V2\ldots\ldots Vn] \quad (3)$$

$$S = \begin{bmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & 0 & \\ & & & \sigma_n \end{bmatrix} \quad (4)$$

where *U* is an M×M matrix, *V* is an N×N matrix, and *S* is an M×N matrix with the diagonal elements represents the singular values, of X. T denotes the transpose of the matrix. This technique is widely used in watermarking process for solving the false positive problem and the problem of rightful ownership [9].

4) Hybrid techniques

For increasing the robustness and imperceptibility hybrid techniques are used for watermarking embedding and extraction.These techniques used two or more frequency domain techniques for watermarking process. Hybrid techniques are more robust than a single frequency domain technique [9].

V. Applications of Watermarking

By using various techniques of watermarking on different watermarks, watermarked images are obtained.These watermarked images or media are used in various areas so as to protect important data from unauthorized user. Following are the various application of watermarking.

Content identification and management: Digital watermarking provide a unique digital identity to all forms of media content, it helps to easily identify the content wherever it exists.

Fingerprinting: For acquiring copyright protection, fingerprinting is used. Watermarks are used as fingerprints and are easily traced by authorized users. By acquiring fingerprinting through watermarking no one can use the copyright illegally.

Access control: Access Control is a property through which only the authorized author have privilege to change the media. This property is an application of watermarking.

Image authentication: Watermarking which is meant for security purposes only, uses frequency domain techniques in which keys are used for embedding and extraction. These keys should be known to the authorized persons only. So watermarking provides image authentication to the authorized users only.

Media forensics: Media forensics applications enhance the ability of the owner to detect the misuse of any media. This application is widely used for security purposes only.

Document and image security: To protect the images from misuse and illegal use watermarking is used as a secure technique for the protection of images.

VI. Conclusion

Watermarking is a vast concept through which security of important media is easily achieved. The security is required at embedding level as well as at extracting level to preserve the image from illegal access. But the quality of the watermarked image is highly depends upon the type of watermarking technique used. The spatial technique gives good watermarked images but the quality of these techniques is much lower than the quality of the watermarked images obtained by frequency domain techniques. The spatial domain techniques are easy enough than frequency domain techniques. So the choice from these two domains depends upon the requirements directly. If there is a requirement of a highly robust, secure and imperceptible image then any of the frequency domain technique should used. But if the images are required at small level with high speed then any of the spatial domain technique should used.

References

[1] N. Nikolaidis and I. Pitas, "Digital image watermarking: An overview," in *Proc. IEEE International Conference on Multimedia Computing and Systems*, 1999, pp. 1–6.

[2] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Transaction on Image Processing*, vol. 8, no. 1, pp. 58-68, 1999.

[3] L. Y. Wang and P. C. Chen, "On the protection and authentication of digital image based on wavelet transformation," in *Proc. IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, 2002, pp. 148-151.

[4] M. K. Deepa, "SVD based image watermarking scheme," *International Journal of Computer Applications*, pp. 21-24, 2010.

[5] G. Kaur and K. Kaur**, "**Image watermarking using LSB (Least Significant Bit)," *International Journal of Advance Research in Computer Science and Software Engineering*, vol. 3, no. 4, April 2013.

[6] A. J. Zargar, "Digital image watermarking using LSB technique," *International Journal of Scientific & Engineering Research*, vol. 5, no. 7, pp. 202-205, July 2014.

[7] S. Kaur and R. K. Sidhu, "Robust digital image watermarking for copyright protection with SVD-DWT-DCT and Kalman filtering," *International Journal Emerging Technologies in Engineering Research*, vol. 4, no. 1, pp. 59-63, 2016.

[8] M. Durvey and D. Satyarthi, "A review paper on digital watermarking," *International Journal of Emerging Trends and Technology in Computer Science*, vol. 3, no. 4, pp. 99-105, 2014.

[9] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain," *National Academy Sciences Letter*, vol. 37, no. 4 pp. 351-358, 2014.

Rajiv Vasudev is M.Tech in Computer Science and Engineering. He is working as Assistant Professor in Anand College of Engineering & Management, Kapurthala. His research area Include Database Management System, Data Mining, Security Issues related to Database, Wireless Sensor Networks.