International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol. 8, No. 5 (2015), pp. 145-150
http://dx.doi.org/10.14257/ijsip.2015.8.5.15

A Survey on Digital Image Watermarking and Its Techniques

Manjinder Kaur[1] and Varinder Kaur Attri[2]

[1]*M.Tech, Department of Computer Science Guru Nanak Dev University, Regional Campus*
Jalandhar, India
[2]*Prof., Department of Computer Science Guru Nanak Dev University, Regional Campus Jalandhar, India*
gurman5667@yahoo.com, Varinder2002@yahoo.com

Abstract

Watermarking is an art in which we hide some secret information in another file like image, audio, video, text etc. Watermarking is a concept closely related to steganography. In these, both hide information in a digital image. The information hide in this is in different forms like an image, song, video within the signal itself. In this paper, we present survey on image watermarking. In this paper, we also explain the types of watermarking and various techniques of watermarking and requirements of digital watermarking. We survey on some papers of image watermarking.

Keywords: *digital image watermarking, types of watermarking, watermarking techniques, requirements of digital watermarking*

1. Introduction

Digital image watermarking is solitary such technology that has made to protect digital images from illicit manipulations. Digital watermarking is a concept intimately related to steganography, in that they both hide a message inside a digital signal. Watermarking tries to hide a message related to the actual content of the digital signal, but in steganography the digital signal has no relation to the message, and it is used as a cover to hide its existence. Watermarking is used for providing a kind of security for various types of data. It may be image, audio, video, *etc.*, [2]. Digital watermarking is that which is the process of embedding information into a digital signal. That may be used to verify its authenticity and the identity of its owners, in same manner as paper bearing a watermark. For visible identification, the signal may be audio, pictures, or video in digital watermarking. If the signals are copied, then the information is also carried in the copy. Signal may be carry many different watermarks at the same time [1].

Watermarking *is* different to steganography; it has the extra requirement of robustness against possible attacks. Watermark can be either visible or invisible. Using digital watermarking, copyright information can be implanted into the multimedia data. This is implemented by using algorithms. Information such as number, images or text with special implication can be embedded. The purpose of this can be for copyright protection, covert communication, authenticity distinguish of data file, *etc*. [2].

2. Types of Watermarking

There are some types of watermarking:

2.1. Visible: The watermark is visible that can be a text or a logo. It is used to identify the owner [3].

ISSN: 2005-4254 IJSIP

2.2. Invisible: The watermark is embedded into the image in such a way that it cannot be seen by human eye. It is used to protect the image authentication and also prevent it from being copied [3]. Invisible watermark can be further classified into three types:

2.2.1. Robust Watermark: Robust Watermark aims to embed information in a file that cannot be easily destroyed. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks [3].

2.2.2. Fragile Watermark: They are designed with very low robustness. It is used to check the integrity of objects [3].

2.2.3. Public and Private Watermark: They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark [3].

3. Watermarking Techniques

The various watermarking techniques are:

3.1. Spatial Domain Techniques: Spatial domain watermarking tiny modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. Various spatial domain techniques are as follows [3]:

3.1.1. Least Significant Bit Coding (LSB): LSB coding is one of the earliest methods. Least significant bit can be applied in any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component [3].

3.1.2. Predictive Coding Schemes: Predictive coding scheme was proposed by Matsui and Tanaka for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust as compared to LSB coding [3].

3.1.3. Correlation-Based Techniques: In this method a pseudo random noise (PN) with a pattern W(x, y) is added to an image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not [3].

3.1.4. Patchwork Techniques: In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount [3].

3.2. Frequency Domain Techniques:

Frequency domain is that in which the secret data are hidden in the lowest or middle frequency portions in protected image, because of the higher frequency portion is more be suppressed by compression. It is important and difficult that how to select the best frequency portions of the image for watermark. There are various frequency domain techniques that are as follows:

3.2.1. Discrete Cosine Transform (DCT) based Technique: It is a process that is convert a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. It is very robust to JPEG compression, since JPEG compression itself uses DCT. However, DCT methods lack resistance to strong geometric distortions [3].

3.2.2. Discrete Fourier Transformation based technique: It is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.DFT uses complex numbers, while DCT uses just real numbers [3].

3.2.3. Discrete Wavelet Transform based Technique: DWT based methods enable good spatial localization and have multi resolution significance that is same to the human visual system. This approach also shows the robustness to low pass & median filtering. But, these are not robust to geometric transformations [3].

3.3. Wavelet Transform based Watermarking: The wavelet transform based watermarking technique divides the image into four sidebands a low resolution approximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform [3].

4. Requirements of Digital Watermarking

The basic requirements in digital watermarking are closely related to its purpose of applications, different application has different demands. In general, the requirements of digital watermarking are as following [1]:

4.1. Robustness: Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking annotation watermarking do not need resist malicious attacks [1].

4.2. Non-perceptibility: Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits [1].

4.3. Verifiability: Watermark should be able to provide full and reliable evidence for the ownership of copyright protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying [1].

4.4. Security: Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection [1].

4.5. Capacity: Image watermarking capacity is evaluation that of how much secret information can be hidden in a digital image. Watermarking capacity is determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder [1].

5. Related Work

Vinita Gupta, Mr. Atul Barve [2] in 2014, here they surveyed the paper on digital image watermarking. They also classified the watermarking techniques based on the transform domain where the watermark is embedded. Also, explain the watermarking properties, applications and techniques used. This paper also shows the different techniques and discusses the important technology called QR code which can be used in future work.

Sasmita Mishra, Amitav Mahapatra, Pranati Mishra [3] in 2013, in this paper, they presented a comprehensive survey on various digital watermarking techniques their requirements and applications. The use of different type of watermark is application dependent. But there are neither type of watermarks are ideal when considering "information preserving" transformations that preserve the meaning of the content & "information altering" transformations that change the expression of the content. To solve this problem a semi fragile watermark is for images which can detect the information altering transformations even after the watermarked contents are subjected to information preserving alterations have to be used.

Prof. Manoj Ramaiya Richa Mishra [4] in 2012, in this paper a new robust watermarking technique for color images was performed. In this paper, the RGB image is converted to HSV and watermarked by using discrete wavelet transform. Watermarking embedded stage and extraction stage is designed using another low power invisible watermarking algorithm. In this, the host signal is an image and after embedding the secret data a watermarked image is obtained and then extracts secret image and original image separately. In future the resulted watermarked image was tested with several attackers to verify the robustness and VLSI implementation of invisible watermarking algorithm using VHDL code and also check various performances like power, PSNR and tamper detection and area, *etc*.

Surya Pratap Singh, Asst. Prof. Paresh Rawat and Prof. Sudhir Agrawal [5] in 2012, this paper shows that the spatial methods are relatively fast and requires low resources and even they can provide comparable performance when compared for attack (only scaling and noise) resilience to transform domain methods but does not resilience with attacks like rotation, compression, blurring and filtering like Gaussian. Hence the transform domain method provides a much better option at higher processing cost. They have also analyzed the techniques in terms of their complexity, robustness and processing time.

Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh [6] in 2013, here they have reviewed some recent algorithms, proposed a classification based on their intrinsic features, inserting methods and extraction forms. Many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with SVD. In this paper they also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, properties of watermarking and its applications have been presented. In future works, the use of coding and cryptography watermarks will be approached.

Manjit Thapa, Dr. Sandeep Kumar Sood and A.P Meenakshi Sharma [8] in 2011, they proposed the algorithm for digital image watermarking method based on singular value decomposition, there are both of the L and U components are explored for watermarking method. This method refers to the watermark embedding procedure. Also for watermark extracting procedure. Digital image watermarking method for copyright protection is robust. The experimental results shows that the quality of the watermarked image is very good & there is strong resistant against many attacks. The image watermarking method help to achieves artificial intelligence. Digital image watermarking is the most effective solution in this & digital watermarking is used to protect the information that is increasingly exponentially day by day. The results show that the quality of the watermarked image is better.

Gurpreet Kaur, Kamaljeet Kaur [9] in 2013, in this paper they use spatial domain method LSB for security of images, which is easy and simple and more effective method. Process of LSB is simple when they used LSB in MATLAB. A different image in MATLAB tells different process steps and their result. In future LSB may also use for other type of data and test on different type of images.

6. Conclusion

In this paper, we present the survey on digital image watermarking. In this paper, we also explain the types of watermarking and various techniques of watermarking and also we explained the requirements of digital watermarking. We also survey on some papers of image watermarking. In future work we can combine watermarking techniques with other techniques of security for data hiding in image and also improve the quality of image and find the best result with the help of PSNR. Previous work has some advantages and disadvantages. So in future we can work on new algorithms of watermarking combine with other techniques that may reduce or remove the disadvantages of previous algorithms.

References

[1] Shraddha S. Katariya, “Digital Watermarking: Review”, International Journal of Engineering and Innovative Technology, ISSN:2277-3754, Volume 1, Issue 2, February 2012.

[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, ISSN:2277 128X, Volume 4, Issue 1, January 2014.

[3] Sasmita Mishra, Amitav Mahapatra,Pranati Mishra, “A Survey on Digital Watermarking Techniques”, International Journal of Computer Science and Information Technologies, ISSN:0975-9646, Vol. 4 , 2013, 451-456.

[4] Prof. Manoj Ramaiya Richa Mishra, “ Digital Security using Watermarking Techniques via Discrete Wavelet Transform”, National Conference on Security Issues in Network Technologies August 11-12, 2012.

[5] Surya Pratap Singh, Asst. Prof. Paresh Rawat and Prof. Sudhir Agrawal, “A Literature Review on Water Marking Techniques”, International Journal of Scientific Engineering and Technology, ISSN:2277-1581, Volume No.1, Issue No.4, pp:21-23, 01 Oct. 2012.

[6] Y. Shantikumar Singh, B. Pushpa Devi, and 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.

[7] M.Mohamed Sathik and S.S.Sujatha, “A Novel DWT Based Invisible Watermarking Technique for digital images”, International Arab Journal of e-Technology, Vol.2, No. 3, January 2012.

[8] Manjit Thapa, Dr. Sandeep Kumar Sood and A.P Meenakshi Sharma, “ Digital Image Watermarking Technique Based on Different Attacks”, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011

[9] Gurpreet Kaur, Kamaljeet Kaur, “Image Watermarking Using LSB (Least Significant Bit)”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN:2277 128X, Volume 3, Issue 4, April 2013.

Authors

Manjinder Kaur, M. Tech, Student, Department of Computer Science Guru Nanak Dev University, Regional Campus Jalandhar, India