Volume 4, No. 8, August 2013

Journal of Global Research in Computer Science

ISSN-2229-371X

REVIEW ARTICLE

Available Online at www.jgrcs.info

DESIGN AND DEVELOPMENT OF USER SELECTION SYSTEM FOR WATERMARKING TECHNIQUE AS VISIBLE AND INVISIBLE

Sandeep Singh[1], Rakesh singh[2]

[1]University College of Engineering, Punjabi University, Patiala, Punjab, India
sunny.nimwala@gmail.com[1]
[2]Assistant Professor, University College of Engineering, Punjabi University, Patiala, Punjab, India.
rksinghrajput@gmail.com[2]

Abstract :Watermarking is the process that embeds data called a watermark, a tag, or a label into a multimedia object, such as images, video, or text, for their copyright protection. According to human perception, the digital watermarks can either be visible or invisible. A visible watermark is a secondary translucent image overlaid into the primary image and appears visible to a viewer on a careful inspection. The invisible watermark is embedded in such a way that the modifications made to the pixel value are perceptually not noticed, and it can be recovered only with an appropriate decoding mechanism. This paper presents new visible and invisible watermarking using discrete wavelet transform (DWT). The proposed architecture is designed to compare the results of visible and invisible watermark on the basis of BER, MSE and PSNR.

Keywords: Digital watermarking, MATLAB, BER, MSE and PSNR, visible and invisible watermarking.

INTRODUCTION

The process of embedding the watermark into a digital data is known as Digital Watermarking. It is a process of embedding unremarkable logos or labels or information data or pattern into the digital data [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. Digital image watermarking is a new approach, which is suitable for medical, military, and archival based applications. 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 digital data. To overcome this and to retrieve the original data, reversible watermarking has been implemented, which considered as a best approach over the cryptography.

HISTORY

Digital watermarking is a technique to insert a digital signature into the content so that the signature can be extracted for the purposes of ownership verification and/or authentication. The term watermark has been derived from the German term *wassermarke* [2], which resembles the effect of water on paper. The oldest watermark was found in a paper originated in the town of Fabriano in Italy in the year 1282 [2]. The introduction of watermark within the paper helps to identify ownership among the papermaking industry [3]. In the year 1887 in France, two watermarked letter helps to solve a prosecution case. William Congreve, an Englishman, invented a technique for paper watermarking by inserting dyed material into the middle of the paper at the time of producing the paper [2]. Another Englishman, William Henry Smith was developed a method of paper watermarking by pressing the paper mold with a sort of shallow relief sculpture [2]. Paper

watermarks are extensively used in bank notes and stamps nowadays. In 1954, Emil Hembrooke of Muzak Corporation has designed a technique to watermark musical property [2]. In 1979, Szepanski developed a watermark pattern for anti-counterfeiting and in the late 1980‟ s, there evolved a term called digital watermarking analogues to the paper watermarking. In the year 1986, Holt et al. described a watermarking method for audio signal [2]. In the year 1988, Komatsu and Tominga, first coined the term *digital watermark* in their works. Since 1995, digital watermarking has gained a lot of attention from researchers as well as from several different organizations and growing very rapidly [3]. In the year 1996, digital watermarking gets its first global acceptance when they are included as one of the primary topics in the Information Hiding Workshop (IHW) [2].

Watermarking Types

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. 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 marks because it is not easily being attacked. For example, if we embed a robust watermark throughout a picture, the ownership of the picture can be secured by this copyright mark, Perter (2002) and Petitcolas et al (1999). Watermarks can also be divided into informed and blind watermarks by using different detection techniques. Informed watermark can only be detected by comparing watermarked image and the original image. Blind watermark does not depend on original image. Therefore, blind watermarking is a technique that the original image is not needed in watermark extraction process. Internet digital information protection is achieved through blind watermarking because with watermarked information, message can be detected successfully without original data.

Properties of Digital Watermarking

An effective digital watermarking algorithm must have number of properties. This section describes the number 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. This property is known as imperceptibility or transparency of the watermarking system. The embedded watermark should not be visible to human eye. To calculate the imperceptibility, generally Peak Signal to Noise Ratio (PSNR) is used.
- **Robustness:** The capability of survival of watermark against both legitimate and illegitimate attacks is referred as robustness. All watermarking system needs to resists against any legitimate and illegitimate attacks, except fragile watermarking system. For manipulation recognition in original data the watermark has to be fragile to detect altered media. 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.
- **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 _rm against different attacks. Attacks try to remove, modify or embed (unwanted information) 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.
- **Complexity:** The time and effort needed to embed and retrieve the watermark information is known 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. Such as in telemedicine domain, to cut the cost of bandwidth consumption during the transmission of medical data less complex watermarking algorithms are implemented.
- **Capacity:** Capacity of the watermarking system describes embedding of maximum amount of watermark information i.e. embedding the multiple watermarks in single data. The higher capacity of embedding information in a data can be obtained by com- promising either imperceptibility or robustness of algorithm.
- **Invertibility:** This property of digital watermarking system describes the possibility of generating original data during the extraction process of watermark.
- **Verification:** This property defines the procedure of verification i.e. private key verification and public key verification, depending on its respective algorithm.

Application of Watermarking

Increasing research on watermarking from the past decades has been largely motivated by its applications in copyright management and protection. The digital watermarking technique is highly suitable for medical, military, and archival based applications.

- Broadcast monitoring 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 is also a 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.
- 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.
- 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 (different watermark for different recipient) will help in tracking the source of leak in case of movie leaked to the internet.
- 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.

Attacks on Watermarks

- **Removal Attacks:** Removal attacks achieve complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm. This category includes denoising, quantization, remodulation, averaging, and collusion attacks. Not all of these methods always come close to complete watermark removal, but they may damage the watermark information significantly.

- **Geometrical Attacks:** Geometrical attacks do not remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. To this category there belong the cropping, flip, rotation and synchronization removal attacks too.[4] geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information.
- **Cropping:** This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.
- **Flipping:** Many images can be flipped without losing quality. Few watermarks survive flipping, although resilience to flipping is easy to implement.

Original Image

Flipped Image

- **Cryptographic Attacks:** Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is brute-force search for the embedded secret information. Practically, application of these attacks is restricted due to their high computational complexity.
- **Protocol Attacks:** Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is the copy attack. The main idea of a copy attack is to copy a watermark from one image to another image without knowledge of the key used for the watermark embedding to create ambiguity with respect to the real ownership of data [5]. Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. Protocol attacks aim at attacking the entire concept of the watermarking application.

Proposed Watermarking Method

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. Compare the results of visible and invisible watermarking on the basis of MSE, BER and PSNR. There are the three block diagrams. First block diagram is for the user selection watermarking either it is visible or invisible. The second and third diagrams are for visible and invisible watermarking simultaneously.

Proposed algorithm:-

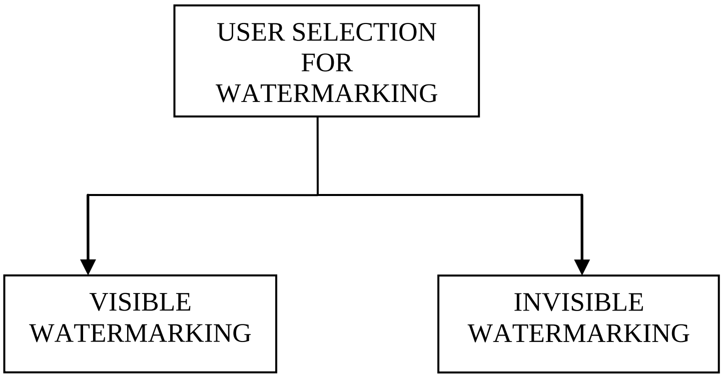

Figure1. Block diagram of main function

Step 1-First of all user should select the type of watermarking either it is visible or invisible.

Step 2-After selecting the type of watermarking, watermark process begins according to the selection.

VISIBLE WATERMARKING

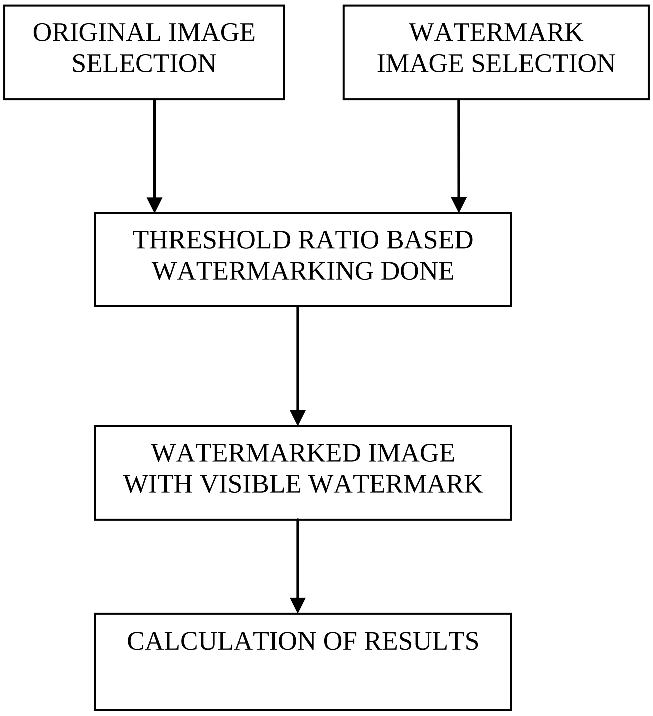
ORIGINAL IMAGE SELECTION
WATERMARK IMAGE SELECTION
THRESHOLD RATIO BASED WATERMARKING DONE
WATERMARKED IMAGE WITH VISIBLE WATERMARK
CALCULATION OF RESULTS

Figure2.Block diagram of visible watermarking

INVISIBLE WATERMARKING

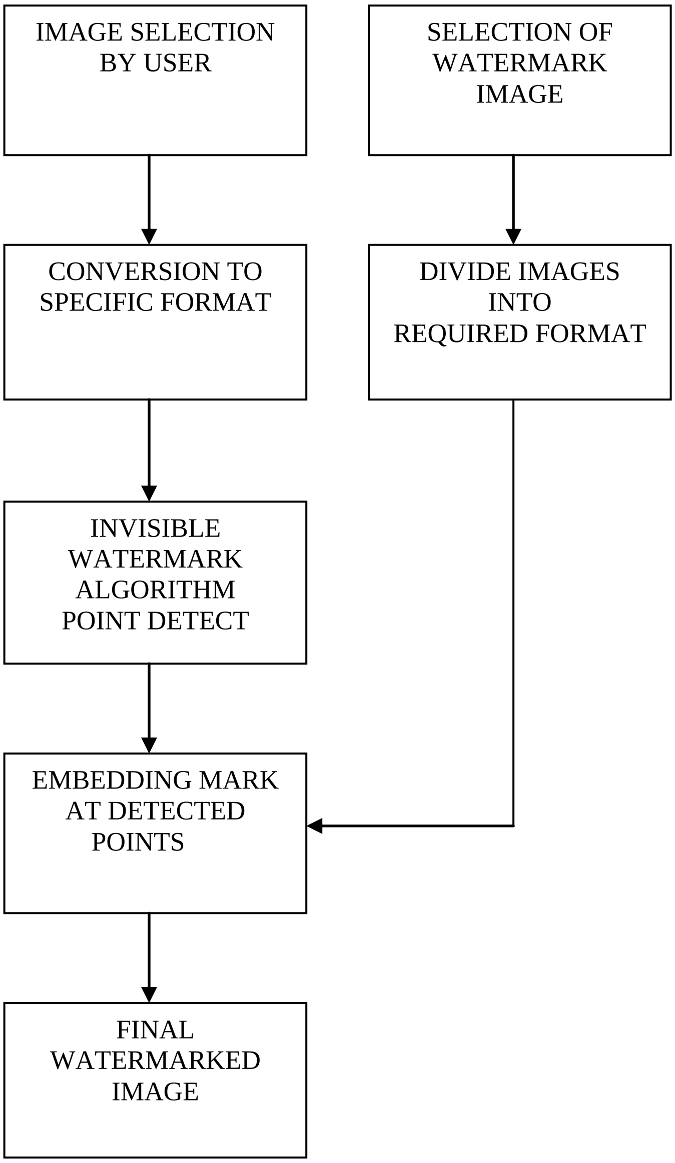
IMAGE SELECTION BY USER
SELECTION OF WATERMARK IMAGE
CONVERSION TO SPECIFIC FORMAT
DIVIDE IMAGES INTO REQUIRED FORMAT
INVISIBLE WATERMARK ALGORITHM POINT DETECT
EMBEDDING MARK AT DETECTED POINTS
FINAL WATERMARKED IMAGE

Figure3. Block diagram of invisible watermarking

Conclusion

In this paper a new method of visible and invisible watermarking with the help of discrete wavelet transform technique has been proposed. By use of this technique an original image embed the blocks of watermark image on to the original image. 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. In the visible watermarking, the watermark image is visible on the original image but in the invisible watermarking, the watermark image is hidden behind the original image. 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] FromWikipediahttp://en.wikipedia.org/wiki/Digital_watermarking.

[2] J. J. Cox, M. L. Miller, J. A. Bloom, J. K. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann Publishers, 2nd Edition, 2003.

[3] S. Katzenbeisser, and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking,

[4] Artech House, Boston, USA, 2000.

[5] Jahnvi Sen et al / Indian Journal of Computer Science and Engineering (IJCSE)

[6] Dr. Murali Subbarao/ ESE558 DIGITAL IMAGE PROCESSING.

SHORT BIODATA OF ALL THE AUTHOR

Sandeep Singh is pursuing M.Tech in Computer Engineering from Punjabi University, Patiala. He has done his B.Tech from HCTM, Kaithal(Haryana). His areas of interest include image processing and computer graphics. Sandeep Singh can be contacted at neternagra@gmail.com

Rakesh Singh is Assistant Professor in Department of Computer Engineering at Punjabi University, Patiala. His area of interest is image processing. Rakesh Singh can be contacted at rksinghrajput@gmail.com