International Journal of Current Trends in Engineering & Technology
Received 1 June 2018, Accepted 20 July 2018, Available online 31 July 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 04 (Jul-Aug, 2018)

A Survey on Watermarking Method based Image Data Hiding Method

Priyanka Sharma
Assistant Professor,
Computer Science & Engineering Department
Corporate Institute of Research & Technology, Bhopal
Sharma2018.priyanka@gmail.com

Neeraj Sharma
Assistant Professor,
Computer Science & Engineering Department
Corporate Institute of Science & Technology, Bhopal
Neeraj.bpl83@gmail.com

Abstract: *Watermarking algorithmic rule is studied using digital watermarking technology supported the distinct moving ridge discrete wavelet transform multi-resolution decomposition algorithmic rule. Three-level moving ridge decomposition is utilized so images are divided into three serial sub-graphs with the high-frequency band and one sub-graph with the low-frequency band. Since low-frequency data is additionally sensitive to human eyes than high-frequency data, watermarking is embedded into the high-frequency coefficients of the wavelet image. In our experiment, watermarking data is embedded into the initial images by Matlab simulation. This paper presents totally different techniques of digital image watermarking supported special and frequency domain, that shows that spatial domain technique provides security and watermark recovery of watermark image and better PSNR price compared to a frequency domain.*

Keywords: data hiding, wavelet transforms, DFT, spatial localization, watermarking, human visual system, PSNR.

I. Introduction

Electronic commerce, usually referred to as e-commerce, is that the shopping for and commerce of product or service over electronic systems like the internet & different PC networks. Therefore the growth of e-commerce applications within the World Wide internet needs the necessity to extend the protection of information communications over the internet to produce security to those applications encryption and knowledge activity techniques were introduced & developed. There are several approaches like Cryptography, Watermarking and Steganography to transfer the data/image to the supposed user at destination with none modifications. A watermark may be a secondary image that is overlaid on the first image, and provides a method of protective the image [1] .With the event of recent digital technology illegal operation and illegal authorization of the digital product are more and more rampant. Illegal use, copyright impersonation and intentional tampering of digital product wide exist in industrial and non-commercial areas that end in the piracy drawback that greatly affects social development. Affects social development, However, traditional protection technology cannot effectively settle these current issues aimed toward these things, this paper provides some algorithms, particularly the digital image watermarking algorithmic rule supported wavelet transformation, using the imperceptions, robustness, security and watermarking. This algorithmic rule makes an attempt to enhance the protection and hardiness of the watermarking data by choosing and decision making the embedded position and balances the contradiction between imperceptions and hardiness by choosing the embedded intensity issue. This paper embeds the watermarking data into the initial pictures by Matlab simulation and employs several types of attack experiments to check the algorithmic rule. Experiments show that watermarking are often well extracted through several attacks are added, that proves the transparency, robustness, security and easy-to-extract characteristics of the watermarking [2].

II. Digital Image watermarking frameworks

Digital watermarking systems usually include two primary components: the encoder and also the decoder. The inputs are the cover media knowledge, the embedding security key, and watermarks within the watermark encoder. The encoder inserts a machine-readable code (watermark) into audio, video, and pictures with variant embedding algorithms, conceptions, and schemes by modifying physical or electronic media and most watermarking procedures are controlled by non-public keys, that are assigned to the insertion and extraction procedure to extract the watermark data suitably and to warrant basic security. The outputs are the security key and also the watermarked contents within the watermark encoder. A watermark extractor or detector involves a two-step method. Watermark retrieval is that the opening that applies some scrambling algorithms to extract a sequence observed as retrieved watermarks.

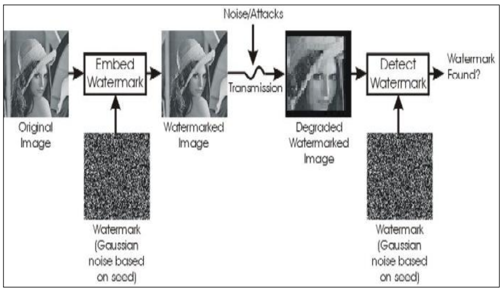
Noise/Attacks
Embed Watermark
Original Image
Watermarked Image
Transmission
Degraded Watermarked Image
Detect Watermark
Watermark Found?
Watermark (Gaussian noise based on seed)
Watermark (Gaussian noise based on seed)

Figure1. Digital Image Watermark frameworks Model

Then, within the second step, in digital watermarking the embedded image watermark are detected and extracted original watermark from a suspected signal of containing watermarks. The second step commonly needs the analysis and comparison of the unreliable watermark with the initial one, and also the consequences can be many types of confidence assessment displaying the similarity between the extracted watermark and also the original one. Digital Watermarking represents a good technique for authentication and ownership right protections. It involves embedding [3].

III. Digital Image Watermarking Classification

Some of the necessary forms of watermarking supported completely different watermarks are given below.

1 Visible watermarks

Visible watermarks are an extension of the thought of logos. Such watermarks are applicable to pictures only. These logos are inlaid into the image however they're clear. Such watermarks can't be removed by cropping the middle a part of the image.

2 Invisible watermarks

Invisible watermark is hidden within the content. It is often detected by an authorized agency only. Such watermarks are used for content and author authentication and for detection unauthorized duplicator.

3 Fragile watermarks

Fragile watermark also is called tamper-proof watermarks. Such watermark is destroyed by knowledge manipulation or in alternative words it's a watermark designed to be destroyed by any variety of repetition or encryption apart from a bit-for-bit digital copy. The absence of the watermark indicates that a replica has been created [4].

IV. Needed Properties of Digital Watermarking

Digital image watermarking issues to resolve some problems properly, thus, this paper highlights the most needs of watermarked image as following:

1. Robustness: The hardiness is that the ability of detection the watermark once some signal process modification like spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation, and alternative operations like digital to analog, analog to digital conversions, cutting, image improvement. Additionally, not all watermarking algorithms have a similar level of hardiness, some techniques are strong against some manipulation operations, however, and that they fail against different stronger attacks. Moreover, it's not continuously desirable for the watermark to be strong, in some cases; it's desired for the watermark to be fragile. Therefore, the hardness is often classified as following [5].

i. Fragile: The watermark in this kind is meant to be destroyed at any reasonable modification, to observe any illegal manipulation, even slight changes, involving incidental and intentional attacks. Fragile watermarks are in the main utilized in content authentication and integrity verification. They use blind detection sort because it is going to be mentioned in Detection varieties. Additionally, the implementation of fragile techniques is simpler than the implementation of strong ones [6].

ii. Semi-fragile: The watermark in this kind is strong against incidental modifications, however fragile against malicious attacks. And it's used for image authentication [7].

iii. Robust: The watermark is designed to be able to survive against incidental and intentional attacks. These types of watermarking are often used in broadcast observance, copyright protection, process, control management [8].

2. Imperceptibility: Imperceptibility (also referred to as invisibleness and Fidelity) is that the most vital requirement in the watermarking system and it refers to the perceptual similarity between the first image before watermarking method and also the watermarked image [5]. In alternative words, the watermarked image ought to look like the first image, and also the watermark should be invisible in spite of occurrence of little degradation in image contrast or brightness. However, the challenge is that imperceptibility might be achieved, however, the hardness and also the capability are reduced, and vice versa, imperceptibility is also sacrificed by increasing the hardness and also the capability. Moreover, the watermark not continually desired to be invisible, sometimes, it's most well-liked to possess visible watermark into the image [8].

3. Security: Security is that the ability to resist against intentional attacks. These attacks intended to alter the aim of embedding the watermark. Attacks varieties are often divided into 3 main categories: unauthorized removal, unauthorized embedding, and unauthorized detection [5]. Consistent with the precise usage of watermarking, the particular feature ought to be available within the watermark to resist the attacks. Therefore, for unauthorized removal, the watermark ought to be strong and to not be removed, and for unauthorized embedding (also referred to as forgery), the watermark ought to be fragile or semi-fragile to sight any modification. Lastly, for unauthorized detection, it ought to be imperceptible watermark [9].

4. Capability: Capacity (also referred to as Payload) refers to the quantity of bits embedded into the image. The capability of a picture might be completely different consistent with the appliance that watermark is designed for [5]. Moreover, finding out the capability of the image will show the USA the limit of watermark data that will be embedded and at a similar time satisfying the imperceptibility and hardiness [10].

V. Literature Survey

Cho *et al.* [11] proposed a fragile algorithm in the wavelet domain to authenticate semi-regular meshes. They first apply several wavelet decompositions on the original triangular mesh and then consider the facets in the obtained coarser mesh as authentication primitives. The basic idea is to slightly modify each facet so that the values of two predefined functions are the same, in order to make all these facets valid for authentication. Both function inputs are invariant to similarity transformations. However, it seems that two problems exist: first, the causality problem occurs because the modification of the current to be-watermarked facet can influence the validities of its already watermarked neighboring facets, and this problem is not mentioned by the authors; secondly, the watermark is inserted in a relatively coarse mesh obtained after several wavelet decompositions, which seems disadvantageous to provide precise attack localization capability.

Mohamed Ali HAJJAJI *et al.* [12] proposed watermarking of medical image, in which a set of data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data. For 10% compression rate, the watermark is successfully recovered. Disadvantage of this technique is that, all the substituted data cannot properly extract when a Gaussian noise is applied in the watermarked image.

Praun *et al.* [13] applied these decomposition and reconstruction methods for watermarking. They picked out the vertex split steps of the reconstruction process that introduced the most significant geometric modifications. For each vertex to be split in these selected steps, they defined a zone containing all its incident facets in the coarse mesh. They then found the corresponding area in the original dense mesh and took this area as the watermark carrier. One bit was inserted in each area by deforming it using a modulation function. Actually, their watermarking technique lies between spatial and classical spectral methods. Here, the multire solution analysis serves to find the "low frequency", salient, spatial parts of the mesh, and the insertion in these parts is supposed to be more robust. Unfortunately, these iterative edge collapse operations are still dependent on the mesh connectivity. Thus, this algorithm is non-blind mainly due to the connectivity recovery before extraction.

Maha Sharkas *et al. [12]* Senior Members IEEE, proposed a dual digital image watermarking technique for improved protection and robustness. They applied frequency domain technique (DWT) into the primary watermark image and then embedded secondary watermark in the form of a PN sequence. The resulting image is embedded into the original image to get the watermarked image. They applied compression, low pass filtering, salt and pepper noise and luminance change attack into the watermarked image to increase the robustness of then technique. In all four attacks secondary watermark was detectable.

Meenakshi Sharma *et al.* [14] in, 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.

Koushik Pal *et al.* [15] proposed biomedical image watermarking technique, modified bit replacement algorithm in spatial domain, which is much better than the conventional simple LSB technique. They embedded multiple copies of the same information in several bits of the cover image starting from the lower order to the higher orders. So even if some of the information is lost due to an attack, they still collect the remaining information and recover the watermark from the cover image using the bit majority algorithm.

Xiang-Gen Xia *et al.* [16] proposed a watermarking technique based on the Discrete Wavelet Transform (DWT). They perform two–level decomposition using the Haar wavelet filters. The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the DWT transformed image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and half toning were performed on the watermarked images.

.

VI. Expected Outcome

In a study in the field of the watermark could also be of a visible or invisible kind and every methodology has its own strengths and weaknesses. The standard of watermarked pictures is measured in terms of PSNR (Peak Signal to Noise Ratio) and notice is reliable image, authentication, information hiding and sensible hardiness.

VII. Conclusion

In this paper, we present the survey on digital image watermarking. During this paper, we additionally make a case for the categories of watermarking and numerous techniques of watermarking and additionally we explained the necessities of digital watermarking. We additionally survey on some papers of image watermarking. In future work, we can mix watermarking techniques with different techniques of security for knowledge activity in an image and additionally improve the standard of the image and notice the simplest result with the assistance of PSNR. Totally different techniques of digital image watermarking supported spatial and frequency domain techniques are mentioned. On the premise of higher than survey, it's clear that spatial domain is most generally used the technique because the watermark will with success and simply be recovered if the image has been cropped or translated. As compared to the frequency domain. On the opposite hand, frequency domain provides additional security however at constant time recovery of the watermark at the receiver finish is more difficult because the quality will increase. Successful recovery of watermark can't be provided by the frequency domain techniques.

Reference

[1]. Manpreet Kaur, Sonika Jindal, Sunny Behal "A Study of Digital Image Watermarking" IJREAS Volume 2, Issue 2, ISSN: 2249-3905, pp. 126-136, February 2012.

[2]. Zhu Xiaosong, Mao Yaowu, Dai Yaowei, Wang Zhiquan, "HVSbased wavelet watermarking scheme "Journal of Nanjing University of Science and Technology, Vol.25 No.3:262-268, Jun.2001.

[3]. Usha Pal, Dinesh Chandra, "SURVEY OF DIGITAL WATERMARKING USING DCT", International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 4 No. 09 Sep 2012.

[4]. F. A. P. Petitcolas, R.J. Anderson, R. J. and M. G. Kuhn, "Information hiding - A survey," Proceedings of the IEEE, Volume 87, Issue 7, 1999, pages 1062-1078.

[5]. M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, Digital Watermarking and Steganography: Morgan Kaufmann Publishers, 2008.

[6]. N. Cvejic, "Algorithms for Audio Watermarking and Steganography," Department of Electrical and Information Engineering, University of Oulu, 2004

[7]. S. Jun and M. S. Alam, "Fragility and Robustness of Binary Phase-Only-Filter-Based Fragile/Semi fragile Digital Image Watermarking," Instrumentation and Measurement, IEEE Transactions on, vol. 57, pp. 595-606, 2008.

[8]. L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in Information and Communication Technologies, 2005. ICICT 2005. First International Conference on, 2005, pp. 337-341.

[9]. C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE, vol. 90, pp. 64-77, 2002.

[10]. R. F. Olanrewaju, "Development of Intelligent Digital Watermarking via Safe Region," PHD, Electrical and Computer Engineering, International Islamic University Malaysia, Kulliyyah of Engineering, 2011.

[11]. W. H. Cho, M. E. Lee, H. Lim, and S. Y. Park, "Watermarking technique for authentication of 3-D polygonal meshes," in Proc. of the International Workshop on Digital Watermarking'05, 2005, pp. 259 270.

[12]. Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey BOURENNANE, "A Watermarking of Medical Image: Method Based "LSB"", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 12, December 2011, ISSN 2079-8407, pp. 714-721.

[13]. E. Praun, H. Hoppe, and A. Finkelstein, "Robust mesh watermarking," in Proc. of the ACM SIGGRAPH Conference on Computer Graphics'99, 1999, pp. 49–56.

[14]. Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, Senior Member IEEE, "A Dual Digital-Image Watermarking Technique" World Academy of Science, Engineering and Technology 5 2005, pp. 136-139.

[15]. 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 .

[16]. Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce, "A Multiresolution Watermark for Digital Images" Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.