IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

DIGITAL IMAGE WATERMARKING

Bhavi Naik
Electronics&Communication Engg. Dept., S.N.Patel Institute of Tech. & Research. Umrakh, Bardoli, Surat, Gujarat, India[1]

Abstract*: *The rapid expansion of the Internet and the overall development of digital technologies in the past years have sharply increased the availability of digital multimedia content. One of the great advantages of digital data is that it can be reproduced without loss of quality. However, it can also be modified easily. In many contexts, such for legal evidence and for video security systems, any modifications of image, video or audio data have to be detected. Therefore, some work needs to be done in order to develop security systems to protect the information contained in digital data (Cox, 1997).Watermarking (Chiou, 1999; Cox, 2002; Cox, 2001; Nikolaidis, 1996; Wolfgang, 1996; Wolfgang, 1999) is the process of embedding data into a multimedia. A scrambled version of watermark is obtained with the help of Arnold Transform. The operation of embedding and extraction of watermark is done in high frequency domain of Discrete Wavelet Transform since small modifications in domain are not perceived by human eyes. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed to measure image quality.

Keywords: **image watermarking,watermarking properties,watermarking techniques, Applications of watermarking, watermarking Attacks**

INTRODUCTION

A watermark is an invisible mark that is placed on the image which can be visible when the image is compared to the original. The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the original document. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. Further, the invisible watermarks are categorized into watermarking techniques as fragile and robust.The paper has organized as: Properties of watermarking, Techniques of embedding watermarking, Applications of watermarking, Attacks on watermarking

Properties Of Watermark :

A.Robustness:

The robustness is the ability of detecting the watermarkafter some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation , and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement . In addition, not all watermarki algorithms have the same level of robustness, Some techniques are robust against some manipulation operations, however, they fail against other stronger attacks . Moreover, it's not always desirable for watermark to be robust, in some cases; it's desired for the watermark to be fragile.

B.Imperceptibility:

Imperceptibility (also known as *Invisibility* and *Fidelity*) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image . In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness. However, the challenge is that imperceptibility could be achieved, but the robustness and the capacity will be reduced, and vice versa, imperceptibility may be sacrificed by increasing the robustness and the capacity. Moreover, the watermark not always desired to be invisible, sometimes, it is preferred to have visible watermark into the image .

C.Capacity:

Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for . Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness .

D.Security:

Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection . According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks. Therefore, for unauthorized removal, the watermark should be robust and not to be removed, and for unauthorized embedding (also known as forgery), the watermark should be fragile or semi fragile to detect any modification. Lastly, for unauthorized detection, it should be imperceptible watermark.

E.Low Complexity*:*

The cost is the reason behind studying the complexity, so it should be at a reasonable cost . It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used. The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors.

The various properties of watermarks are: The watermark must be difficult or impossible to remove, at least without visibly degrading the originalimage.The watermark must survive image modifications that are common to typical applications, such as scaling and color requantization, commonly performed by a picture editor, or lossy compression techniques like JPEG, used for transmission and storage. An invisible watermark should be

imperceptible so as not to affect the experience of viewing the image. For some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decodability without requiring the original, unwatermarked image would be necessary for efficient recovery of property and subsequent prosecution.

Watermarking Techniques :

In the papers that we have referred, there have defined two techniques for embedding a watermark.

1)spatial domain[3]

I. LSB(least significant beat)
II. ISB(intermediate significant beat)
III. Patchwork

2) transform domain

I. Discrete cosine transform
II. Discrete Wavelet Transform
III. SVD transform.

Several different methods enable watermarking in the spatial domain. The simplest(too simple for many applications) is to just flip the lowest-order bit of chosen pixels in a gray-scale (8-bit) or color(24-bit) image. This works well only if the image will not be subject to any modification, such as color modification done by a photo editor.Another technique embeds a more robustwatermarking.

- **LSB(least significant beat)**

In LSB, information and their effect does not cause visible changes And this technique is used for simple operation to embed information into a host image. The idea behind LSB is very simple; the host image pixels are changed by no of bits of the secret message. Despite of the number was embedded into the first 8 bytes of the grid, the 1 to 4 least bits needed to be modified according to the embedded secret message. On the average, only half of the bits in an image will need to be changed to hide a secret message using a host image. Because the quality of the Watermarked image is low, less than over the 4 least significant bits, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be recognized by the human visibility system. However, a passive attacker can easily extract the changed bits, because it has performed very simple operation. For instance, Figure 3 shows the 4-bit LSB. In Figure 3, the pixel value of the cover image is 150 (10010110) and the secret data are 1100. Then the changed pixel value of the cover is 156 (10011100). LSB can store 4-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data [3].

- **The watermark algorithm in wavelet domain:-**

The aim of the watermark extraction process is to reliably obtain an estimate of the original watermark from a possibly distorted version of the watermarked image. The detection process is inverse procedure of the watermark insertion process. It requires knowledge of the watermarked image $WI(m, n)$ and the key $Key(m, n)$. One of the advantages of wavelet-based watermarking is its ability to spread the watermark all over the image. If a part of the image is cropped, it may still contain parts of the watermark. These parts of watermark may be detected by certain mechanism even if the image has been further scaled or rotated. The watermark extraction algorithm is presented.

The watermark extraction algorithm is described as follows in fig.

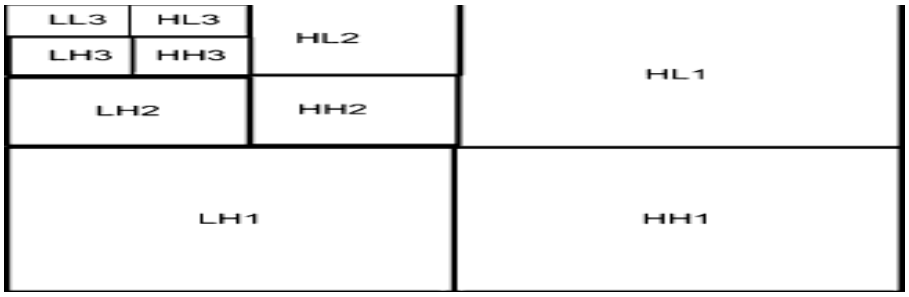

Fig 1:DWT pyramid decomposition of an image[4]

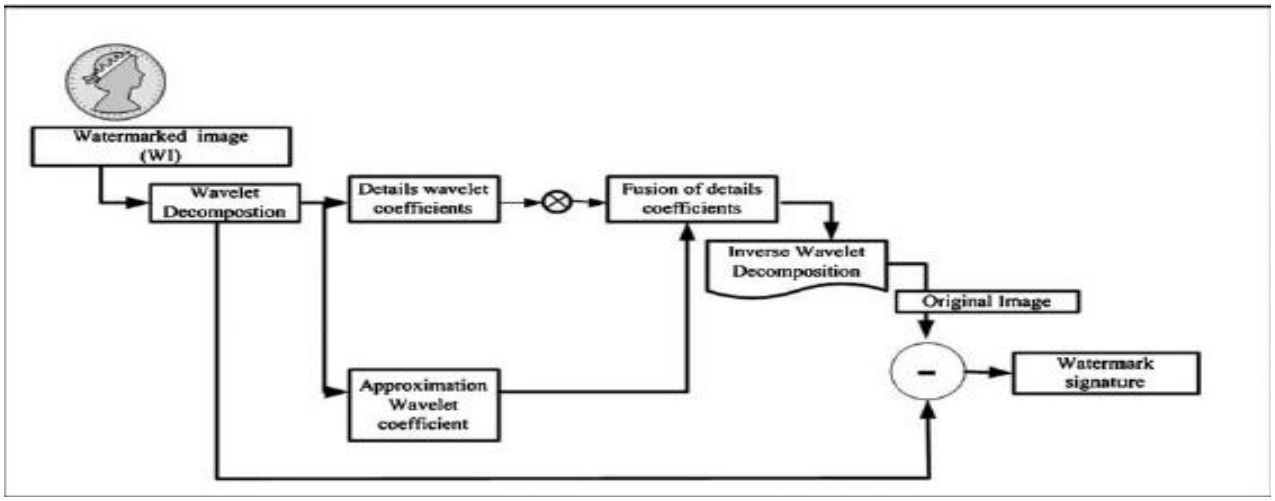

Fig 2: The embedded algorithm in wavelet domain[4]

- **Discrete cosine Transform:-**

DCT is widely used in digital image watermarking since it has strong robustness. In addition, many frequency coefficients are obtained from DCT, such as single direct current DC coefficient, low frequency coefficients, mid frequency coefficients, and high frequency coefficients.By the different characters of these coefficients, we can obtain different effects upon digital watermarking system. Moreover, JPEG standard and Watson visual model based on DCT with block size 8×8, which is commonly used in image watermarking.

The coefficient in the coordinate (0,0) which is represented by a square is the DC coefficient, low frequency coefficients are represented by triangles, mid frequency coefficients are

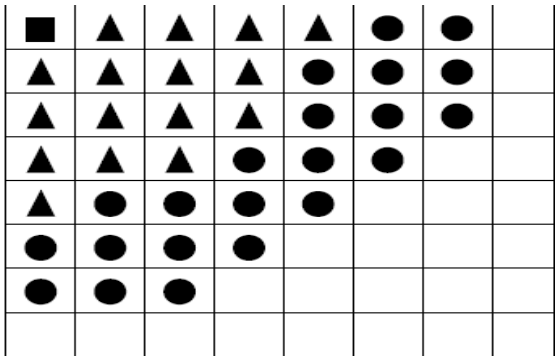

Fig 3: Coefficient of Block DCT[3]

represented by circles, and the rest are the high frequency coefficients. Despite of DCT watermarking techniques have strong robustness; they also have their own drawbacks, such

as low watermarking capacity. coefficients are used compared to DC coefficient. On the other hand, DC has more robust than low frequency coefficients.

Watermarking Applications :

Copyright Protection : The copyright information can be embedded as a watermark into the new production. Once there is a dispute on the ownership, the watermark can be extracted toprovide the evidence of who is the owner of this product. Copyright protection can be done by using various methods of embedding a watermark.[1]

Fig 4: original image watermark watermarked image

Using the DWT method[2]

Protecting Ownership : Digital watermarking allows each image to be uniquely marked for every buyer, so that illicit copies can br traced to their source.

Broadcast Monitoring : This type of monitoring is used especially in the advertisements to make sure that the content broadcasted as the contract between the advertisement company and the customer.

Fingerprinting : The main purpose of fingerprinting is to protect customers. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this .This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient.Thus, the owner can identify who redistributed this product by extracting the watermark from the illegal copy.

Copy Control: The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software for updating the watermark whenever it has been used. It also provides copy tracking for unauthorized distribution since the owner of data is embedded in the watermark.

Medical Applications*:* Image watermarking can be used in medical images for several purposes. It's used to protect the patient's information from unauthorized people. In addition, it can be used for authentication if the patient lost the image. Moreover, it is needed to protect the copyright of the medical image [6]. For example, mammograms contain diagnostic information which can be used for early detection of breast cancer diseases and breast abnormality.

Protection and authentication of such images are now becoming increasingly very significant in telemedicine field where images are easily distributed over the internet. For mammogram medical image, it should be sure that embedding watermark does not affect the diagnostic information of the mammogram.

Attacks On Watermark :

Digital image watermarking attacks can be classified to intentional attacks and non-intentional attacks. An attack succeeds in overcome a watermarking scheme if it weakens the watermark less than acceptable limits. On the other hand, recall the differentiation between

achieving robustness and imperceptibility at the same time, it should be a balance to achieve them together. However, this paper highlights the attacks that affect the robustness directly, it highlights some common attacks such as JPEG compression attack, Noise, and Geometric attacks. First, JPEG is a standard compression technique, and it reduces the size of images for the goals of storage and transmission. As the compression rate increases, the quality of the image decreases. Second, Noise attacks are the data that are not part of the original image which caused by other sources. There are many types of noise such as Gaussian noise, and blurring noise [7]. Lastly, Geometric attack is a set of parameters that can be applied on the image. There are many types of geometric attacks such as rotation, cropping, and other transformations [3].

CONCLUSION

This paper has covered the concept of digital watermarking and its properties along with the various techniques for embedding a watermark.it has also outlined its applications and techniques of achieving a few.

ACKNOWLEDGMENT

This work is supported by my faculty and I thank them for their valuable suggetions.

REFERENCES

[01] **J.J.K.Ruainaidh, W.J.Dowling, F.M.Boland,** Watermarking digital image for copyright protection

[02] Hal Berghel University of Arkansas Lawrence O'Gorman Bel Laboratories Protecting Ownership rights though digital watermarking**.**

[03] **Mohammad Abdullatif Akram M. Zeki Jalel Chebil Teddy Surya Gunawan** Properties of Digital Image Watermarking.

[04] **Ella HASSANIEN** A Copyright Protection using Watermarking Algorithm

[05] **Dr.M.Mohamed Sathik and S.S.Sujatha** An Improved Invisible Watermarking Technique for Image Authentication.

[06] **A. M. Zeki, A. A. Manaf, C. F. M. Foozy, and S. S. Mahmod**, "A

[07] Watermarking Authentication System for Medical Images," presented at the World Congress on Engineering and Technology (CET 2011), Shanghai, China, 2011.

[08] **O. O. Khalifa, Y. binti Yusof, A. H. Abdalla, and R. F. Olanrewaju**, "State-of-the-art digital watermarking attacks," in *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, 2012, pp. 744-750

