International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 05 (SEPTEMBER-OCTOBER, 2016)

A Survey on Digital Image Watermarking Based on DCT and NPA

Ankita Agrawal, Anubha prajapati
Department of CSE
O.I. S.T, Bhopal (M.P.), India

Abstract: - A digital image watermarking technique has been as a possible declaration to the necessity of modifying, copyright protection and authentication of transmission data in an exceedingly much networked setting, it makes possible to identify the author, owner, approved client of document victimization Discrete Cosine Transformation technique were developed in recent years. As a results of it's going to recover the watermarked data back to the first host image reversible watermarking algorithms are appropriate for military, medical and completely different fields. We proposed a new propose algorithm (NPA) supported reversible bit replacement technique in watermarking rule supported bit replacement methodology. It will entirely recover the first data to a high extent, however even have strong robust and hard quality and recover time also minimum as compare to DCT The watermark is superimposed in choose coefficients with necessary image energy at intervals the transform domain. Benefits of the technique improved resistance to attacks on the watermark, hidden visual masking utilizing the time-frequency localization property of transform domain. Digital image watermarking that doesn't want the first image for watermark detection and purpose reversible technique is strong robust and provide ownership, protection.

Keywords: - Digital watermarking, DCT, NPA, Robustness, Embedding Method

I. INTRODUCTION

Digital information is available in World Wide Web in the appearance of Images, Audio and video in huge amount. It is very simple to create duplicate copy of digital information, to spread this data, to manipulate and obliterate by the impostors. Therefore it is required for shielding the integrity of the multimedia information. Hence, the techniques which are essential to keep away from illegal replication or moderation of digital data. This technique is named as Digital Watermarking. The digital watermarking is a process of information hiding. There are various techniques for hiding the information in the form of digital contents like image, text, audio and video. Basically digital watermarking is a method for embedding some secret information and additional information in the cover image which can later be extracted or detected for various purposes like authentication, owner identification, content protection and copyright protection, etc. The digital watermarking is used for the security of the digital content and to protect the data from illegal users and provides the ownership right for the digital data. The efficiency of digital watermarking algorithms is totally based on the robustness of the embedded watermark against various types of attacks.

1. Digital Watermarking Technology

Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author's serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario.

2. Digital Image Watermarking Working

Digital Watermarking is a technique which is used in the digital signal processing of embedding hidden information into multimedia data. This information is not usually visible, only dedicated detector or extractor can seen and extracts that information. Digital Image Watermarking use digital image for embedding the hidden information, after embedding the watermarked image is generated and the watermarked image is more robust against attacks. Figure 1 shows the stages of digital watermarking. Basically working of digital image watermarking can be divided in three stages [1]

A. Embedding Step

The embedding stage is the first stage in which the watermark is embedded in the original image by using the embedding algorithm and the secret key. Then the watermarked image is generated. So the watermarked image is transmitted over the network.

B. Distortion/Attack Step

In this stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.

C. Detection/Retrieval Step

In the detection stage, the watermark is detected or extracted by the dedicated detector from the watermarked image by applying some detection algorithm and by using secret key. In addition to this, noise is also detected.

3. Digital Image Watermarking Techniques

Digital watermarking contains various techniques for protecting the digital content. The entire digital image

watermarking techniques always works in two domains either spatial domain or transform domain. The spatial domain techniques works directly on pixels. It embeds the watermark by modifying the pixels value. Most commonly used spatial domain techniques are LSB. Transform domain techniques embed the watermark by modifying the transform domain coefficients. Most commonly used transform domain techniques is DCT, DWT and DFT. For achieving the robustness and imperceptibility, the transform domain techniques are more effective as compare to the spatial domain.

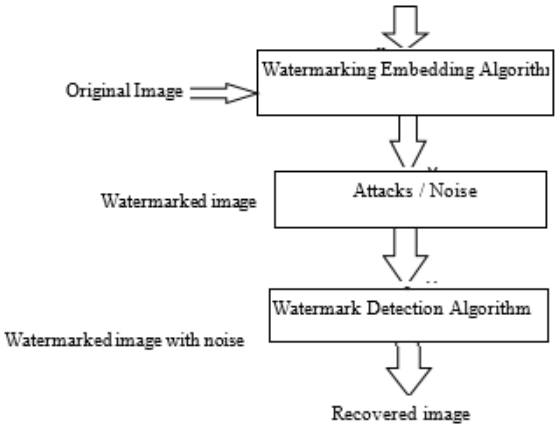

Fig 1: Stages in Digital Image Watermarking

4. Spatial Domain Watermarking:

The spatial domain represents the image in the form of pixels. The spatial domain watermarking embeds the watermark by modifying the intensity and the color value of some selected pixels [3]. The strength of the spatial domain watermarking is:

A. Simplicity.

B. Very low computational complexity.

C. Less time consuming.

The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is LSB.

5. Least Significant Bit (LSB)

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking [3]. Image: 10010101 00111011 11001101 01010101…. Watermark: 1 0 1 0….. Watermarked Image: 1001010**1** 0011101**0** 1100110**1** 0101010**0**….. The main advantage of this method is that it is easily performed on images and it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade. The main drawback of LSB technique is its poor robustness to common signal processing operations because by using this technique watermark can easily be destroyed by any signal processing attacks.

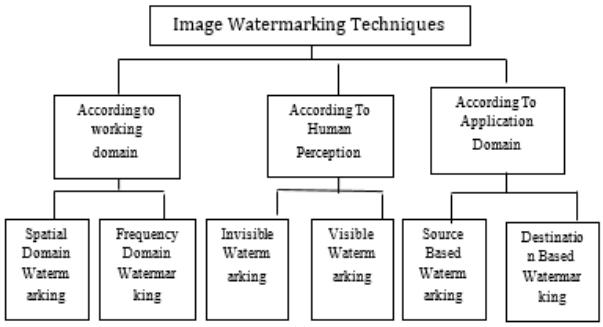

Fig 2: Techniques of Digital Image Watermarking [2]

5.1 Limitations of spatial domain watermarking

The spatial domain watermarking is simple as compared to the transform domain watermarking. The robustness is the main limitation of the spatial domain watermarking. It can survive simple operations like cropping and addition of noise.

6. Transform Domain Watermarking

In the transform domain watermarking, the image is represented in the form of frequency. In the transform domain watermarking techniques, firstly the original image is converted by a predefined transformation. Then the watermark is embedded in the transform image or in the transformation coefficients. Finally, the inverse transform is performed to obtain the watermarked image. [4] Most commonly used transform domain methods is Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT).

7. Discrete Cosine Transform

Discrete Cosine Transform (DCT) used for the signal processing. It transforms a signal from the spatial domain to the frequency domain. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DCT watermarking is more robust as compared to the spatial domain watermarking techniques. In DCT, for embedding the watermark information, we divide the image into different frequency bands. In Fig: 3 FL denotes the lowest frequency component of the block, while FH denotes the higher frequency component and FM denotes the middle frequency component. The literature survey deals mainly with middle frequency bands. The embedding of watermark in a middle frequency band does not spread out to the important visual important parts of the image i.e. the low frequencies. It does not overexpose them to remove through image compression and noise attacks where high frequency components are chosen.

8. Discrete Wavelet Transform

Discrete wavelet transform (DWT) of the image produces multi resolution representation of an image. DWT divides the image into high frequency quadrants and low frequency quadrants. The low frequency quadrant is again split into two more parts of high and low frequencies and this process is repeated until the signal has been entirely decomposed. DWT decomposes the image into sub bands of different resolutions [5]. Whenever image is delivered decompositions of an image can be done at different DWT levels through series of low pass and high pass filters. This allows us to use higher energy watermarks in important regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH, HL, and HH).

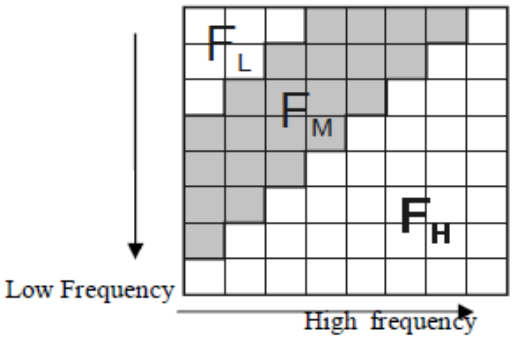

Fig: 3 Discrete Cosine Transform Regions

8.1 **Demerits of DWT over DCT**

The main disadvantage of DWT is that the DWT is more complex than the DCT. The other drawback is that computation cost is higher and its computation time is longer.

9. Discrete Fourier Transform

Discrete Fourier Transform (DFT) offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT decomposes an image in sine and cosine form. The DFT based watermark embedding techniques are divided in two types: one is the direct embedding and the other one is the template based embedding. According to the direct embedding technique the watermark is embedded by modifying DFT magnitude and phase coefficients. The template based embedding technique introduces the concept of templates. A template is structure which is embedded in the DFT domain to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, and then the detector is used to extract the embedded spread spectrum watermark.

9.1 Disadvantage of DFT over DWT and DCT

The main disadvantage of the DFT is that the output of the DFT is always in complex value and it requires more frequency rate. Its computational efficiency is very poor. So, the DFT not used because of these disadvantages.

10. Application of DWT Fingerprinting

Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared. Copyright Protection: When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence. Security: In the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports. Image and Content Authentication: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place. Tamper Detection: Temper detection is used to disclose alterations made into an image. It is closely related to authentication. If tampering is detected in an image, then the image is considered inauthentic. Medical Application: Patients Information can be printed on the X-ray reports and MRI scans using techniques of visible watermarking.

II. LITERATURE SURVEY

Baisa L. Gunjal et al. [5]. "An Overview of Transform Domain Robust Digital Image Watermarking Algorithms'' Aim of this paper is to provide complete overview of Digital Image watermarking. The study focuses on quality factors essential for good quality watermarking, Performance evaluation metrics (PSNR and Correlation Factors) and possible attacks. The paper recommends DWT based techniques for achieving Robustness in Digital Image Watermarking.

Y. Shantikumar Singh et al. [6] "A Review of Different Techniques on Digital Image Watermarking Scheme''. In this paper we mainly discussed about two methods via spatial domain and frequency domain. In spatial (pixel) domain, watermark is inserted directly by modifying the pixel values of host image. Such algorithms are very easy at the time of implementation. However they have some problems like Low hiding capacity of watermark information, less PSNR, less correlation between original and extracted watermark and less security, so anyone can detect such algorithms. In frequency domain such as DCT, DFT, DWT etc, the watermark is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against watermarking attacks because information can be spread out to entire image.

Anoopa Arya et al. [7] "Digital Watermarking Analysis using DCT and DWT." In the paper the digital watermarking is discussed with the cryptographic encryption and decryption technique. We are proposing the watermark extraction using both DCT and DWT technique. In this paper the MATLAB simulation is carried out for digital watermarking using both DCT and DWT algorithms. It is noticed that the simulation time for the DCT is 1.48 seconds and for DWT it is 0.9 seconds for the same size of image. It is tested on 10 images. So, it can be estimated that DWT is much faster than DCT.

Preeti Parashar et al. [8]. "A Survey: Digital Image Watermarking Techniques". This paper presents a survey on the existing digital image watermarking techniques. In this paper, survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, DFT) this survey analyses the limitations and strengths of the watermarking methods. Digital watermarking is still a challenging research field with many interesting problems, like it does not prevent copying or distribution and also cannot survive in every possible attack.

Arisudan Tiwari et al. [9] "Digital Watermarking Encryption and Decryption Using DWT." The paper focuses on the MATLAB simulation of watermark Decoding scheme using Discrete Wavelet Transform (DWT) The watermarking scheme is simulated successfully in MATLAB. The work is carried out for images. The limitation of the watermarking algorithms implemented is that the processing needs to be done pixel-by-pixel. In future, we are aiming to investigate block-by-block processing.

Meenu Singh et al. [10] "Digital Image Watermarking Techniques: A Survey." This paper then categorizes the various watermarking techniques into numerous categories dependent upon the domain in which the concealed data is inserted. We have also provided the comparative analysis of these techniques that can help us to know the positive and negative of these techniques. This comparison can further be used to improvise and propose various new techniques for the same. This paper provides thorough outline of Digital Image Watermarking techniques in spatial domain as well as transform domains. The Transform domain based watermarking techniques are recommended to achieve robustness. This survey on different digital watermarking techniques shows different robustness level on different attacks.

Dr. K. Sathiyasekar et al. [11] "A Research Review on Different Data Hiding Techniques" Data transmission needs security. Data hiding can be achieved through many methods. Different data hiding techniques are discussed in this paper which includes watermarking, steganography, fingerprinting, cryptography and digital signature. Since internet provides images, audio and video in digital form, distributing copies of copyright material are avoided by adding data hiding methods.

Das et al. [12]. "Steganography and Steganalysis: Different Approaches" The authors have mainly focused on how steganography can be used and combined with cryptography to hide sensitive data. In this approach they have explained and listed various methods like Plaintext Steganography, Still Imagery Steganography, Audio, Video Steganography and IP Datagram Steganography which can be used to hide data. The authors have also elucidated the Steganalysis process which is used to detect if steganography is used for data hiding.

Shihadeh Alqrainy et al. [13] "A Survey of Digital Image Processing Techniques in Character Recognition" This paper presents a brief overview of digital image processing techniques such as image restoration, image enhancements, and feature extraction, a framework for processing images and aims at presenting an adaptable digital image processing method for recognition of characters in digital images. More research is needed though in order to improve the prevailing issues (software performs well either in terms of accuracy or speed but not better) with regard to digital imaging. Recognition of characters helps in capturing the best photographs and images that are visible both closely and from a distance.

III. CONCLUSION

A digital image watermarking algorithm based on the secondary LSB replacement, DCT-DWT and SVD which allows near lossless recovery of the original host image. This algorithm not only can recover the original host image to a high extent, but also have good performance in robustness, hiding ability and computing complexity. The embedding capacity of this algorithm is mainly decided by the ratio between the size of the host image and watermark. Also, the main defect of this algorithm is the low embedding capacity, the algorithm may fail. Focused on improving the reversibility and performance of the algorithm. Digital image watermarking technique based on discrete wavelet transform and discrete cosine transform has been presented, where the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficients. The watermark is added in select coefficients with significant image energy in the discrete wavelet transform domain in order to ensure ability of the watermark.

REFERENCE

[1]. L. Robert and T. Shanmugapriya," A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no.2, (2009) May.

[2]. Chirag Sharma, Deepak Prashar, "DWT based robust technique of watermarking applied on digital Images", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-2, May 2012.

[3]. N. Chandrakar and J. Baggaa, "Performance Comparison of Digital Image Watermarking Techniques:A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[4]. F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes", Pattern Recognition Letter (2013).

[5]. Baisa L. Gunjal, R.R Manthalkar, "An Overview of Transform domain Robust Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences" Volume 2, 2010.

[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]. Arisudan Tiwari, Anoopa Arya, Shubham Shukla, "Digital Watermarking Analysis Using DCT And DWT'' International Journal of Emerging Technology and Innovative Engineering Volume I, Issue 6, June 2015 (ISSN: 2394 – 6598).

[8]. Preeti Parashar, Rajeev Kumar Singh, "A Survey: Digital Image Watermarking Techniques'' International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014).

[9]. Arisudan Tiwari, Anoopa Arya, Shubham Shukla, "Digital Watermarking Encryption and Decryption Using DWT'' International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 02 Issue: 02 www.irjet.net.

[10]. Meenu Singh, Abhishek Singhal and Ankur Chaudhary "Digital Image Watermarking Techniques: A Survey.'' International Journal of Computer Science and Telecommunications [Volume 4, Issue 6, June]

[11]. Dr. K. Sathiyasekar, S. Karthick Swathy, and Krishna K.S, "A Research Review On Different Data Hiding Techniques'' International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 3 Issue 1, 2014.

[12]. Soumyen du Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications, pp. 1-11.

[13]. Shihadeh Alqrainy, Mahmud S. Alkoffash, Hasan Muaidi "A Survey of Digital Image Processing Techniques in Character Recognition'', IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March.