Watermarking Methods for User Selection System As Visible and Invisible Using DWT

Sapna Singla, Rajiv Bansal

Abstract— **Digital watermarking has become one of the most popular copyright protection methods. According to human perception, the digital watermarks can be visible and invisible. Visible watermark places a watermark over an image in such a way that it is visible to all the users about the owner of the image. The invisible watermark is done in such a way that watermark content is hidden from the user. In this paper, we presents both visible and invisible watermarking methods applied on digital images for copyright protection. In our purposed scheme we apply DWT (Discrete Wavelet Transform) to both visible and invisible methods. The proposed scheme is implemented with the help of GUI (Graphical User Interface) in MATLAB . After this, we will compare the results of visible and invisible watermark on the basis of BER(Bit Error Rate), MSE(Mean Square Ratio) and PSNR(Peak Signal To Noise Ratio).**

Index Terms — **Digital Watermarking, Discrete Wavelet Transform (DWT), Visible and Invisible watermarking, Peak Signal To Noise Ratio (PSNR), Bit Error Rate (BER), Mean Square Ratio(MSE).**

I. INTRODUCTION

In recent year all the business applications are moving towards the digital era, because of great development in latest technologies such as in the area of communication, networked multimedia system, digital data storage etc. Also from the last two decades use of internet is rapidly increased in business environment towards achievement of effectiveness and Security by introducing the digitization in their work. It is, hence, copyright protection becomes more concerned to all content owners. The technique that is useful to avoid unauthorized copying or tempering of digital data is Watermarking.

The process of embedding the watermark into a digital data is known as Digital Watermarking. Watermarking is the process of embedding data called a watermark into a multimedia object such as images, video, or text for their copyright protection[1]. The embedded watermark may be either visible or invisible. The concept of digital watermarking is associated with the steganography. It is defined as covered writing, which hides the important message in a covered media while, digital watermarking is a way of hiding a secret or personal message to provide copyrights and the data integrity. The embedded watermarks are difficult to remove and typically imperceptible, could be in the form of text, image, audio, or video. The embedding of secret watermark in digital data, no matter how much invisible it may be. However it leads to some degradation in the resultant embedded data. To overcome this limitation and to retrieve the original data, reversible watermarking has been implemented which is considered as a best approach over the cryptography.

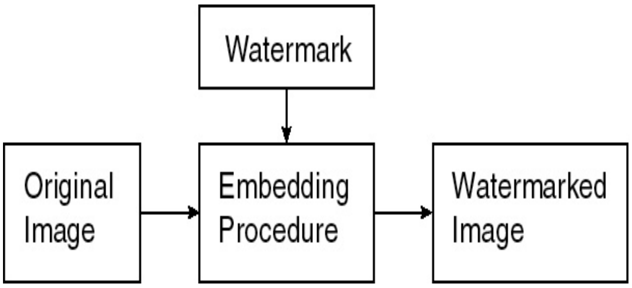

Fig1. Watermarking Algorithm general form

In digital watermarking, watermarks can be classified as many types according to its properties [4]. In terms of its visibility, digital watermark can be divided into both visible and invisible watermark. Invisible Watermarking hides the data inside the image. If an intruder tries to copy and modify the image that is already watermarked, he can be caught. Visible watermark places a watermark over an image in such a way that it is visible to all the users about the owner of the image. The invisible watermark falls into two categories: fragile watermark and robust watermark, Cox et al (2002). The fragile watermark is very easily modified. There are some built-in applications in some of the digital cameras. Each application allows the user to embed a fragile watermark into the photos produced by the digital camera. If anyone changes the photos by modifying the pixel values then this fragile watermark is broken. However, the robust watermark is used very often for copyright protection because it is not easily being attacked. In this paper we will develop a robust technique to these attacks and also discuss the quality loss factors that affect the quality of watermarking technique. Here we are using Discrete Wavelet Transformation technique for insertion and extraction of watermark from the image using invisible and visible watermarking methods.

Scholar Sapna Singla, *Department of Computer Science and Engg.., JMIT Radaur, Yamunanagar, Haryana, India.*

Assistant Professor Rajiv Bansal*, Department of Computer Science and Engg., JMIT Radaur, Yamunanagar, Haryana, India.*

Watermarking system that has been studied widely in recent years is one of the efficient methods. Research has found many watermarking algorithms that are visible, invisible, fragile and robust. Future work in the field of digital watermarking should try to encompass multiple layers of watermarks. This is because a visible watermark is not reliable and is not able to fully protect against attacks from users on the internet. Here the problem is that the person viewing the webpage where media is displayed may or may not know if it is copyright protected or not. It is up to the owner of the web page to provide valid documentation that represents the image is under copyright protection. Therefore having two layers of watermark, visible and invisible, will allow for a direct knowledge to the user visiting the website that the image is under copyright, and should not be tampered with. The one of the main features of watermarking are quality of the image.

There are a number of techniques have been developed for watermarking. Watermarks can be applied in spatial domain and in frequency domain. The spatial-domain techniques directly modify the intensity values of some selected pixels. The main disadvantage of spatial domain watermarking is that a frequent picture cropping operation may remove the watermark. The frequency-domain techniques modify the values of some transformed coefficients. This method is similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies. Upon inverse transformation, watermarks applied to the frequency domain will be dispersed over the entire spatial image, so this method is not as susceptible to defeat by cropping as the spatial technique. The watermarking scheme which is based on the frequency domains can be classified into the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) domain methods. In this paper, we will develop a system in which firstly the user will select as what type of watermarking does it need. The visible and invisible watermarking is done with the help of DWT(Discrete Wavelet Transform) technique. In invisible watermarking, watermark image can also be extracted. After this, we will compare the results of visible and invisible watermarking on the basis of MSE(Mean Square Error), BER(Bit Error Rate) and PSNR(Peak Signal To Noise Ratio).

A. Properties of Digital Watermarking

This section describes the properties of digital watermarking algorithm:

- **Imperceptibility:** The basic requirement of digital watermarking is to have the watermarked image should look alike as the original image. This confirms there is not much degradation on the original image. The embedded watermark should not be visible to human eye. To calculate the imperceptibility, generally Peak Signal to Noise Ratio (PSNR) is used.
- **Security:** The watermarking system should be secured i.e. hacker should not be in position to extract the watermark without having the knowledge of embedding algorithm. Watermarking system must be capable of stand against different attacks. Attacks try to remove, modify or embed into the watermark. Attacks are mainly classified in two different types i.e. passive attack and active attack. Passive attack only detects the watermark information, while active attack tries to modify the watermark information.
- **Robustness:** The capability of survival of watermark against both legitimate and illegitimate attacks is referred as robustness. Robustness depends on watermarks information capacity, visibility and strength. Generally a good watermarking algorithm should be robust against filter processing, noise addition, geometrical transformations such as rotation, scaling, translation and lossy compression such as JPEG compression.
- **Capacity:** Capacity of the watermarking system describes embedding of maximum amount of watermark information in single data. The higher capacity of embedding information in a data can be obtained by compromising either imperceptibility or robustness of algorithm.
- **Complexity:** The time and effort needed to embed and retrieve the watermark information is called as complexity of the watermarking system. The complex algorithm in watermarking system requires more software and hardware resources to implement it, which results in increasing the computation cost. To reduce the computational cost of watermarking system, it should be less complex. data less complex watermarking algorithms are implemented.
- **Invertibility:** This property of digital watermarking system describes the possibility of generating original data during the extraction process of watermark.

B. Applications of Digital Watermarking

Increasing research on watermarking from the past decades has been largely motivated by its applications in copyright management and protection.

- **Copyright Protection:** Digital watermarks can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.
- **Broadcast monitoring**: It is the well known application of watermarking, which helps advertising agencies to track the specific video broadcast by a TV Channel or station. Embedding the watermarked video to the host video will provide you easier way to track and monitor the broadcast.
- **Owner Identification:** It is also the well known application of watermarking, which helps in identifying the owner of video or image. Such as copyright authorities, where instead of providing copyright notice with every image or video the

watermark could be directly embedded in to the image or video itself.

- **Copy Control:** Another well know application of watermarking is copy control which helps preventing the illegal copy of songs or images of movies etc. Where by embedding watermark in songs or images of movie would instruct a watermarking compatible DVD or CD writer to not write the song or movie as it is an illegal copy**.**
- **Transaction tracking:** With the help of watermarking Transaction Tracking can be achieved by recording the transaction details in the history of a copy in digital work. For example issuing each recipient a legal copy of movie by embedding the watermark will help in tracking the source of leak in case of movie leaked to the internet.
- **Medical application:** Medical image watermarking is one of the important applications of watermarking. Medical image authentication systems which can not only authenticate medical images but would also be able to secretly communicate auxiliary information can be achieved by watermarking technique. Only the authorized people of the hospital would thus be able to modify the content of medical image.

II. DISCRETE WAVELET TRANSFORM

The DWT (Discrete Wavelet Transform) is a powerful and useful multi-resolution decomposition method in digital watermarking. DWT uses discrete wavelet transform to decompose the original image into four sub-bands LL1, LH1, HL1, and HH1, which can be separate into lower frequency sub-bands and higher frequency sub-bands. And the low frequency sub-band LL1 which stands for the coarse level coefficients can be further decomposed into four sub-bands LL2, HL2, LH2, and HH2 shown in fig. The decomposition can be repeatedly performed on the low sub image to obtain the next four images. The process is repeated several times, which is determined by the requirement of the user. When DWT is applied to the image, the image components are divided into 4 components: approximation, vertical, diagonal and horizontal. The low frequency image usually has better stability against the image distortion. DWT is easy to implement and can efficiently reduce the computation time. DWT has significant advantages over geometric attacks such as compression, scaling & cropping. It is generally observed that DWT is more robust to cropping. One more advantage of DWT is that it shows acceptable performance with scaling attacks whereas DCT technique doesn't work with scaling attacks.

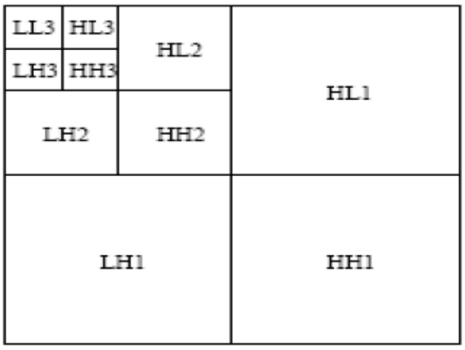

Fig2. DWT Decomposition with three levels

III. PROPOSED ALGORITHM

Our proposed scheme is based on DWT (Discrete Wavelet transform) .We are using dwt2 for 2D wavelet. The technique which is used by our proposed scheme is daubechies. Here the four components that are to be modified are approximation, horizontal, vertical and diagonal .Since we are using color images it means we have 3 layers for the colored image that are RGB (Red Green and Blue). The watermark is applied to these layers one by one. In this paper, we will develop a system in which firstly the user will select as what type of watermarking does it need. In our proposed work, visible and invisible watermarking is done with the help of DWT(Discrete Wavelet Transform) technique. In invisible watermarking, watermark image can also be extracted. After this, we will compare the results of visible and invisible watermarking on the basis of MSE (Mean Square Error), BER (Bit Error Rate) and PSNR (Peak Signal To Noise Ratio).

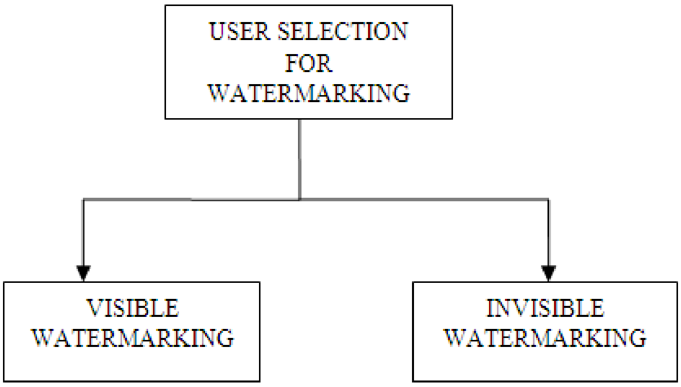

Fig3. Block Diagram of main function

A. Visible Watermarking

In visible watermarking of images, a secondary image (the watermark) is embedded in a primary (host) image such that watermark is intentionally perceptible to a human observer. Visible watermark places a watermark over an image in such way that it is visible to all the users about the owner of the image. In visible watermarking watermarked data is view as digitally stamped document. Visible watermark consists of visible message or a company logo, used to identify the owner. In visible watermarking, the watermark signal is visible in the image, video or text.

Example- Logo of the broadcaster such as ZEE TV, SONY, Life OK etc is on the right top corner of the television, it is visible to every user.

B.Invisible Watermarking

In invisible watermarking system watermark is embedded into the original data in such a way that the embedded watermark should not be visible by naked eyes. Only electronic devices (or specialized software) can extract the embedded information to prove the authenticity. Such type of system is used to identifying the source, creator, owner, and authorized consumer of a multimedia data.

C. Quality Factors

The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio. PSNR block computes the peak signal-to-noise ratio, in decibels. This ratio is frequently used as a quality measurement between the original and a watermarked image. It is given by equation:

$$\text{PSNR}= 10 \log_{10}\frac{255^2}{MSE}$$

Here MSE= Mean Squared Error between Original and Distorted Images. It is given by equation:

$$\text{MSE} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(\frac{[OI(i,j)-DI(i,j)]^2}{MxN}\right)$$

Bit Error Rate is determined by Inverse of PSNR values. The more is BER lesser will be the quality of Watermarking technique.

$$BER = \frac{1}{PSNR}$$

So BER is inversely proportional to PSNR. More the value of BER lesser will be PSNR value. Hence we will calculate PSNR , MSE and BER for visible and invisible methods and find out which one yields better results.

IV. Conclusion

In this paper a new method of visible and invisible watermarking with the help of discrete wavelet transform technique has been proposed. In the visible watermarking, the watermark image is visible on the original image but in the invisible watermarking, the watermark image is hidden from the user. The proposed scheme is implemented with the help of GUI (Graphical User Interface) in MATLAB . After that, this process is analysed on the basis of MSE(Mean square error), BER(Bit error rate) and PSNR(Peak signal to noise ratio). The high value of PSNR describes the very much better value of watermarking is obtained. Also the watermark image is extracted in invisible watermarking. The quality of the image is not much degraded through this technique. The security, accuracy and robustness is increased through this method. Hence, the comparison of the results of visible and invisible watermarking is obtained.

References

[1] M. Mohamed Ismai Majeed, S. C Ramesh, and R. Ahuja , "Implementation of a visible watermarking in a secure still digital camera using VLSI design", *International Symposium on Computing, Communication, and Control, Vol. 1, 2009.*

[2] Navas K. A., Ajay Mathews Cheriyan, Lakshmi. M, Archana Tampy. S, and Sasikumar M, "DWT-DCT-SVD Based Watermarking", *2008 3^{rd} International Conference on Communication Systems Software and Middleware and Workshops, pp. 271-274, 2008.*

[3] Shu-Kei Yip, Oscar C. Au, Chi-Wang Ho, and Hoi-Ming Wong, "Losseless Visible Watermarking", *IEEE Conference on Multimedia and Expo, pp. 853-856, 2006.*

[4] Bassem S. Rabil, Robert Sabourin, and Eric Granger, "Intelligent Watermarking with Multi-Objective Population Based Incremental Learning", *IEEE Workshop on Computational Intelligence in Biometrics and Identity Management, pp. 13-20, 2011.*

[5] Ee-Chien Chang, and Michael Orchard, "Geometric Properties of Watermarking Schemes", *International Conference on Image Processing, Vol. 3, pp. 714-717, 2000.*

[6] Shih-Hsuan Yang, and Hsin-Chang Chen, "Bit Plane Watermarking for ZeroTree Coded Images", *Asia Pacific Conference on Circuits and Systems, Vol. 2, pp. 73-78, 2002.*

[7] Wen Xing, Zhe-Ming Lu, and Hao-Xian Wang, "A Digital Watermarking Method Based on Classified Labeled-Bisecting-K-Means Clustering", *International Conference on Machine Learning and Cybernetics, Vol. 5, pp. 2891-2895, 2003.*

Sapna Singla received the B.Tech degree in Computer Science from HCTM, Kaithal in 2011 (Kurukshetra University, Kurukshetra) and the M.Tech degree in Computer Science pursuing from JMIT Radaur 2014 (Kurukshetra University Kurukshetra). Her research interests include watermarking, SQL, Computer Graphics.

Rajiv Bansal received the B.Tech degree in Computer Science from DVIET, Karnal in 2005 and the M.Tech degree in Computer Science 2010 from Department of Computer science and Applications Kurukshetra University Kurukshetra. His research interests include automata, Distributed system , Parallel processing.