# Optimization of Invisible Watermarking using Point Detection Algorithm

**Prachi Sharma[1] Parvinder Yadav[2]**
[2]Assistant Professor
[1]Shree Siddhivinayak Group of Institutions, Kurukshetra University, Kurukshetra (Haryana)
[2]IITT College of Engineering, Sirmour, H.P.(173030)

*Abstract*— In a digital image watermarking system, information carrying watermark is embedded in an object, the object may be an image or audio or video. Image object have been used in this paper. In general, watermark can be embedded in spatial domain or transform domain technique of an image. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

***Key words:*** Watermarking, Data Hiding, Watermarking Techniques, Watermarking Requirements

## I. INTRODUCTION

Digital watermarking is defined as a process of embedding data (watermark) into a multimedia object to protect the owner's right to that object. The embedded watermark may be either visible or invisible. Images can be processed in two main approaches as spatial domain and frequency domain approach. Watermarking algorithm that rely on spatial domain, hide the watermark by modifying pixel values of the host image. On the other hand in frequency based techniques the host image is first converted into different frequencies by suitable transform. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

## II. 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 [1], 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 [1]. The introduction of watermark within the paper helps to identify ownership among the papermaking industry [2]. 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 [1]. Another Englishman, William Henry Smith was developed a method of paper watermarking by pressing the paper mold with a sort of shallow relief sculpture [1]. 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 [1]. In 1979, Szepanski developed a watermark pattern for anti-counterfeiting and in the late 1980ʺs, 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 [1]. 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 [2]. 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) [1].

## III. WATERMARKING TYPES

In digital watermarking, watermarks can be classified as many types according to its properties. [3] 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 afragile 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

## IV. DIGITAL WATERMARKING APPLICATIONS

### *A. Owner Identification*

The owner identification can be printed on the covers or mentioned somewhere on the item. Examples are the identification mark of an audio company on the CD Copy 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.
Boadcast Monitoring: This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

### *B. Tamper Detection*

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

 

### *C. Authentication and Integrity Verification*

Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image.

### *D. Fingerprinting*

Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared.

## V. ATTACKS ON WATERMARKS

### *A. 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.

### *B. 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.

### *C. 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.

### *D. 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

Fig. 1:

### *E. 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.

### *F. 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.[4] 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.

## VI. PROPOSED WATERMARKING METHOD

In our proposed work, watermarking is done with the help k-harries point detection algorithm which is is used to find sharp points in the original image. the harries algorithm is basically edge point detection algorithm. the below diagram depicts the whole work of points are found on original image and when to embed watermark blocks onto that points;

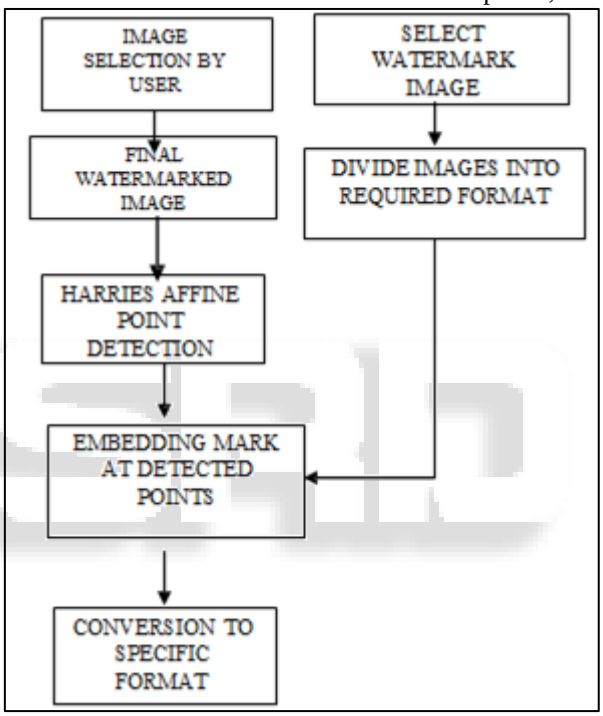


Fig. 1: Watermarking Preces

### *A. Water marking scheme consists of*

watermark embedding and watermark extracting. The encoding process is outlined in Figure 3, whereby the watermarking will be embedded / encoded into host image ether for visible and invisible watermarking. Watermarked image and key file will be obtained [5].

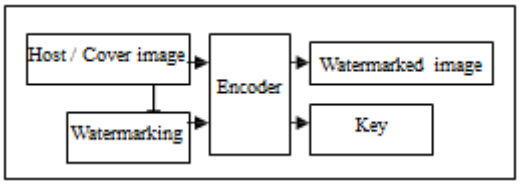


Fig. 3: Watermark Embedding

The Decoding step conversely requires reading the watermarked image and the key file to extract the watermarking. The watermarking will be extracted by using the same key used in the embedding / encoding stage. The decoding process is outlined in Figure 4. The proposed technique extracts the watermark from the marked image only without the original one.

 

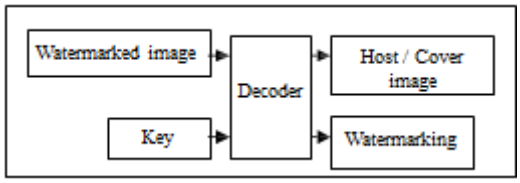


Fig. 4: Watermark Detection

- Step 1-First of all user should select the image accordindg to the image format which is defined by him/her
- Step 2-After selecting the image, check that whether the image is colour image or gray image. If image is colour image then convert the given image into grey image whereas if image is grey image then leave the image as it is. my work is on grey image that's why i convert the image into grey format.
- Step 3-After that, use the harries affine point detection algorithm to find the sharp edge points in the selected image. Step 4-Select the watermark which you want to embed or hide in the carrier image. convert the selected watermark image into grey format if it is in colour format otherwise, leave it .The conversion is done in the same way as it is done in the step 2. Step 5-Divide the watermark image into blocks of equal size for example take [33 33] size of the blocks of watermark image. water mark image image is divided into blocks in order to increase the security. so, that no un-authorized be able to encrypt the image.
- Step 6-In this step check the required harries point to embed the blocks of watermark image. If Available points are more than required then embed the blocks of watermark image into the points of orignal image which are find using harries affine point detection algorithm otherwise chaze the size of blocks of watermark image.
- Step 7-The detail of available points, required points, harries points are also embed into the original image. This information is used while extracting the watermark image from original image.

## VII. WATERMARK EXTRACTION

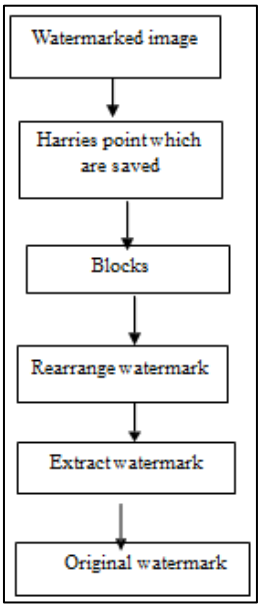


Fig. 5: Extraction of watermark

The watermark extraction process is opposite of the watermarking the image. In this watermark is extracted from watermarked image through the harries points which are being saved by us during watermarking in step 7.These saved harries points tells the detail on to which points the blocks of watermark image is embed with the help of these detail we can easily extract the blocks. After that, the extract blocks are to be reagganged in order to create the original watermark image. During extraction only authorized user can only extract the watermark from the image as the un-authorized user do not know the coding or procedure of embedding the blocks on to harries points. our work is on on invisible watermarking. so, here we have to extract the invisible watermark.

## VIII. CONCLUSION

In this paper a new method of invisible watermarking with the help of k-harries point edge detection algorithm has been proposed. By use of algorithm find harries points on original image and embed the blocks of watermark image on to the harries points of orignal image. By the use of this procedure psnr(peak signal to noise ratio) value of image is obtained this value is much better than the value obtained through through lsb technique. Along with psnr mse(mean square error) andber(bit error rate) is also counted which provide satisfactary results. The security accuracy and robuteness is increased through this method. The quality of the image is not much degraded through this technique. Hence, it is difficult to detect the changes in the original image.

## REFERENCES

[1] 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.
[2] S. Katzenbeisser, and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston, USA, 2000.
[3] Jahnvi Sen et al / Indian Journal of Computer Science and Engineering (IJCSE)
[4] Dr. Murali Subbarao/ ESE558 DIGITAL IMAGE PROCESSING.

 