A Survey on Watermarking Techniques

Ameena Ahammed[1], Reeba R[2]

[1] PG Scholar, Department of Computer Science & Engineering,
Sree Buddha College of Engineering, Alappuzha, India
ameenamazhuppayil@gmail.com

[2] Assistant Professor, Department of Computer Science & Engineering,
Sree Buddha College of Engineering, Alappuzha, India
reeba.amjith@gmail.com

Abstract

Now a days protection and illegal redistribution of digital media has become an important issue. Because internet is supported by more people. It increases the recording, editing and replication of multimedia data. Digital watermarking can be used to protect digital information from illegal manipulations and distributions. It provides a robust solution to the problem occurs during intellectual property rights for online information. Digital watermarking have applications in different areas like broadcast monitoring, copy right protection etc. This paper reviews different methods of digital watermarking for protecting digital information**.**

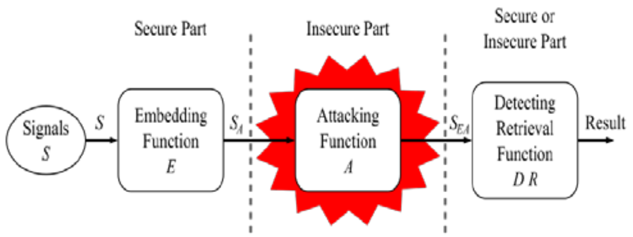
Keywords: *Digital Watermark, DWT or DCT, pseudo noise sequence, ridgelet coefficients Stirmark****.***

1. Introduction

Digital watermarking is the techniques of hiding a message related to a digital signal such as an image, song, video etc. within the signal itself. It is a technique that closely related to steganography, which hide a message inside a digital signal. Watermarking is a technique which hide a message related to the original content of the digital signal, but in steganography the digital signal is not related to the message, and it is just used as a cover to hide its existence.

Watermarking has been found for several centuries, in the form of watermarks found in plain paper and subsequently in paper bills and now a days it is used for many different applications. One of the first applications for watermarking was broadcast monitoring. It is very important to track when a specific video, broadcasted by a TV station and also important to advertising agencies that want to ensure that their commercials are up to date. Watermarking can be used for owner identification. It is very important to identify the owner of a digital work of art, such as a video or image can be quite difficult. Transaction tracking is another application of watermarking. In transaction tracking, the watermark embedded in a digital work can be used to understand transactions taking place in the copy of this work. Copy control is another application for watermarking. In this, watermarking can be used to avoid the illegitimate copying of songs, images of movies, by embedding a watermark in them. A general watermarking scheme must meet requirements such as robustness, imperceptibility, fidelity, payload size, false positive and effectiveness.

There are two groups of model for watermarking process. The first group includes models which are based on a communication-based vision of watermarking and the second group contains models based on a geometric vision of watermarking. Communication based models consider watermarking as a traditional models of communication systems. Watermarking is actually a process of communicating a message from the watermarking encoder to the watermarking decoder. Therefore, it utilizes models of secure communication to model this process. And watermarking is described in geometric terms. In this model, images, watermarked and unwatermarked, can be treated as high-dimensional vectors, called the media space. Geometric models are useful to better visualize the watermarking process based on number of regions with desirable properties of watermarking



.

Fig1. General digital watermark life-cycle phases

In digital watermarking, the data to be embedded in an image is called a digital watermark, sometimes, watermark is considered as the difference between the watermarked image and the cover image. The signal in which the watermark is to be encoded is called the host image. A watermarking system is divided into three distinct phases, embedding or encoding, attack, and detection. Figure 1 shows the three phases of watermark life-cycle. In embedding, an algorithm accepts the host and the data to be embedded or encoded, which results in watermarked signal .Then the watermarked digital signal is stored or usually transmitted to another person. If this person introduces a modification, an attack occur. Detection or extraction is an algorithm which is used to retrieve the watermark from attacked signal. If the signal was modification during transmission, then the watermark doesn't undergo change and it can be extracted. In robust digital watermarking applications, watermark doesn't undergo any modification during attack. In fragile digital watermarking, the extraction algorithm fail to extract watermark, if any change is made to the signal. In this survey, different techniques of watermarking has been reviewed. They are discussed in the following section.

2. Related Works

Y. Xiang [1] proposes a novel dual-channel time-spread echo method for audio watermarking. It increase the robustness and perceptual quality. In the embedding stage, the host audio signal is divided into two sub signals, which are obtained from two audio channels that are virtual. The watermarks are implanted into the two sub signals simultaneously. Then the sub signals embedded with watermarks are combined to form the watermarked image. At the decoding stage, the watermarked signal is split up into two watermarked sub signals. A pseudonoise sequence is used, the large peaks of its auto-correlation function can be used to enhance the performance of extraction. Compared to the present time-spread echo-based methods, the proposed method is robust to attacks and has high resistance to perceptibility.

N. K. Kalantari [2] propose a robust image watermarking scheme in the ridgelet transform domain. So sparse representation of an image which contain line singularities is obtained. For achieving robustness and transparency, the watermark data is embedded in the selected blocks of the cover image by modifying the amplitude of the ridgelet coefficients which represent the most energetic direction. Decoder extracts the watermark data using the variance of the ridgelet coefficients of the most energetic direction in each block. A robust noise estimation scheme is proposed to fulfill the requirements of the decoder such as the noise variance to perform decoding. Implementation of error correction codes and analytical derivation of bit error probability is also carried out.

N. F. Johnson [3] proposes methods which based on inherent features within images that can be used to "fingerprint" images and it is a alternative method for image recovery. These identification marks can be applied to locate images and recover image size and information from distorted images. It does not depend on embedded information and can be used to recover images distorted by various geometric transformations.

E. Nezhadarya [4] propose a robust quantization-based image watermarking scheme, which is called as gradient direction watermarking (GDWM), that is based on the uniform quantization of the direction of gradient vectors. In this method, at multiple wavelet scales, the watermark bits are embedded by quantizing the angles of significant gradient vectors. This scheme increases the invisibility of the embedded watermark because the watermark is embedded in significant gradient vectors and robustness to amplitude scaling attacks because the watermark is embedded in the angles of the gradient vectors, and also increased watermarking capacity as it uses multiple-scale embedding. The gradient vector at a pixel is indicated in terms of the discrete wavelet transform (DWT) coefficients. In order to quantize the gradient direction, the DWT coefficients are modified with respect to the derived relationship between the changes in both the coefficients and the gradient direction.

F. Davoine [5] proposes a compensation technique allowing to retrieve a watermark in an image attacked by random local geometric distortions, with the help of original image or its edges. In order to compensate the parts of geometric distortions that could be caused by Stirmark software, a flexible triangular 2-D mesh is used.

.

J.-S. Tsai [6] propose a novel feature region selection method for robust digital image watermarking. This method tries to select a non-overlapping feature region set, which has the greatest robustness to resist various attacks and can preserve image quality as much as possible after watermarking. In first step it, performs a simulated attacking procedure using some predefined attacks and then evaluate the robustness of every candidate feature region. According to this, a track-with-pruning procedure is used to search a minimal primary feature set which can overcome the most predefined attacks. For enhancing the resistance to undefined attacks under the condition of preserving image quality, the primary feature set is expanded by adding some auxiliary feature regions. This method is formulated as a multidimensional knapsack problem and solution is based on genetic algorithm.

J.Dugelay [7] propose an original blind watermarking algorithm which is robust to local geometrical distortions such as the deformations caused by Stirmark. At insertion step, a predefined additional information is added to the useful message bits. These additional bits are called as resynchronization bits or reference bits. Reference bits are modulated in the same as the information bits. During the extraction step, the reference bits are used as anchor points to estimate and compensate for small changes local and global geometrical distortions. The deformations are estimated using a modified basic optical flow algorithm.

S. Pereira [8] propose a method for the secure and robust copyright protection for digital images. In this method digital watermark is embedded into an image using the Fourier transform. For this purpose watermark included as a template in the Fourier transform domain to make it secure against general linear transformations. This algorithm based on polar maps which accurately and efficiently recover the template in an image which has undergone a general affine transformation.

M. Alghoniemy [9] proposes a method in which the watermark is used in an authentication context. Two solutions are proposed for this problem. Both geometric and invariant moments are used in the proposed techniques. An invariant watermark is designed and tested using attack caused by Stirmark with the use of invariant moments. On the other hand, an image normalization technique is proposed to create a normalized environment for watermark embedding and detection. The proposed algorithms is robust, computationally efficient, and no overhead during transmission.

X. Kang [10] proposes, a blind discrete wavelet transform-discrete Fourier transform (DWT-DFT) composite image watermarking algorithm which resist the alteration of image during both affine transformation and JPEG compression. This algorithm improves the robustness by using new embedding strategy, watermark structure, 2-D interleaving, and synchronization technique. A spread-spectrum-based watermark including training sequence embedded in the coefficients of the LL subband in the DWT domain, also a template is embedded in the middle frequency components in the DFT domain. During watermark extraction, first detect the template of a corrupted watermarked image to obtain the parameters of affine transform for converting the image back to its original shape. Then perform translation registration with training sequence embedded in the DWT domain for finally extracting the informative watermark.

3. Conclusion

Digital watermarking is a method for providing security to the digital content on the internet .Digital watermarking is still remain as a challenging research field with many interesting problems, such as, it does not prevent copying or distribution and cannot withstand every possible attack. In this paper, different techniques of digital image watermarking has been reviewed. Most of the methods proposed in the literature only address the global affine transformation problems (e.g., rotation, scaling, and translation). New technologies to merge existing techniques for considering all possible attacks in watermarking field must come out.

References

[1] Y. Xiang, I. Natgunanathan, D. Peng, W. Zhou, and S. Yu, "A dualchannel time-spread echo method for audio watermarking," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 383–392, Apr. 2012.

[2] N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image watermarking in the ridgelet domain using universally optimum decoder," IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 3, pp. 396–406, Mar. 2010.

[3] N. F. Johnson, Z. Duric, and S. Jajodia, "Recovery of watermarks from distorted images," in Proc. 3rd Int. Workshop Inf. Hiding, 1999, pp. 318–332.

[4] E. Nezhadarya, Z. J. Wang, and R. K. Ward, "Robust image watermarking based on multiscale gradient direction quantization," IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1200–1213, Dec. 2011..

[5] F. Davoine, "Triangular meshes: A solution to resist to geometric distortions based watermark-removal softwares," in Proc. EURASIP Signal Process. Conf., 2000, pp. 493–496.

[6] J.-S. Tsai, W.-B. Huang, and Y.-H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," IEEE Trans. Image Process., vol. 20, no. 3, pp. 735–743, Mar. 2011.

[7] J. Dugelay, S. Roche, C. Rey, and G. Doerr, "Still-image watermarking robust to local geometric distortions," IEEE Trans. Image Process., vol. 15, no. 9, pp. 2831–2842, Sep. 2006.

[8]S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Trans. Image Process., vol. 9, no. 6, pp. 1123–1129, Jun. 2000.

[9] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," IEEE Trans. Image Process., vol. 13, no. 2, pp. 145–153, Feb. 2004.

[10] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 776–786, Aug. 2003.