Digital Image Watermarking using Spread Spectrum Technique under DWT Domain

Jobenjit Singh Chahal[1]
Research Scholar: Department of CSE
CTIEMT Shahpur (Jalandhar), India

Shivani Khurana[2]
Assistant Professor: Department of CSE
CTIEMT Shahpur (Jalandhar), India

***Abstract* - In the recent few years, it has become a daily need to distribute digital images as a part of widespread multimedia technology by means of the World Wide Web. Digital Image Watermarking techniques have been developed to protect digital images from illegal reproductions and illegal modifications. So these techniques have developed widely to maintain the broadcasting media and content authentication, broadcast monitoring, tamper detection, copyright protection, and many other applications. This paper highlights a new scheme for Digital Image Watermarking using Spread Spectrum Technique under DWT Domain. It starts with the general watermarking procedure, the attributes and applications of Digital Image Watermarking and attacks on Digital Image Watermarking. Moreover, the experimental results showed that the proposed scheme provides better quality of watermarked images in terms of watermark invisibility to human eyes and low data payload during embedding and extraction process. In addition, some possible attacks on watermarked images are discussed. To check the Imperceptibility and Robustness, Peak Signal Noise Ratio (PSNR) is being used.**

General Terms

World Wide Web (WWW), Digital Image Watermarking, Spread Spectrum, Discrete Wavelet Transform (DWT).

Keywords
Tamper detection, Copyright protection, Imperceptibility, PSNR.

1. INTRODUCTION

The term 'Digital Watermarking' was first appeared in 1993, when Tirkelpresented two watermarking techniques to hide the watermark data in the images [1]. Security of digital data has become a popular topic due to the rapid development of the widespread multimedia technology by means of computer networks. With the increasing use of internet, copyright protection for multimedia data has become an important issue. The traditional information security technology based on cryptography theory has its own limitations. In order to resolve the shortcomings of traditional information security technology, more and more researchers have been focusing on the study of the Digital Image Watermarking technology because it can effectively compensate for the deficiencies of the security and protection application of traditional information security technology. The watermark information can be copyright information, authentication information or controlling information so as to determine the copyright owner of the digital data. To certify the authenticity and integrity of multimedia content, control copying according to the embedded control information, achieve the purpose of copyright protection. The Digital Image Watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and labeling the user information. It has become a very important field in information hiding.

In this paper we proposed performance analysis of a new Digital Image Watermarking scheme based on Spread Spectrum technique under Discrete Wavelet Transform (DWT) Domain. Watermarking scheme quality is determined using robustness, transparency and capacity. Transparency means after insertion of watermark the original image should not be distorted [2, 3]. Robustness is related to attacks. If watermark removal is difficult to various attacks like rotation, scaling, compression, noise then watermarking scheme is robust [4, 5]. Capacity means the amount of information inserted intothe original image.

2. DIGITAL IMAGE WATERMARKING

The process of embedding a watermark in a multimedia object is termed as watermarking. Digital watermarking is the best solutions for copyright protection of multimedia data. This technique is mostly used because it does not increase overhead. In this paper we make plan to present a new watermarking algorithm that can embed watermark in the original image without affecting the imperceptibility and it can extract blindly from the watermarked image.

2.1 General Watermarking Procedure

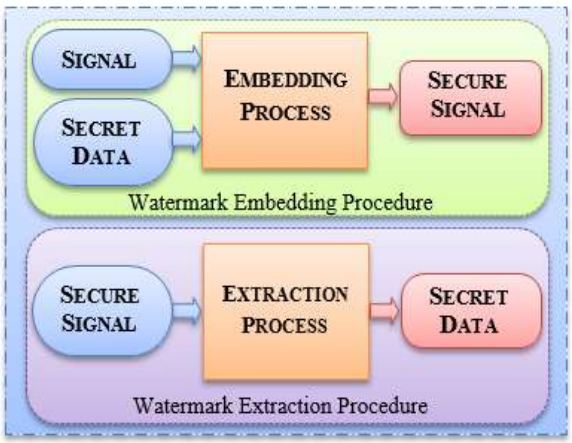

Fig 1: Block Diagram for Watermarking Procedure

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove [5]. The signal may be audio, pictures or video. In this paper image is the signal, and the watermark is the secret data. The watermark is embedded to the original image in embedding process and extract the same watermark in the extraction process from watermarked image.

2.2 Attributes of Digital Image Watermarking

The requirements for Digital Image Watermarking can be treated as characteristics, properties or attributes of Digital Image Watermarking. Different applications demand different properties of watermarking. Requirements of Digital Image Watermarking vary and result in various design issues depending on applications and purpose. These attributes need to be taken into consideration while designing watermarking system. There are five basic requirements as follows [6].

2.2.1 Robustness

The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning, printing, lossy compression, translation, scaling, and rotation [7]. Watermarks should not be removed intentionally or unintentionally by simple image processing operations. Hence watermarks should be robust against variety of such attacks. Robust watermarks are designed to resist normal processing. On the other hand, fragile watermarks are designed to convey any attempt to change digital content.

2.2.2 Fidelity

Fidelity (also known as Imperceptibility and Invisibility) is the most significant requirement in watermarking system, and it refers to the similarity of un-watermarked and watermarked images [6]. In other words fidelity can be considered as a measure of perceptual transparency or imperceptibility of watermark. This perspective of watermarking exploits limitation of human vision. Watermarking should not introduce visible distortions as it reduces commercial value of the watermarked image.

2.2.3 Data Payload

Data payload (also known as capacity) refers to the number of bits embedded into the original image. The data payload of an image could be different according to the application that the watermark is designed for [7]. It is the maximum amount of information that can be hidden without degrading image quality. It can be evaluated by the amount of hidden data. This property describes how much data should be embedded as a watermark so that it can be successfully detected during extraction process.

2.2.4 Security

Secret key has to be used for embedding and detection process in case security is a major concern. Security is the ability to resist against intentional attacks.

2.2.5 Computational Complexity

The cost is the reason behind studying the complexity, so it should be at a reasonable cost [8]. Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. To ensure security and validity of watermark, more computational complexity is needed. Conversely, real-time applications necessitate both speed and efficiency.

2.3 Applications of Digital Image Watermarking

There are diverse applications of Digital Image Watermarking. These are listed as follows [6]:

2.3.1 Copyright protection

The copyright information can be embedded as a watermark into the new image. In case of dispute of ownership, this watermark can provide evidence [6].

2.3.2 Broadcast Monitoring

This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not [6].

2.3.3 Tamper Detection

Fragile watermarks are used for tamper detection. If the watermark is degraded or destroyed, it indicates the presence of tampering and hence digital content cannot be trusted.

2.3.4 Authentication and Integrity Verification

Content authentication is able to detect any change in digital content. Integrity verification can be achieved by using fragile or semi fragile watermark which has the low robustness to modification of an image [6].

2.3.5 Fingerprinting

Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared [6]. This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient.

2.3.6 Content Description

The watermark can contain some detailed information of the host image such as labeling and captioning. The capacity of watermarking for this kind of application should be relatively large and there is no strict requirement of robustness.

2.3.7 Medical Applications

Digital Image Watermarking can also be used in medical images to protect the patient information from unauthorized people. Protection and authentication of such images are now becoming increasingly very significant in the telemedicine field where images are easily distributed over the internet.

2.4 Attacks on Digital Image Watermarking

Digital Image Watermarking attacks can be classified to geometric and non-geometric attacks. An attack succeeds if it weakens the watermark less than acceptable limits [6].

2.4.1 Geometric attacks

Geometric attacks are a set of parameters that can be applied to the image. In other words geometric attacks are basic geometric transformations in an image. These attacks may include rotation, cropping, scaling, warping, translation etc. these attacks attempt to destroy synchronization of detection.

2.4.2 Non Geometric Attacks

Non Geometric attacks (also known as signal image processing attacks) are common image processing attacks which include compression of image, averaging, filtering, brightness, sharpening, printing, scanning, addition of noise, gamma correction etc.

3. THE PROPOSED SCHEME

Based on Spread-Spectrum technique under DWT domain, we proposed a new watermarking algorithm for Digital images. The proposed algorithm is divide into three parts, Create Watermark, Watermark Embedding and Watermark Extraction.

3.1 Create Watermark

Let g (m, n) be the original image to be watermarked with the binary image w (m_1, n_1). In this process we create the binary image with the help of a function Fe. The function Fe takes the parameters of the original image and creates the binary image such that $m=m_1$ and $n=n_1$. The function Fe is working on the basis of spread-spectrum technique. Let me shown the create watermark process with the help of an example in Fig 2.

Fig 2: Create Watermark Process

3.2 Watermark Embedding

Step One: The Discrete Wavelet Transform is applied to the original image g (m, n). The Fig 3 shows the 3-level DWT decomposition of an image.

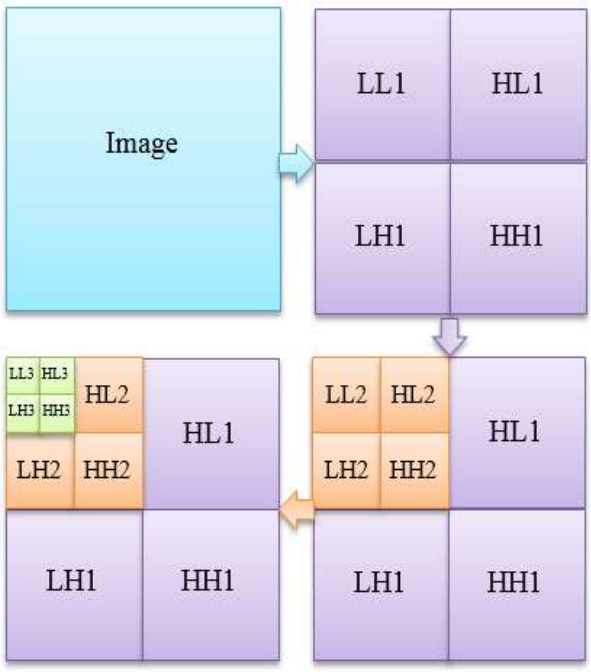

Fig 3: 3-Level Discrete Wavelet Decompositions

Step Two: The binary image w (m_1, n_1) is embedded to the original decomposed image.

Step Three: The decomposed components of the original image and the binary image are multiplied by a scaling factor and are added in the embedding process.

Step Four: Inverse DWT transformation is performed.

Step Five: Store the resulting image wi (m, n).

The resulting image wi (m, n) is watermarked image. We will able to embed binary image without affecting the imperceptibility of the original image. Fig 4 shows the block diagram of watermark embedding process.

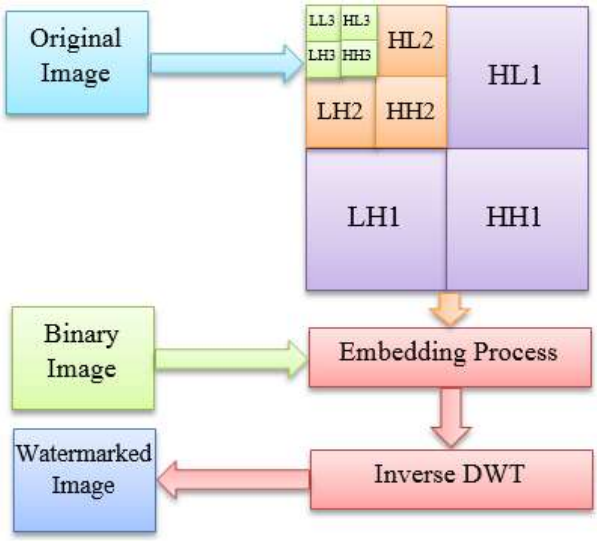

Fig 4: Watermark Embedding Process

3.3 Watermark Extraction

Step One: The Discrete Wavelet Transform is applied to the watermarked image wi (m, n).

Step Two: The decomposed components of the watermarked image are analyzed and the binary image is create in extraction process.

Step Three: Store the binary image.

The resulting binary image is the watermark extracted from watermarked image. The extraction process blindly detect watermark from watermarked image in proposed scheme. The block diagram of extraction process is shown in Fig 5.

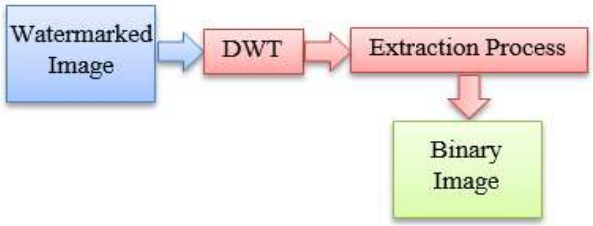

Fig 5: Watermark Extraction Process

4. EXPERIMENTAL RESULTS

Several experiments are presented to demonstrate the performance of the proposed approach. The color images "Lena" of size (256*256) and "Baboon" of size (349*350) are used as the original images. These images are shown in Fig 6(a) and (b). Fig 6(c) and (d) illustrates the created watermark images, respectively.

Fig 6: (a) Lena (256*256) (b) Baboon (349*350)

Fig 6: (c) Lena Watermark (b) Baboon Watermark

To check the efficiency of proposed algorithm different size of images are considered as shown in Fig 6(a) and (b). The Fig 7(a) and (b) shows the watermarked images with respect to 6(a)-(c) and 6(b)-(d).

Fig 7: (a) Watermarked Lena (b) Watermarked Baboon

Table 1 shows the results of proposed approach.

Without Attack	**Lena**	**Baboon**
Between Original and Watermarked images	57.6689	56.5642
Between Original and Extracted Watermarks	∞	∞

Table 1: Results of Proposed Algorithm

For comparing the similarities between the original image with the watermarked image and the original watermark with the extracted watermark, the PSNR (Peak Signal Noise Ratio) is used.

To check the efficiency of proposed approach after attacks on watermarked images. We performed cropping of Fig 7(a) and editing of Fig 7(b) which shows in Fig 8(a) and 8(b). The extracted watermarks of Fig 8(a) and 8(b) are shown in Fig 8(c) and 8(d) respectively.

Fig 8: (a) Cropped Lena (b) Edited Baboon

Fig 8: (c) Extracted watermark (d) Extracted watermark

Table 2 shows the results of proposed approach after attacks on watermarked images.

After Attack	**Lena (Cropping)**	**Baboon (Editing)**
Between Original and Attacked images	37.2354	17.6272
Between Original and Extracted Watermarks	87.2149	24.3368

Table 2: Results of Proposed Algorithm after attacks

5. CONCLUSION

The Digital Image Watermarking is progressing very fast and various researchers from various fields are focusing to develop robust watermarking schemes. In this paper, a new approach based on spread-spectrum technique under discrete wavelet domain has been introduced. The experimental results showthat PSNR has been improved which means better quality watermarked image has obtained. Finally, it reviews the robustness of watermark against various possible attacks.

6. REFERENCES

[1] R.G. Schyndel, A. Tirkel, and C.F. Osbome, "A Digital Watermark". IEEE International conference on Image Processing ICIP-1994, pp. 86-90.

[2] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding". IBM Systems Journal, vol. 35, no. 3&4, pp. 313-336, 1996.

[3] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia". IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, December 1997.

[4] JJKO Ruanaidh, W. J. Dowling and F. M. Boland, "Watermarking digital images for copyright protection". IEEE Proceedings – Vision, Image and Signal Processing, vol. 143, no. 4, pp. 250-256, August 1996.

[5] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data-embedding and watermarking techniques". Proceeding of the IEEE, vol. 86, no. 6, pp. 1064-1087, June 1998.

[6] Vaishali S. Jabade and Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques". International Journal of Computer Applications, vol. 31, no. 1, pp. 28-34, October 2011.

[7] M. L., I. J. Cox, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker,"Digital Watermarking and Steganography". Morgan Kaufmann Publishers in 2008.

[8] Jeng-Shyang Pan, Hsiang-Chch Huang, Lakhmi C. Jain and Wai-Chu Fang, "Intelligent Multimedia Data Hiding". Springer 2004.