International Journal of Digital Contents and Applications for Smart Device
Vol.2, No.1, (2015), pp.1-10
http://dx.doi.org/10.21742/ijdcasd.2015.2.1.01

A Survey: Digital Watermarking with its Applications using Different Methods

Khusboo Agrawal[1] and Rajesh Singh[2]

Department of Computer Science & Engineering
NITM Gwalior,
M.P, India
Khusboo02agrawal@gmail.com, raj25682@gmail.com

Abstract

We presented in this survey, digital watermarking is an important method to add hidden patent notices to digital audio, image. The Watermarking techniques with frequency domain make better results either concern with image excellence or invisibility of the watermark. In this paper, we present review on Image Watermarking for Good Robustness. In this paper, we talk about the various factors used in watermarking, properties and application area where water- marking technique requires to be used. Also a survey on the some new work is done in image watermarking field.

Keywords: *DWT; DFT; Applications; Methods*

1. Introduction

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. In general a digital watermark is a technique which allows an individual to add hidden copyright information or other verification message to digital media. The procedure Watermarking is that embeds documents named a digital signature or watermark or label or tag into a multimedia object such that watermark can be detected or mined later to create an assertion about the object. Digital watermark is a sequence of information containing the owners copyright for the multimedia data. It is inserted visibly or invisibly into another image so that it can be extracted later as an evidence of authentic owner. Usage of digital image watermarking technique has grown significantly to protect the copyright ownership of digital multimedia data as it is very much prone to unlawful and unauthorized replication, reproduction and manipulation. The watermark may be a logo, label or a random sequence. A typical good watermarking scheme should aim at keeping the embedded watermark very robust under malicious attack in real and spectral domain. Incorporation of the watermark in the image could be performed in various ways.

Article history:
Received (February 7, 2015), Review Result (April 14, 2015), Accepted (May 16, 2015)

ISSN: 2287-8505 IJDCASD

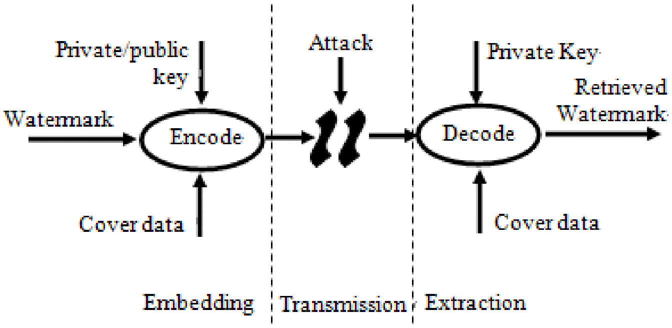


Figure 1. General processes involved in a watermarking system [4]

Digital watermarking hides the patent data into the digital data through some procedure. The secret data to be embedded can be certain text, author‘s serial number, company logo, images with some special significance. This top-secret knowledge is set in to the digital documents (audio, video, and images) to confirm the safety, information certification, documentation of owner and patent security.

The watermark can be unseen in the digital documents either seen or unseen. For a tough watermark set in, a noble watermarking method is wanted to be useful. Watermark can be set in either in spatial or frequency domain. Together the domains are dissimilar and have their individual pros and cons and are used in not like condition. If the pointer was not customized through communication, then the watermark is still here and it can be extracted. If the pointer is unoriginal, then the documents are too accepted in the duplicate. If the signal is unoriginal, then the data is too carried in the duplicate. The set in takes place by operating the element of the digital documents, which means that the data is not set in in the structure from place to place of the documents, it is carried with the signal itself. Among these discrete Fourier transform (DFT) based watermarking algorithms have attracted scientists because of its straightforwardness and several smart mathematical properties of DFT. A preprocessing step before the watermark extraction has been projected which creates the procedure hardy to geometric attack i.e. RST attack. Presentation of this watermarking system has been examined. By estimating the toughness of the procedure against geometric attack counting scaling, rotation, translation and few additional attacks. Experimental results have been compared with existing algorithm which seems to be promising.

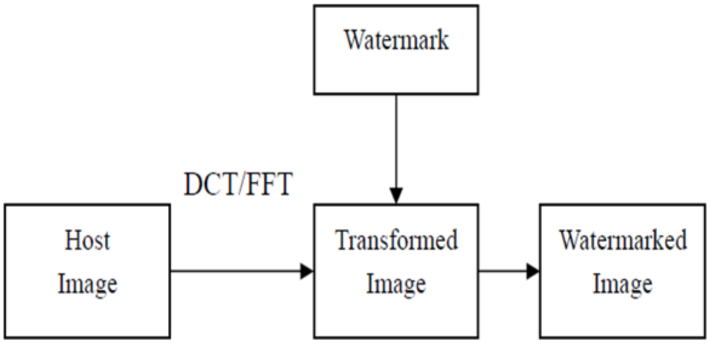


Figure 2. General block diagram of embedding process

2. Requirements of watermarking

2.1. Transparency

The embedded watermark should not corrupt the original image. It is able to be seen distortions are introduced in the image; it creates disbelief and makes life no difficulty for the attacker. It also degrades the commercial value of the image.

2.2. Robustness

This is by far the most important requirement of a watermark. There are various attacks, unplanned (cropping, compression, scaling) and planned attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks.

2.3. Capacity or data load

This quantity defines the extreme quantity of documents that can be set in into the image to ensure proper recovery of the watermark during extraction.

3. Types of watermarking

- **Image watermarking***:* This is useful to the purpose of the unseen the superior data into the image and to later discover and mine that exceptional data for the author‘s rights.
- **Video watermarking:** This is enhances the watermark in the video stream to manage video applications. It is the extension of image watermarking. This technique needs actual period abstraction and strength for compression.
- **Audio watermarking*:*** This presentation area is the greatest standard and hot issue due to internet music, MP3.
- **Text watermarking:** This enhances watermark is to the purpose of the PDF, DOC and additional edition file to avoid the ups and downs prepared to edition. The watermark is introduced in the font form and the space among characters and line spaces.
- **Graphic watermarking:** It set in the watermark to 3D or 2D computer produced graphics to show the patent

4. Related work

Sheetal Sharma (2012), In order to advance the healthiness and imperceptibleness of the procedure, a novel set in and removing process with DWT-SVD is proposed. The approximation matrix of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark to the singular value of DWT coefficient. The planned set in and removing technique was working to speed up the hybrid DWT-SVD watermarking and to ignore the escape of watermark. This hybrid technique leads to optimize both the fundamentally conflicting requirements. The new results display equally the decent robustness under numerous attacks and the great loyalty. The period wanted to execute the package is importantly reduced [6].

Ye Xueyi-In this scheme, the inscribed circle of the original image matrix is selected as the ZM calculation area, and the square of the inscribed circle is chosen to embed watermark.

Firstly, the watermarking embedding area is conducted with 1-level DWT and the low frequency DWT coefficient is divided into non-overlapping blocks; SVD is applied to every block. Secondly, a bit of the watermark is embedded through slight modifications of the singular value (SV) matrix in each block. Finally, some selected ZM of the watermarked image are saved to detect and correct the possible geometric attacks. The simulation has proved that the proposed not just has good resistance to rotation, scaling attacks, and as well, kinds of common signal processing, and can achieve blind extraction [7].

Kazutake Uehira (2014)-In this paper, define about novel feature to assessing the robustness of the visual watermarking method, which is a single method that can enhance watermarked data to objective image documents occupied with digital cameras without any unambiguous additional hardware construction. Still, since these knowledge usages graceful with set in watermarked data, which is exposed onto objective images, the situation of taking an image with digital cameras may disturb the precision with which set in watermarked documents can be identified. [8]

Ravinder Singh (2013) -The Color Image Watermarking is prepared by choosing unique color element from Red, Green, and Blue (RGB) Mechanisms of Color Image. The Watermark set in into some nominated element and then again combines with additional elements. The Red ®Element acting most significant part to the current the color object in addition to it is healthy to the reservation data related with it. So, in this research, Red ®Element is nominated to unseen Watermark. This method is additional protected since the set in watermark can only be mine from the Red Element later decomposing. [9]

Hao-Tang Chan (2013) in this paper represents a fresh alter able delicate watermarking procedure for hologram verification. In the procedure, the watermark is set in in the transform domain. The noticeable hologram is then kept in the spatial domain with the finite resolution level. Due to the uncomplicatedness of the transform, a satisfactory situation on the resolve level of marked holograms is resulting for assuring the reversibility of watermarking. [10]

Mr. Navnath S. Narwade (2013)-discrete fourier transform (DFT) based watermarking algorithms have paying attention scientists because of its uncomplicatedness and certain smart mathematical properties of DFT. A preprocessing step before the watermark extraction has been planned which creates the procedure resilient to geometric attack i.e. RST attack. Presentation of the watermarking system has been examined. By assessing the robustness of the procedure against geometric attack including rotation, scaling, translation (RST). [11]

Mr. Atul Barve (2014)-The paper proposed a colour image watermarking scheme based on the encrypted watermark with QR code and DWT. In this research, we are working on the security enhancement of image watermarking technique with the latest QR codes. The proposed methodology making image watermarking system more secure and robust adding encryption of watermark being embedded in cover image. The advantages of our proposed methodology are the watermark is completely invisible in cover image as well as the encryption process is quite simple but robust in nature .The recovered watermark is about nearest the main watermark. Experimental results show that the proposed algorithm enhances the anti- attack capability and the hidden nature of the image, increases the security of the watermarking detection, and has maximum robustness to cutting, random noise attack and JPEG compression.

5. Methodology

The various watermarking techniques are:

5.1. Spatial domain techniques

Spatial domain watermarking a little modifies the pixels of one or two accidentally selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not dependable when subjected to normal media operations such as filtering or lossy compression.

5.2. Frequency domain techniques

In Frequency domain the protected documents are unseen in the lesser or central frequency portions of the secure image; because of the advanced frequency section is more likely to be suppressed by compression. Another important and difficult topic. Numerous frequency domain methods are as follows:-

5.2.1. Discrete fourier transformation (DFT) 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 [5].

5.2.2. Discrete wavelet transform (DWT) based technique: DWT-based methods enable good spatial localization and have multi resolution features, which are the alike to the social graphic scheme. Similarly this method displays robustness to low-pass and middle cleaning.

5.3. 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 recurring iteratively to produce N scale transform. The Figure 2 below shows the wavelet based transforms:

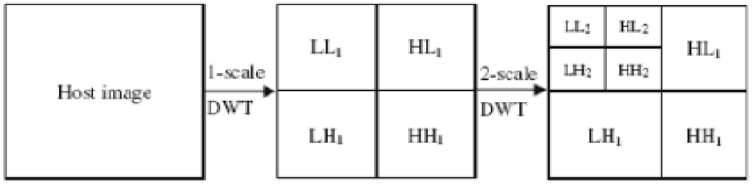


Figure 2. Wavelet based transforms

Digital watermarking techniques are classified according to various criteria like robustness, perceptibility, embedding and retrieval methods. Robustness is an important criterion which means the ability of watermark to resist common image processing operations. Watermarking techniques based on robustness can be further divided into three main categories:

(1) Robust
(2) Fragile
(3) Semi-fragile

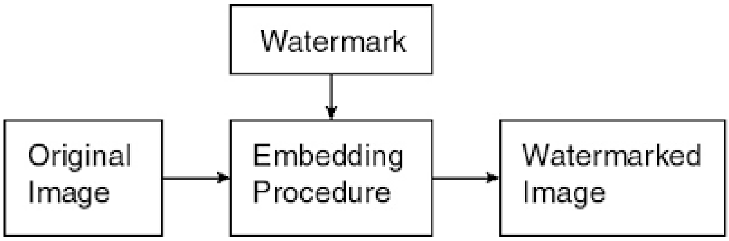


Figure 3. Basic structure of watermarking system

Robust watermarking schemes are applied for proving possession claims whereas fragile watermarking is applied to multimedia content authentication. These watermarking schemes have their own requirements in terms of robustness. Robust watermarks should be able to survive a wide range of friendly operations and malicious attacks, whereas weak watermarks are impossible to both horrible and content preserving operations. Fragile watermarking techniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image verification. Some grave applications similar to medical imagining and forensic image archiving also require the fragile watermarks to be reversible. The different quantitative parameters such as PSNR, True and false positive may be used for the estimate of the technique of watermarking schemes.

6. Application of watermarking

6.1. Copy and playback control

The information accepted by watermark may be as well containing data concerning duplicate and show authorizations. Then, a safe component can be additional in duplicate or playback tools to by design mine this approval data and block further processing if necessary.

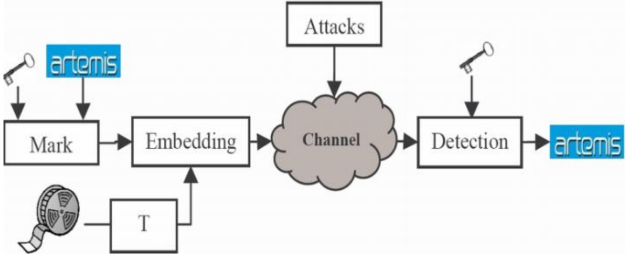
6.2. Fingerprinting

This is alike to the earlier application and agrees to acquisition devices to enclosure information about the specific device (*e.g.*, an ID number) and date of creation [4].

Original Digital Media
Digital Media is Fingerprinted
Digitally Fingerprinted Content

6.3. Watermarking attacks [3]

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing soft wares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under,



6.3.1. Removal attack: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.

6.3.2. Interference attack: Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks.

6.3.3 Geometric attack: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

6.3.4 Low pass filtering attack: A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

6.3.5 Forgery attack: The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.

6.3.6 Security attack: In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

6.3.7 Protocol attack: The protocol attacks do neither aim at destroying the embedded information nor at disabling the ISSN.

7. Conclusion

In this paper we reviewed the current text on digital image watermarking. We described watermarking algorithms based on the transform domain in which the watermark is surrounded. Also, we study the watermarking properties, types, attacks and algorithms used. This paper shows the different methods and their advantages and disadvantages. In this paper we tried to give the complete information about the digital watermarking which will help the new researchers to get the maximum knowledge in this domain.

References

[1] G. Bouridane and A.M.K. Ibrahim, "Digital Image Watermarking Using Balanced Multi wavelets", IEEE Transaction on Signal Processing, Vol. 54, No. 4, pp. 1519-1536, (**2006**).

[2] I.J. Cox, M.L. Miller and J.A. Bloom, "Digital Watermarking", Morgan Kaufmann, (**2001**).

[3] P. Singh and R.S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Vol. 2, No. 9, March (**2013)**.

[4] B. Ram, "Digital Image Watermarking Technique Using DiscreteWavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Vol. 2, No. 4, April **(2013)**.

[5] V. Gupta and A. Barve, "A Review on Image Watermarking and Its Techniques", IJARCSSE, Vol. 4, No. 1, January (**2014)**.

[6] Seema, Sheetal Sharma, "DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality", International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, No. 4, April (**2012)**.

[7] X. Ye, M. Deng, Y. Wang and J. Zhang, "A Robust DWT-SVD Blind Watermarking Algorithm based on Zernike Moments", Communications Security Conference (CSC 2014), pp. 1-6, **(2014)**.

[8] Y. Ishikawa and K. Uehira, "Tolerance Evaluation for Defocused Images toOptical Watermarking Technique", Journal of Display Technology, Vol. 10, No. 2, February (**2014)**.

[9] R. Singh and M. Mathuria, "A Robust Color Image Watermarking using Combination of DWT and DCT", 4th International IT Summit Confluence, (**2013).**

[10] H.T. Chan, W.J. Hwang, and C.J. Cheng, "Digital Hologram Authentication Using a Hadamard-Based Reversible FragileWatermarking Algorithm", Journal of Display Technology, Vol. 11, No. 2, pp. 193-203, Feb. **(2015)**.

[11] N.S. Narwade, N.P. Deshmane, P. Elchatwar and P.L. Pande, "Robust Watermarking for Geometric attackusing DFT", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)Vol. 2, No. 2, March-April (**2013)**.

[12] V. Gupta, A. Barve, "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes", International Journal of Computer Applications ,Vol. 100, No. 14, August (**2014)**.